AX2340S Software Manual

Operation Command Reference

For Version 2.5

AX23S-S004X-60

AlaxalA

■ Relevant products

This manual applies to the models in the AX2340S series of switches. It also describes the functions 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

Cisco is a registered trademark of Cisco Systems, Inc. in the United States and other countries.

Ethernet is a registered trademark of Xerox Corporation.

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

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

Python is a registered trademark of Python Software Foundation.

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

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

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

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

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

Other company and product names in this document are trademarks or registered trademarks of their respective owners.

■ Reading and storing this manual

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

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

■ Note

Information in this document is subject to change without notice.

■ Editions history

June 2024 (Edition 1) AX23S-S004X-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 19

Command description format 20
Specifiable values for parameters 22
List of character codes 25
Error messages displayed by the entry-error location detection function 26

PART 2: Operation Management

2. Switching the Command Input Mode 29

enable 30
disable 31
quit 32
exit 33
logout 34
configure(configure terminal) 35

3. Operation Terminals and Remote Operations 37

set exec-timeout 38
set terminal help 39
set terminal pager 40
show history 41
telnet 42
ftp 44
tftp 48

4. Configurations and File Operations 51

show running-config(show configuration) 52
show startup-config 53
copy 54
erase startup-config 57
show file 58
cd 60
pwd 61
ls 62
dir 63
cat 66
cp 67
mkdir 69
mv 70

rm 71
rmdir 72
delete 73
undelete 74
squeeze 75

5. Login Security and RADIUS/TACACS+ 77

adduser 78
rmuser 80
password 81
clear password 83
show sessions (who) 84
show whoami (who am i) 85
killuser 88
show accounting 90
clear accounting 94
restart accounting 95
dump protocols accounting 96

6. SSH 97

ssh 98
sftp 101
scp 105
show ssh hostkey 108
set ssh hostkey 110
erase ssh hostkey 112
show ssh logging 113
clear ssh logging 120

7. Time Settings and NTP 121

show clock 122
set clock 123
show ntp associations 124
restart ntp 126

8. Utilities 127

diff 128
grep 129
more 130
less 131
tail 132
hexdump 133

9. Device Management 135

show version 136

show system 138
clear control-counter 144
show environment 145
reload 149
show tech-support 151
backup 154
restore 156

10. Checking Internal Memory and Memory Cards 159

show mc 160
format mc 161
show flash 162

11. Resource Information 165

show cpu 166
show processes 169
show memory 171
df 172
du 173

12. Dump Information 175

erase dumpfile 176
show dumpfile 177

13. Memory Card Operation Mode 179

set mc-configuration 180
update mc-configuration 181

14. Software Management 183

ppupdate 184
set license 186
show license 187
erase license 188

15. Power Saving Functions 189

show power 190

16. Log 191

show logging 192
clear logging 194
show logging console 195
set logging console 196

17. SNMP 197

show snmp 198
show snmp pending 203

snmp lookup 205
snmp get 206
snmp getnext 207
snmp walk 208
snmp rget 210
snmp rgetnext 211
snmp rwalk 213

18. Advanced Script 215

python 216
stop python 220
pyflakes 221
install script 222
uninstall script 224
show script installed-file 225
show script running-state 227
show event manager history 229
show event manager monitor 231
clear event manager 235
restart script-manager 237
restart event-manager 238
dump script-user-program 239
dump script-manager 241
dump event-manager 242

19. Python Extension Library 243

List of provided modules 244
__init__ method (commandline.CommandLine class) 245
exec method (commandline.CommandLine class) 246
exit method (commandline.CommandLine class) 248
set_default_timeout method (commandline.CommandLine class) 249
set_default_logging method (commandline.CommandLine class) 250
sysmsg.send 252
eventmonitor.regist_sysmsg 254
eventmonitor.regist_cron_timer 258
eventmonitor.regist_interval_timer 261
eventmonitor.event_delete 263
eventmonitor.event_receive 264
eventmonitor.get_exec_trigger 267

PART 3: Network Interfaces

20. Ethernet 271

show interfaces 272

clear counters 281
show port 282
activate 293
inactivate 294
test interfaces 295
no test interfaces 298
show power inline 301
activate power inline 305
inactivate power inline 306

21. Link Aggregation 307
show channel-group 308
show channel-group statistics 317
clear channel-group statistics lacp 321
restart link-aggregation 322
dump protocols link-aggregation 323

PART 4: Layer 2 Switching

22. MAC Address Table 325
show mac-address-table 326
clear mac-address-table 330

23. VLAN 333
show vlan 334
show vlan mac-vlan 342
restart vlan mac-manager 344
dump protocols vlan 346

24. Spanning Tree Protocols 347
show spanning-tree 348
show spanning-tree statistics 375
clear spanning-tree statistics 381
clear spanning-tree detected-protocol 383
show spanning-tree port-count 385
restart spanning-tree 388
dump protocols spanning-tree 389

25. Ring Protocol 391
show axrp 392
restart axrp 395
dump protocols axrp 396

26. IGMP/MLD snooping 397
show igmp-snooping 398

clear igmp-snooping 405
show mld-snooping 407
clear mld-snooping 412
restart snooping 413
dump protocols snooping 414

PART 5: IP Interfaces

27. IPv4 Communication 415
show ip-dual interface 416
show ip interface 419
show ip arp 422
clear arp-cache 425
show netstat(netstat) 427
ping 429
traceroute 432
show ip route 434
show tcpdump (tcpdump) 435

28. IPv6 Communication 443
show ip-dual interface 444
show ipv6 interface 445
show ipv6 neighbors 448
clear ipv6 neighbors 450
show netstat(netstat) 451
ping ipv6 452
traceroute ipv6 455
show ipv6 route 457
show ipv6 router-advertisement 458
show tcpdump (tcpdump) 460

29. DHCP Server Function 461
show ip dhcp binding 462
clear ip dhcp binding 464
show ip dhcp import 465
show ip dhcp conflict 467
clear ip dhcp conflict 468
show ip dhcp server statistics 469
clear ip dhcp server statistics 471
restart dhcp 472
dump protocols dhcp 473
dhcp server monitor 474
no dhcp server monitor 475

PART 6: Filters and QoS

30. Filters 477

show access-filter 478
clear access-filter 482

31. QoS 485

show qos-flow 486
clear qos-flow 488
show qos queueing 490
clear qos queueing 494

PART 7: Layer 2 Authentication

32. IEEE 802.1X 495

show dot1x statistics 496
show dot1x 499
clear dot1x statistics 503
clear dot1x auth-state 504
reauthenticate dot1x 506
restart dot1x 508
dump protocols dot1x 510
show dot1x logging 511
clear dot1x logging 521

33. Web Authentication 523

set web-authentication user 524
set web-authentication passwd 525
set web-authentication vlan 526
remove web-authentication user 527
show web-authentication user 528
show web-authentication login 530
show web-authentication logging 532
show web-authentication 544
show web-authentication statistics 548
clear web-authentication logging 550
clear web-authentication statistics 551
commit web-authentication 552
store web-authentication 553
load web-authentication 554
clear web-authentication auth-state 556
set web-authentication html-files 558
clear web-authentication html-files 560
show web-authentication html-files 561

clear web-authentication dead-interval-timer 563
set web-authentication ssl-crt 564
clear web-authentication ssl-crt 566
show web-authentication ssl-crt 567
restart web-authentication 569
dump protocols web-authentication 571

34. MAC-based Authentication 573

show mac-authentication login 574
show mac-authentication logging 576
show mac-authentication 588
show mac-authentication statistics 591
clear mac-authentication auth-state 593
clear mac-authentication logging 594
clear mac-authentication statistics 595
set mac-authentication mac-address 596
remove mac-authentication mac-address 598
commit mac-authentication 599
show mac-authentication mac-address 600
store mac-authentication 602
load mac-authentication 603
restart mac-authentication 604
dump protocols mac-authentication 605
clear mac-authentication dead-interval-timer 606

35. Multistep Authentication 607

show authentication multi-step 608

PART 8: Security

36. DHCP snooping 611

show ip dhcp snooping binding 612
clear ip dhcp snooping binding 615
show ip dhcp snooping statistics 617
clear ip dhcp snooping statistics 619
show ip arp inspection statistics 620
clear ip arp inspection statistics 622
show ip dhcp snooping logging 623
clear ip dhcp snooping logging 634
restart dhcp snooping 635
dump protocols dhcp snooping 636

PART 9: High Reliability Based on Redundant Configurations

37. GSRP aware 637

show gsrp aware 638
restart gsrp 640
dump protocols gsrp 641

38. Uplink Redundancy 643

show switchport-backup 644
set switchport-backup active 648
restart uplink-redundant 649
dump protocols uplink-redundant 650
show switchport-backup statistics 651
clear switchport-backup statistics 653

PART 10: Network Monitoring Functions

39. L2 Loop Detection 655

show loop-detection 656
show loop-detection statistics 659
show loop-detection logging 661
clear loop-detection statistics 663
clear loop-detection logging 664
restart loop-detection 665
dump protocols loop-detection 666

40. Storm Control 667

show storm-control 668
clear storm-control 672

PART 11: Network Management

41. sFlow Statistics 673

show sflow 674
clear sflow statistics 677
restart sflow 678
dump sflow 679

42. IEEE 802.3ah/UDLD 681

show efmoam 682
show efmoam statistics 684
clear efmoam statistics 686
restart efmoam 687
dump protocols efmoam 688

43. CFM 689

l2ping 690
l2traceroute 693
show cfm 696
show cfm remote-mep 700
show cfm fault 704
show cfm l2traceroute-db 707
show cfm statistics 711
clear cfm remote-mep 715
clear cfm fault 716
clear cfm l2traceroute-db 717
clear cfm statistics 718
restart cfm 720
dump protocols cfm 721

44. LLDP 723

show lldp 724
show lldp statistics 732
clear lldp 734
clear lldp statistics 735
restart lldp 736
dump protocols lldp 737

PART 12: Response Messages

45. Response Messages 739

45.1 Response messages 740
45.1.1 Common 740
45.1.2 Switching the command input mode 740
45.1.3 Operation terminals and remote operations 740
45.1.4 Configurations and file operations 743
45.1.5 Login security and RADIUS/TACACS+ 746
45.1.6 SSH 747
45.1.7 Time settings and NTP 750
45.1.8 Device management 751
45.1.9 Checking internal memory and memory cards 752
45.1.10 Dump information 752
45.1.11 Memory card operation mode 753
45.1.12 Software management 753
45.1.13 SNMP 754
45.1.14 Advanced script 755
45.1.15 Ethernet 756
45.1.16 Link aggregation 758

45.1.17 MAC address table 759
45.1.18 VLAN 759
45.1.19 Spanning tree protocols 760
45.1.20 Ring Protocol 760
45.1.21 IGMP/MLD snooping 761
45.1.22 IPv4 communication 762
45.1.23 IPv6 communication 765
45.1.24 DHCP server function 765
45.1.25 Filters 766
45.1.26 QoS 766
45.1.27 IEEE 802.1X 767
45.1.28 Web authentication 767
45.1.29 MAC-based authentication 769
45.1.30 Multistep authentication 770
45.1.31 DHCP snooping 770
45.1.32 GSRP aware 770
45.1.33 Uplink redundancy 771
45.1.34 L2 loop detection 771
45.1.35 Storm control 771
45.1.36 sFlow statistics 772
45.1.37 IEEE 802.3ah/UDLD 772
45.1.38 CFM 772
45.1.39 LLDP 773

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.

Parameters

Describes in detail the parameters that can be set by the command. For details on the behavior of a command when all omissible parameters are omitted, see "Behavior when all parameters are omitted".

For details on the behavior when only a specific parameter is omitted, see "Behavior when this parameter is omitted". For details on the behavior when each parameter is omitted, see "Behavior when each parameter is omitted".

Example

Provides examples of appropriate command usage.

Display items

Describes the display items generated by the example.

The following table describes the Date display item displayed immediately after command execution in Example for each command.

Table 1-1: Display of the time when the command was received

Item	Displayed information
Date	yyyy/mm/dd hh:mm:ss timezone: year/month/day hour:minute:second time zone The item displays the time when the command was received.

The Switch assigns names to corresponding interfaces set by configuration. If <interface name> is shown in Display items, the Switch displays any of the interface names shown in the following table.

Table 1-2: List of interface names assigned by the command in each input format

Input format	Interface name <interface name>
interface gigabitethernet	geth1/0/1 The numeric values represent <switch no.>/<nif no.>/<port no.>.
interface tengigabitethernet	tengeth1/0/27 The numeric values represent <switch no.>/<nif no.>/<port no.>.
interface vlan <vlan id>	VLAN0002 The last four digits represent <vlan id>.
interface loopback 0	loopback0

Impact on communication

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

Notes

Provides cautionary information on using the command.

Specifiable values for parameters

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

Table 1-3: Specifiable values for parameters

Parameter type	Description	Input example
Name	For the names of access lists, 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. Note that if the command input format permits specification of either a name, or a command name and parameters (or keywords), and you specify a name that is identical to a command name or a parameter (or keyword), the system assumes that the command or the parameter (or keyword) has been entered.	ip access-list standard inbound1
MAC address, MAC address mask	Specify these items in hexadecimal format, separating 2-byte hexadecimal values by periods (.).	1234.5607.08ef 0000.00ff.ffff
IPv4 address, Subnet mask	Specify these items in decimal format, separating 1-byte decimal values by periods (.).	192.168.0.14 255.255.255.0
IPv6 address	Specify this item in hexadecimal format, separating 2-byte hexadecimal values by colons (:).	3ffe:501:811:ff03::87ff:fed0:c7e0 fe80::200:87ff:fe5a:13c7
IPv6 address with an interface name (for a link-local address only)	Specify a percent (%) between an IPv6 address and an interface name. Only link-local IPv6 addresses can be used as this parameter type.	fe80::200:87ff:fe5a:13c7%VLAN0001

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

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

Table 1-4: Ranges 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 1-5: Ranges of <switch no.>, <nif no.>, and <port no.> values (when a PoE port is specified)

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 <port list>

The <port list> parameter can accept multiple ports, with a hyphen (-), comma (,), or asterisk (*) in the <switch no.>/<nif no.>/<port no.> format. It can also accept one port, as when <switch no.>/<nif no.>/<port no.> is specified as the parameter input. The ranges of permitted values are the same as the ranges of <switch no.>, <nif no.>, and <port no.> values in the above tables.

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

1/0/1-3,5: A hyphen (-) cannot be specified in the switch number.

Example of a range specification that uses asterisks (*):

1/*/*: Specifies all ports on the device. Note that an asterisk (*) cannot be specified in the switch number.

■ Range of <channel group number>

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

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

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

■ How to specify <channel group list>

The <channel group list> parameter can accept multiple channel group numbers, separated by hyphens (-) and commas (,). You can also specify one channel group number. The range of permitted values is all the channel group numbers set by the configuration command.

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

1-3,5,10

■ Range of <vlan id>

The range of values the <vlan id> parameter accepts is from 1 to 4094.

■ How to specify <vlan id list>

The <vlan id list> parameter can accept multiple VLAN IDs, separated by hyphens (-) and commas (,). You can also specify one VLAN ID. The range of permitted values is VLAN ID=1 (VLAN ID for the default VLAN) and other VLAN IDs set by the configuration command.

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

1-3,5,10

■ How to specify an interface

The following table shows how to specify <interface type> and <interface number> parameters applicable to the interface type group in the leftmost column.

Table 1-7: How to specify an interface

Interface type group	Interface name specified for <interface type>	Interface number to be specified for <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

The following table shows the ports corresponding to the <interface type> parameter of an Ethernet interface.

Table 1-8: Ports corresponding to <interface type> of an Ethernet interface

<interface type> of an Ethernet interface	Ports corresponding to the <interface type> value
gigabitethernet	• 10BASE-T/100BASE-TX/1000BASE-T port • 100BASE-TX/1000BASE-T/2.5GBASE-T port • SFP port
tengigabitethernet	• SFP+/SFP shared port

List of character codes

Character codes are listed in the following table.

Table 1-9: List of character codes

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

Note

To enter a question mark (? or 0x3F), press Ctrl + V, and then type a question mark.

Error messages displayed by the entry-error location detection function

The following table lists and describes error messages output by the entry-error location detection function. (See "Configuration Guide Vol. 1, 5.2.3 Entry-error location detection function".)

Table 1-10: List of error messages output by the entry-error location detection function

No.	Message	Description	Occurrence condition
1	% illegal parameter at '^' marker	An invalid command or parameter is entered at '^'.	When an unsupported command or parameter is entered
2	% too long at '^' marker	A parameter entered at '^' exceeds the limit for the number of digits.	When a parameter that exceeds the limit for the number of digits is entered
3	% Incomplete command at '^' marker	Some parameters are missing.	When some parameters are missing
4	% illegal option at '^' marker	An invalid option is entered at '^'.	When an invalid option is entered
5	% illegal value at '^' marker	An invalid numeric value is entered at '^'.	When an invalid numeric value is entered
6	% illegal name at '^' marker	An invalid name is entered at '^'.	When an invalid name is entered
7	% out of range '^' marker	A numeric value entered at '^' is out of the valid range.	When a numeric value that is out of the valid range is entered
8	% illegal IP address format at '^' marker	An invalid IPv4 address or IPv6 address is entered at '^'.	When the input format of the IPv4 address or IPv6 address is invalid
9	% illegal combination or already appeared at '^' marker	A parameter entered at '^' has already been entered.	When a parameter that has already been entered is re-entered
10	% illegal format at'^' marker	A parameter entered at '^' is an invalid format.	When the input format of the parameter is invalid
11	% Permission denied	This command cannot be executed in user mode.	When a command that can be executed only in administrator mode is executed in user mode.
12	% internal program error	A program is faulty. Contact maintenance personnel.	When an invalid action other than described above occurs
13	% Command not authorized.	The executed command is not authorized.	When the executed command is not authorized by the RADIUS/TACACS+ server via RADIUS/TACACS+ command authorization function
14	% illegal parameter at '<word>' word	An invalid character '<word>' is entered. <word>: Invalid word	When '<word>' is entered at positions where a character cannot be entered
15	% illegal switch number at '^' marker	An invalid switch number is entered at '^'.	When an invalid switch number is entered

No.	Message	Description	Occurrence condition
16	% list entry over at '^' marker	The number of entries that exceeds the maximum number is specified for the list at '^'.	When the number of specified entries exceeds the maximum number of them that can be specified for the list

2 Switching the Command Input Mode

enable

Changes the command input mode from user mode to administrator mode. In administrator mode, you can execute commands, such as the "configure" command, which cannot be entered in user mode.

Syntax

```
enable
```

Input mode

User mode

Parameters

None

Example

Figure 2-1: Changing the command input mode from user mode to administrator mode

```
> enable
Password:******
#
```

If password authentication is successful, the administrator mode prompt (#) is displayed.

Display items

None

Impact on communication

None

Notes

Initially, no password is set. To ensure better security, we recommend that you use the "password" command to set the password.

disable

Changes the command input mode from administrator mode to user mode.

Syntax

```
disable
```

Input mode

Administrator mode

Parameters

None

Example

Figure 2-2: Changing the command input mode from administrator mode to user mode

```
#  disable
>
```

Display items

None

Impact on communication

None

Notes

None

quit

Ends the current command input mode as follows:

1. If you are in user mode, you are logged out.
2. If you are in administrator mode, the current mode ends, and you are returned to user mode. (The "disable" command can also be used.)

For details about how the command works in configuration command mode, see "Configuration Command Reference".

Syntax

```
quit
```

Input mode

User mode, administrator mode, and configuration command mode

Parameters

None

Example

Figure 2-3: Exiting administrator mode and returning to user mode

```
# quit
>
```

Display items

None

Impact on communication

None

Notes

None

exit

Ends user mode or administrator mode and logs out from the device.

For details about how the command works in configuration command mode, see "Configuration Command Reference".

Syntax

```
exit
```

Input mode

User mode, administrator mode, and configuration command mode

Parameters

None

Example

Figure 2-4: Exiting administrator mode and logging out from the device

```
# exit
```

Display items

None

Impact on communication

None

Notes

Use the "disable" command to return the command input mode from administrator mode to user mode.

logout

Logs out from the device.

Syntax

```
logout
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 2-5: Exiting the administrator mode and logging out from the device

```
# logout
login:
```

Display items

None

Impact on communication

None

Notes

None

configure(configure terminal)

Changes the command input mode from administrator mode to configuration command mode, and starts configuration editing.

Syntax

```
configure [terminal]
```

Input mode

Administrator mode

Parameters

terminal

Enables editing of the running configuration stored in memory.

Example

Figure 2-6: Changing the command input mode to configuration command mode

```
# configure
(config)#
```

Display items

None

Impact on communication

None

Notes

1. The device starts operation based on the settings in the startup configuration file that is read into memory at power up. The running configuration stored in memory is the file subject to editing. Note that if you do not save the settings to the startup configuration file after editing the running configuration stored in memory, the configuration settings will be lost when the device is restarted. We recommend that you execute the "save" configuration command to save the settings in the startup configuration file after the editing.
2. By using the "status" configuration command, you can check the status of the configuration being edited.
3. Do not interrupt the "configure" command by pressing Ctrl + C before the command processing finishes. If you do so, the "copy" command might result in an error.

   If the error occurs, use this command to switch to configuration command mode, and then use the "end" configuration command to end the configuration command mode. If the user who interrupted the processing has logged out, use the "show logging" command to check the user's tty name, and then log in with that tty name. After that, use this command to switch to configuration command mode, and then use the "end" configuration command to end the configuration command mode.

3 Operation Terminals and Remote Operations

set exec-timeout

Sets the idle time (in minutes) for auto-logout (see "Configuration Guide Vol. 1, 4.3 (3) Auto-logout"). This setting can be configured for each user.

Syntax

```
set exec-timeout <minutes>
```

Input mode

User mode and administrator mode

Parameters

<minutes>

This parameter specifies the idle time for auto-logout in minutes. The specifiable values are from 0 to 60.

If 0 is specified, auto-logout does not apply. The default upon initial installation is 60 minutes.

Example

Figure 3-1: Setting the auto-logout value to 30 minutes

```
> set exec-timeout 30
```

Display items

None

Impact on communication

None

Notes

- This command temporarily affects the target session only and is disabled when you log out. If you want to enable the setting at all times, use the "username" configuration command with the exec-timeout parameter specified.

set terminal help

Selects the type of command help messages to be displayed. This setting can be configured for each user.

Syntax

```
set terminal help { all | no-utility }
```

Input mode

User mode and administrator mode

Parameters

all

Enables help messages for all permissible operation commands to be displayed. This setting is the default for initial installation.

no-utility

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

Example

Figure 3-2: Enabling help messages for all permissible operation commands to be displayed

```
> set terminal help all
```

Figure 3-3: Enabling help messages for all operation commands, except for utility commands and file operation commands, to be displayed

```
> set terminal help no-utility
```

Display items

None

Impact on communication

None

Notes

- This command temporarily affects the target session only and is disabled when you log out. If you want to enable the setting at all times, use the "username" configuration command with the terminal-help parameter specified.

set terminal pager

Specifies whether to perform paging (see "Configuration Guide Vol. 1, 5.2.8 Paging"). This setting can be configured for each user.

Syntax

```
set terminal pager [{ enable | disable }]
```

Input mode

User mode and administrator mode

Parameters

{ enable | disable }

enable

Paging is performed. This setting is the default for initial installation.

disable

Paging is not performed.

Behavior when this parameter is omitted:

Paging is performed.

Example

Figure 3-4: No paging

```
> set terminal pager disable
```

Figure 3-5: Paging

```
> set terminal pager enable
```

Display items

None

Impact on communication

None

Notes

- This command temporarily affects the target session only and is disabled when you log out. If you want to enable the setting at all times, use the "username" configuration command with the terminal-pager parameter specified.

show history

Displays the history of operation commands executed in the past. When this command is executed in user mode or administrator mode, the history of configuration commands is not displayed.

When this command is prefixed with a dollar sign ($) and executed in configuration command mode, the history of configuration commands is displayed.

Syntax

```
show history
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following is an example of executing the "show history" command:

```
>  show history
    1 show system
    2 show interfaces
    3 show logging
    4 show history
>
```

Display items

None

Impact on communication

None

Notes

None

telnet

Connects via Telnet to the remote operation terminal that has the specified IP address.

Syntax

```
telnet <host> [{/ipv4 | /ipv6}] [/source-interface <source address>] [<port>]
```

Input mode

User mode and administrator mode

Parameters

<host>

Specifies the destination host name or IP address. An IPv4 address, IPv6 address, or IPv6 address with an interface name (only a link-local address) can be specified as the IP address.

{/ipv4 | /ipv6}

/ipv4

Establishes a connection via IPv4 only.

/ipv6

Establishes a connection via IPv6 only.

Behavior when this parameter is omitted:

A connection is established via IPv4 or IPv6.

/source-interface <source address>

Configures a source IP address connected via Telnet. An IPv4 or IPv6 address can be specified as an IP address.

Behavior when this parameter is omitted:

The source IP address selected by the Switch is used.

<port>

Specifies a port number.

Behavior when this parameter is omitted:

Port number 23 is used.

Behavior when all parameters are omitted:

A connection is established with specified <host>.

Example

1. Access the remote operation terminal whose IP address is 192.168.0.1 via Telnet.

   ```
   > telnet 192.168.0.1
   ```

   After the "telnet" command is executed, the following message indicating that you will need to wait for the connection with the remote operation terminal to be established is displayed.

   ```
   Trying 192.168.0.1 ...
   ```

   When the connection is established, the following messages are displayed. If the connection is not established within 30 seconds, it reverts to command input mode.

   ```
   Connected to 192.168.0.1
   ```

```
Escape character is '^]'.
```

2. After the connection is established, you can enter the login name and password.

```
login: username
Password: ********
```

3. Access the remote operation terminal whose IPv6 address is 3ffe:1:100::250 via Telnet.

```
> telnet 3ffe:1:100::250
Trying 3ffe:1:100::250...
```

Display items

None

Impact on communication

None

Notes

1. To interrupt the processing while Trying... is displayed, press the Ctrl + C keys.
2. After a connection is established, to halt execution of this command while the login prompt is displayed, press the Ctrl + D keys.
3. This command sends the input key codes to the login destination remote device without making any modifications. Therefore, the key code output by the terminal on which this command is entered must be the same as the key code required by the login destination terminal. If they are different, the command will not work correctly. For example, as the input key code for the carriage return control code (the Enter key), some terminals generate 0x0D or 0x0D0A, whereas other terminals need to receive 0x0D or 0x0A to recognize a carriage return control code from the login destination terminal. Check key code compatibility beforehand.
4. When the escape character ^] (Ctrl +] keys) is entered while a connection is being established, the mode switches to telnet> mode. In this mode, entering quit ends the "telnet" command (if a connection is established, it is closed). To exit from telnet> mode, enter just a line feed without any other character.
5. When, for example, character strings are being displayed on the screen with a connection established to another device from the Switch, pressing the Ctrl + C keys to interrupt the process can lead to the system not functioning correctly. In that case, enter the escape character ^] (Ctrl+]) and then enter quit to terminate the "telnet" command and then connect remotely again.

ftp

Transfers files between the Switch and a remote operation terminal connected via TCP/IP.

Syntax

```
ftp [<host> [{/ipv4 | /ipv6}] [/source-interface <source address>]]
```

Input mode

User mode and administrator mode

Parameters

<host>

Specifies a remote operation terminal. A host name, IPv4 address, IPv6 address, or IPv6 address with an interface name (only a link-local address) can be specified.

Behavior when this parameter is omitted:

The ftp prompt is displayed. In this state, a connection to the remote operation terminal has not been established. Use the "open" command to establish the connection.

{/ipv4 | /ipv6}

/ipv4

Establishes a connection via IPv4 only.

/ipv6

Establishes a connection via IPv6 only.

Behavior when this parameter is omitted:

A connection is established via IPv4 or IPv6.

/source-interface <source address>

Configures the source IP address used for connection via FTP. An IPv4 or IPv6 address can be specified as an IP address.

Behavior when this parameter is omitted:

The source IP address selected by the Switch is used.

Behavior when all parameters are omitted:

The ftp prompt is displayed. In this state, a connection to the remote operation terminal has not been established. Use the "open" command to establish the connection.

Example

Log in to the remote operation terminal whose IP address is 192.168.0.1:

```
> ftp 192.168.0.1
```

After the "ftp" command is executed, wait for the connection to the remote operation terminal to be established. When the connection is established, the input prompt (see steps 1 and 2 below) is displayed. If a connection is not established, the state is changed to ready for command input.

1. Entering the login name:

   The following prompt is displayed on the command line. Enter the login name for the remote operation terminal, and then press the Enter key:

```
Name:
```

2. Entering the password:

   The following prompt is displayed on the command line. Enter the password for the specified login name, and then press the Enter key:

   ```
   Password:
   ```

3. Entering a file transfer command:

   The following prompt is displayed on the command line.

   ```
   ftp>
   ```

   Enter a file transfer command according to the transfer direction, and then press the Enter key.

   The input format of the file transfer commands is as follows:

   get <remote-file> [<local-file>]

   Transfers a file from the remote operation terminal to the Switch. If <local-file> is omitted, the file name becomes the name of the file on the remote operation terminal.

   mget <remote-files>

   Use this command to receive multiple files. Enter the command in the format mget *.txt.

   put <local-file> [<remote-file>]

   Transfers a file from the Switch to the remote operation terminal. If <remote-file> is omitted, the file name becomes the name of the file on the Switch.

   mput <local-files>

   Use this command to send multiple files. Enter the command in the format mput *.txt.

4. Entering a command other than a file transfer command:

   If the prompt "ftp>" is displayed, the following commands can be executed in addition to the "get" and "put" commands:

   ascii

   Sets ASCII as the transfer format of the file.

   binary

   Sets binary as the transfer format of the file.

   [bye | quit | exit]

   Ends the FTP session, and then the "ftp" command.

   cd <remote-directory>

   Changes the current directory on the remote operation terminal to <remote-directory>.

   cdup

   Changes the current directory on the remote operation terminal to the next higher level.

   chmod <mode> <remote-file>

   Changes the attribute of the file specified by <remote-file> on the remote operation terminal to the attribute specified for <mode>.

   close

   Ends the FTP session, and then displays the prompt "ftp>" waiting for command input.

   debug

   Enables (on) or disables (off) the use of debug output mode. The default is off.

   delete <remote-file>

   Deletes <remote-file> on the remote operation terminal.

hash

Enables (on) or disables (off) the use of hash display ("#" is displayed every 1024 bytes) during data transfer. The default is off.

{help | ?} [<command>]

Displays Help for the command specified by the argument <command>. If no argument is specified, a list of available commands is displayed.

lcd [<directory>]

Changes the current directory on the Switch. If <directory> is omitted, the current directory moves to the home directory for the user.

lols [<local-directory>]

Lists the contents of <local-directory> (current directory if <local-directory> is not specified) of the Switch.

[lopwd | lpwd]

Displays the current directory of the Switch.

lpage <local-file>

Displays the contents of <local-file> on the Switch.

ls [<remote-directory>] [<local-file>]

Lists the contents of <remote-directory> (current directory if <remote-directory> is not specified) on the remote operation terminal. If <local-file> is specified, the contents to be displayed are stored in the file.

mdelete [<remote-files>]

Deletes <remote-files> on the remote operation terminal.

mkdir <directory-name>

Creates a directory on the remote operation terminal.

more [<remote-file> | page <remote-file>]

Displays the contents of <remote-files> on the remote operation terminal.

open <host> [<port>]

Establishes a connection to the FTP server with the specified address. When a port number (optional) is specified, the "ftp" command tries to connect to the FTP server on the specified port.

passive

Enables (on) or disables (off) the use of passive transfer mode. The default is off.

progress

Enables (on) or disables (off) the use of a transmission progress display bar. The default is on.

prompt

Enables (on) or disables (off) the use of interactive mode prompt. When you transfer multiple files, if this prompt is enabled (on), the files can be selected separately. If the prompt is off, the specified files are transferred unconditionally by the "mget" or "mput" command, and they are deleted unconditionally by the "mdelete" command. The default is on.

pwd

Displays the current directory on the remote operation terminal.

rename <from-name> <to-name>

Changes the name of a file on the remote operation terminal from <from-name> to <to-name>.

rmdir <directory-name>

Deletes a directory on the remote operation terminal.

status

Displays the current FTP status.

verbose

Enables (on) or disables (off) the use of redundant output mode. If redundant output mode is on, all responses from the FTP server are displayed for the user. In addition, when file transfer is completed, the statistics of the data transfer are displayed. The default is on.

Display items

None

Impact on communication

None

Notes

1. With a user ID whose password is not set on the login destination terminal, you might not be able to log in via FTP. If this occurs, set the password on the login destination terminal, and then execute the "ftp" command again.
2. If commands cannot be entered, enter the Ctrl + Z keys to exit.
3. When commands are executed from the Switch to an IPv4 host after login through FTP, a message "500 'EPRT |1|xx.xx.xx.xx|xxxx|':command not found (xx.xx.xx.xx|xxxx represents IPv4 address|port number of the Switch)" might be displayed; however, the commands still work correctly.

tftp

Transfers files between the Switch and a connected remote operation terminal by using UDP. This function is used for transferring update files to TFTP servers that support TFTP Option Extension (RFC 2347, 2348, and 2349).

Syntax

```
tftp [<host> [{/ipv4 | /ipv6}] [/source-interface <source address>] [<port>]]
```

Input mode

User mode and administrator mode

Parameters

<host>

Specifies a remote operation terminal. A host name, IPv4 address, IPv6 address, or IPv6 address with an interface name (only a link-local address) can be specified.

Behavior when this parameter is omitted:

The tftp prompt is displayed. In this state, a remote operation terminal has not been specified. Use the "connect" command to specify a remote operation terminal.

{/ipv4 | /ipv6}

/ipv4

Establishes a connection via IPv4 only.

/ipv6

Establishes a connection via IPv6 only.

Behavior when this parameter is omitted:

A connection is established via IPv4 or IPv6.

/source-interface <source address>

Configures the source IP address used for connection via TFTP. An IPv4 or IPv6 address can be specified.

Behavior when this parameter is omitted:

The source IP address selected by the Switch is used.

<port>

Specifies the port number of the connection destination.

Behavior when this parameter is omitted:

Port number 69 is used.

Behavior when all parameters are omitted:

The tftp prompt is displayed. In this state, a connection to the remote operation terminal has not been established. Use the "connect" command to establish the connection.

Example

Files are sent to and received from the remote operation terminal whose IP address is 192.168.0.1:

```
> tftp 192.168.0.1
```

After the "tftp" command is executed, communication with the remote operation terminal is not actually started, and the tftp prompt is displayed. Even if the specified connection destination has a problem, an error is output, and then the tftp prompt is displayed. In this case, use the "connect" command to reset the connection destination, or use the "quit" command to end the "tftp" command.

1. Entering a file transfer command:

   The following prompt is displayed on the command line.

   ```
   tftp>
   ```

   Enter a file transfer command according to the transfer direction, and then press the Enter key.

   The input format of the file transfer commands is as follows:

   get <remote-file> [<local-file>]

   Transfers a file from the remote operation terminal to the Switch. If <local-file> is omitted, the file name becomes the name of the file on the remote operation terminal.

   put <local-file> [<remote-file>]

   Transfers a file from the Switch to the remote operation terminal. If <remote-file> is omitted, the file name becomes the name of the file on the Switch.

2. Entering a command other than a file transfer command:

   If the prompt "tftp>" is displayed, the following commands can be executed in addition to the "get" and "put" commands:

   connect <host> [port]

   Connects to the TFTP server with the specified address. The port number of the connection destination can also be specified.

   mode

   Checks the current file transfer format.

   quit

   Ends the "tftp" command.

   trace

   Enables (on) or disables (off) the use of trace output mode. If the trace output mode is on, traces of packets transferred to the TFTP server are displayed. The default is off.

   status

   Displays statuses such as file transfer format, connection destination, and timeout.

   binary

   Sets binary (octet) as the file transfer format (default).

   ascii

   Sets ascii (netascii) as the file transfer format.

   blksize [<size>]

   Specifies the block size (the value of TFTP Blocksize Option in RFC 2348).

   You can specify a value of 8 to 65464 for <size>. The default is 8192. If you omit <size>, you can enter the parameter interactively.

   ? [<command>]

   Displays Help for the command specified by the argument <command>. If no argument is specified, a list of available commands is displayed.

Display items

None

Impact on communication

None

Notes

- Immediately after executing the "tftp" command or specifying the connection destination by using the "connect" command in tftp> mode, no communication is actually performed except that the address of the connection destination server is obtained. When the "get/put" command is specified in tftp> mode, communication is started. Communication errors such as no route are also output at this time.
- If proper permissions for accessing or writing data are not configured on the TFTP server, errors such as Access violation are output, and transfer fails.
- If commands cannot be entered, enter the Ctrl + Z keys to exit.
- Use TFTP servers that support TFTP Option Extension (RFC 2347, 2348, and 2349) for a connection destination. TFTP (RFC 1350) servers that do not support TFTP Option Extension cannot accept large files such as an update file, resulting in an error (Transfer timed out.) normally.

4 Configurations and File Operations

show running-config(show configuration)

Displays the running configuration.

Syntax

```
show running-config
show configuration
```

Input mode

Administrator mode

Parameters

None

Example and display items

None

Impact on communication

None

Notes

1. If there are many items in the running configuration, command execution might take some time.
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.

show startup-config

Displays the startup configuration used at device startup.

Syntax

```
show startup-config
```

Input mode

Administrator mode

Parameters

None

Example and display items

None

Impact on communication

None

Notes

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

copy

Copies a configuration.

Syntax

```
copy <source file> <target file> [debug]
```

Input mode

Administrator mode

Parameters

<source file>

Specifies the copy-source configuration file or configuration.

<source file> can be specified in the following formats:

<file name>

- Specifying a local configuration file

  Specify the name of the file stored in the device.
- Specify a remotely-stored configuration file.

  The following URL formats can be specified:
  - FTP

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

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

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

  <user name>: User name on the remote server

  <password>: Password for the remote server

  <host>: Specifies the name or IP address of the remote server

  To use an IPv6 address, it needs to be enclosed in [ ] parentheses.

  (Example) [2001:db8::10]

  <port>: Specifies a port number.

  <file path>: Specifies the path to the file on the remote server.

  If <user name> and <password> are omitted when ftp or http is specified, anonymous login is performed. If <password> is omitted, a prompt is displayed requesting the password.

running-config: Running configuration

startup-config: Startup configuration file

<target file>

Specifies the copy-destination configuration file or configuration.

<file name> and startup-config can be specified. However, the same format as that specified for <source file> cannot be specified for <target file> (For example, for a file-to-file copy, copy <file name> <file name> cannot be specified).

Also, HTTP specification for <target file> is not supported.

Note that running-config cannot be specified.

debug

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

When the error "Data transfer failed." occurs while accessing a remote file, if you re-execute the command with this debug parameter specified, then you can see details about the error, such as server responses.

Behavior when this parameter is omitted:

The details about communication status are not displayed.

Example

- Copies the running configuration to the startup configuration.

```
# copy running-config startup-config
  Configuration file copy to startup-config?(y/n):y
```

- Saves the running configuration to a file on a remote server.

```
# copy running-config ftp://staff@192.168.10.10/backup.cnf
  Configuration file copy to ftp://staff@192.168.10.10/backup.cnf?
  (y/n): y

  Authentication for 192.168.10.10.
  User: staff
  Password: xxx (Enter the password stored on the remote server for the user account "staff".)
  transferring

  Data transfer succeeded.
#
```

Display items

None

Impact on communication

None

Notes

1. You cannot copy to a running configuration that is being edited. Execute the "copy" command after the edit is completed.
2. Editing the startup configuration has no effect on the running configuration or communication.
3. If you do not have writing permission for the save destination file, your edits cannot be saved to the file. To save edits to a file on a remote server, change the settings to allow you to write on the remote server.
4. If you copy a configuration file created using an editor or a different device model, the device performance may become unstable even if the "copy" command completes normally. Before copying, confirm that the configuration file contents and interface definitions to be applied are appropriate for the capacity limit of the device and that there is sufficient space for the new configuration file. If you perform a copy by mistake, execute the "erase startup-config" command, restart the device to reset the configuration, and then edit the configuration again.
5. If there is insufficient free space for storing files, a configuration cannot be copied. Use the "show mc" command to check the free space in the user area. The necessary space required for copying a configuration is the total size of the new configuration in the copy source and the existing configuration in the copy destination. About 2 MB of free capacity is required for a maximum-size configuration file.

6. When you use the URL format, we recommend that you omit <password> when executing the command. The executed command is recorded in operation logs, and might be referenced by other users. To ensure security, we recommend that you omit <password> and enter the password on the prompt.
7. In the URL notation, a single "/" located between the <host> specification and the <filepath> specification is not included as a path component. For example, to specify /usr/home/staff/a.cnf on the FTP remote server, specify ftp://<host>//usr/home/staff/a.cnf.
8. When the copy source is a running configuration, and the copy destination is a startup configuration, the same processing as that for the "save" command is performed.
9. In memory card operation mode, when startup configuration is specified as a copy destination to execute this command, the "update mc-configuration" command is also executed automatically. Therefore, the operation log of the "update mc-configuration" command is collected. For details about the operation log, see "Message Log Reference". Note that even if an error is detected in the "update mc-configuration" command, this command is processed successfully.

erase startup-config

Resets the startup configuration file to the defaults. If you want to reset the running configuration to the defaults, execute this command and then restart the device without saving the running configuration.

Syntax

```
erase startup-config
```

Input mode

Administrator mode

Parameters

None

Example

```
# erase startup-config
Do you wish to erase startup-config? (y/n): y
!#
```

Display items

None

Impact on communication

None

Notes

1. After you execute this command and restart the device, the running configuration will reset to the defaults. Note that you will not be able to log in to the Switch via a network after the restart.
2. This command cannot be used while the configuration is being edited. Exit the configuration command mode.

show file

Shows the contents and line numbers of a local or remote server file. For connection via FTP, specify a directory with "/" appended to the file path to get and display the directory list.

Syntax

```
show file <file name> [debug]
```

Input mode

User mode and administrator mode

Parameters

<file name>

Specifies the following items as file names to be displayed.

- Local file specification
  Specify the name of the file stored in the device.
- Remote file specification
  Specifies the following types of URLs:
  - FTP
    ftp://[<user name>[:<password>]@]<host>[:<port>]/<filepath>
  - TFTP
    tftp://<host>[:<port>]/<filepath>
  - HTTP
    http://[<user name>[:<password>]@]<host>[:<port>]/[<filepath>]

  <user name>: User name on the remote server

  <password>: Password for the remote server

  <host>: Specifies the name or IP address of the remote server

  To use an IPv6 address, it needs to be enclosed in [ ] parentheses.

  (Example) [2001:db8::10]

  <port>: Specifies a port number.

  <filepath>: Specifies the path to the file on the remote server.

  If <user name> and <password> are omitted when ftp or http is specified, anonymous login is performed. If <password> is omitted, a prompt is displayed requesting the password.

debug

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

When the error "Data transfer failed." occurs when accessing a remote file, if you re-execute the command with this debug parameter specified, then you can see details about the error, such as server responses.

Behavior when this parameter is omitted:

The details about communication status are not displayed.

Example

- Shows the information of a file on the remote server.

```
> show file ftp://staff@192.168.10.10/backup.cnf
```

```
Date 20XX/01/20 12:00:00 UTC

Authentication for 192.168.10.10.
User: staff
Password: xxx (Enter the password stored on the remote server for the user account "staff".)
transferring…

interface gigabitethernet 0/1
  switchport mode access
!

### Total 3 lines.
>
```

- Show the information of a directory on a remote server.

```
> show file ftp://staff@192.168.10.10//usr/home/staff/
Date 20XX/01/20 12:00:00 UTC

Authentication for 192.168.10.10.
User: staff
Password: xxx (Enter the password stored on the remote server for the user account "staff".)
transferring...

### List of remote directory.
total 9
-rw-------  1 staff user   34 Dec  8 11:31 .clihihistory
-rw-------  1 staff user  408 Dec  8 12:32 .clihistory
-rw-------  1 staff user    0 Dec  8 12:32 .history
-rw-r--r--  1 staff user  109 Dec  8 10:02 .login
-rw-r--r--  1 staff user  268 Dec  8 10:02 .tcshrc
-rw-r--r--  1 staff user   34 Dec 12 12:62 backup.cnf
>
```

Display items

None

Impact on communication

None

Notes

1. Specify ASCII text files as the files to be displayed. Do not specify files that cannot be displayed by terminals, such as binary-format files. If such files are specified, the display might be distorted or display invalid characters. In this case, log in to the Switch again, or reset the terminal.

   For HTTP transfers, such files might be discarded part way through the transfer, the transfer might result in the error "Data transfer failed.", and download might not be performed.
2. When you use the URL format with <file name>, we recommend that you omit the <password> when executing the command. The executed command is recorded in operation logs, and they might be checked by other users. To ensure security, we recommend that you omit <password> and enter the password on the prompt.
3. For access via FTP, specify a directory with "/" appended to the file path to get and display the directory list.
4. In the URL notation, a single "/" located between the <host> specification and the <filepath> specification is not included as a path component. For example, to specify /usr/home/staff/a.cnf on the FTP remote server, specify ftp://<host>//usr/home/staff/a.cnf.

cd

Changes the directory.

Syntax

```
cd [<directory>]
```

Input mode

User mode and administrator mode

Parameters

<directory>

Specifies the name of the destination directory.

Behavior when this parameter is omitted:

Moves to the home directory of the current login user.

Example and display items

None

Impact on communication

None

Notes

None

pwd

Shows the path to the current directory.

Syntax

```
pwd
```

Input mode

User mode and administrator mode

Parameters

None

Example and display items

None

Impact on communication

None

Notes

None

ls

Shows the files and directories that exist in the current directory.

Syntax

```
ls [<option>] [<names>]
ls mc-dir
```

Input mode

User mode and administrator mode

Parameters

<option>

-a: Shows all contents of the current directory, including hidden files.

-l: Shows detailed information related to files and directories.

Behavior when this parameter is omitted:

Hidden files and detailed information are not displayed.

<names>

Specifies a file name or directory name.

Behavior when this parameter is omitted:

Shows a list of the contents of the current directory.

mc-dir

Shows the list of files on a memory card.

Example

Shows the list of files on a memory card.

```
>ls mc-dir
```

Display items

None

Impact on communication

None

Notes

1. The mc-dir parameter cannot be used when a memory card is not inserted.
2. If an error occurs when no memory card is installed, you may see "A:" instead of "C:".

dir

Lists deleted files that are recoverable on the internal flash memory of the Switch. If the /all, summary, or /deleted parameters is not specified, this command has almost the same functions as the "ls" command.

Syntax

```
dir /all [summary]
dir /deleted
```

Input mode

User mode and administrator mode

Parameters

/all

Shows a list of files on the current directory including detailed information. Files that have been deleted by the "delete" command are displayed with an index added. The file names of deleted files are displayed in parentheses [ ].

summary

Shows a list of files on the current directory. Files that have been deleted by the "delete" command are displayed with an index added. The file names of deleted files are displayed in parentheses [ ].

Behavior when this parameter is omitted:

Shows a list of files including detailed information.

/deleted

Shows all the deleted files on the specified internal flash memory with an index added to each. Deleted files are displayed with their full pathname. That full pathname is displayed in parentheses [ ].

Example

- Shows files in the current directory on internal flash memory, including deleted files.

  Figure 4-1: Displaying files when /all and summary are specified

```
> dir /all summary
Directory of ./:
userfile1               userfile2               userfile3
[userfile4]
>
```

- Show files in the current directory on internal flash memory with detailed information. An index number is added to each deleted file.

  Figure 4-2: Displaying files when only /all is specified

```
> dir /all
Directory of ./:
 - -rw-r--r-- user     user       123117 Jan 27 14:18 userfile1
 - -rw-r--r-- user     user          344 Jan 27 14:55 userfile2
 6 -rw-r--r-- user     user           16 Jan 27 17:57 [userfile3]
>
```

- Show deleted files in the current root on internal flash memory with detailed information and index number.

Figure 4-3: Displaying deleted files

```
> dir /deleted
Directory of /mc0:
 4 user2    user         5555 Jan 27 11:10 [/usr/home/user2/testfile]
 6 user1    user           16 Jan 27 17:57 [/usr/home/user1/usefile4]
>
```

Display items

Table 4-1: Display contents when the /all option is specified

Location (digit)	Item	Description
1 to 2	Index number	Indicates the index number of each deleted file (1 to 64).
4 to 13	File attribute	Each symbol has the following meaning: d: Directory attribute r: Read permission exists. w: Write permission exists. x: Execute permission exists. Each display location has the following meanings: +0th digit: Directory attribute +1st digit: Read permission for the owner +2nd digit: Write permission for the owner +3rd digit: Execute permission for the owner +4th digit: Read permission for the group +5th digit: Write permission for the group +6th digit: Execute permission for the group +7th digit: Read permission for the others +8th digit: Write permission for the others +9th digit: Execute permission for the others
15 to 22	Owner name	Indicates the owner name of a file.
24 to 31	Group name	Indicates the group name of a file.
33 to 40	File size	Indicates the file size in bytes.
42 to 51	File modification date	Indicates the file modification date.
53 and up	File name	Indicates the file name.

Table 4-2: Display contents when the /deleted option is specified

Location (digit)	Item	Description
1 to 2	Index number	Indicates the index number of each deleted file (1 to 64).
4 to 9	Owner name	Indicates the owner name of a file.
11 to 16	Group name	Indicates the group name of a file.
18 to 25	File size	Indicates the file size in bytes.
27 to 38	File modification date	Indicates the file modification date.
40 and up	Deleted file name	Indicates the deleted file name.

Impact on communication

None

Notes

None

cat

Shows the contents of a specified file.

Syntax

```
cat [<option>] <file name>
```

Input mode

User mode and administrator mode

Parameters

<option>

-n: Shows the contents of a file with line numbers added.

Behavior when this parameter is omitted:

The contents of the specified file are shown without any modification.

<file name>

Specifies a file name to be displayed.

Example and display items

None

Impact on communication

None

Notes

None

cp

Copies a file.

Syntax

```
cp [<option>] <file name1> <file name2>
cp <file name1> mc-file <mc file name2>
   (Copies a file on the internal flash memory to a memory card.)
cp mc-file <mc file name1> <file name2>
   (Copies a file on a memory card to the internal flash memory.)
```

Input mode

User mode and administrator mode

Parameters

<option>

-r: Copies a directory.

-i: Displays confirmation prompts asking whether to permit overwriting if a file or directory exists in the copy destination.

Behavior when this parameter is omitted:

The specified file is copied without asking for confirmation of overwriting.

<file name1>

Specifies the copy-source file. Or, specifies the name of a file on the copy-source internal flash memory.

<file name2>

Specifies the copy destination file. Or, specifies the name of a file on the copy-destination internal flash memory.

mc-file <mc file name2>

Specifies the name of a file on the copy-destination memory card.

Alphanumeric characters, hyphens (-), underscores (_), and periods (.) can be used for a file name on a memory card. Note that names ending in a period (.) cannot be used.

The maximum number of characters that can be specified is 255 characters.

mc-file <mc file name1>

Specifies the name of a file on the copy-source memory card.

Wildcards cannot be used to specify file names on a memory card.

The maximum number of characters that can be specified is 255 characters.

Example

- Copies file1 from the internal flash memory to the memory card and name as file2.

  ```
  >cp file1 mc-file file2
  ```

- Copies file1 from the memory card to the internal flash memory and name as file2.

  ```
  >cp mc-file file1 file2
  ```

Display items

None

Impact on communication

When mc-file is specified, if the monitoring time or sending interval of the Layer 2 or Layer 3 protocol is set shorter than the initial value on neighboring devices, communication might be disconnected when the Layer 2 or Layer 3 protocol is disconnected.

Notes

1. The mc-file parameter cannot be used when a memory card is not inserted.
2. Accessing a memory card increases load on the device. Before specifying mc-file, if monitoring time and sending interval of a protocol, which are settings for maintaining connection with neighboring devices, are set shorter than the initial value, reset the monitoring time and sending interval to longer values.
3. If an error occurs when no memory card is installed, you may see "A:" or "a:" instead of "C:" or "c:".

mkdir

Creates a new directory.

Syntax

```
mkdir [<option>] <directory>
mkdir mc-dir <directory>
```

Input mode

User mode and administrator mode

Parameters

<option>

-p: Creates a directory as necessary when no parent directory exists.

Behavior when this parameter is omitted:

An error occurs when the parent directory does not exist (The parent directory is not created).

<directory>

Specifies the name of the directory to be created.

mc-dir <directory>

Creates a directory on a memory card.

Alphanumeric characters, hyphens (-), underscores (_), and periods (.) can be used for a directory name on a memory card. Note that names ending in a period (.) cannot be used.

The maximum number of characters that can be specified is 255 characters.

Example

Creates a new directory, newdir, on a memory card.

```
>mkdir mc-dir newdir
```

Display items

None

Impact on communication

None

Notes

1. The mc-dir parameter cannot be used when a memory card is not inserted. In addition, the parameter cannot be used with the -p option.
2. If an error occurs when no memory card is installed, you may see "A:" instead of "C:".

mv

Moves or renames a file.

Syntax

```
mv [<option>] <file name1> <file name2>
mv [<option>] <directory1> <directory2>
mv [<option>] <names> <dir>
```

Input mode

User mode and administrator mode

Parameters

<option>

-f

Forcibly performs a move without requesting confirmation.

Behavior when this parameter is omitted:

A confirmation message is displayed, and then a file is moved or renamed.

<file name1>

Specifies the name of a file to be moved (renamed).

<file name2>

Specifies the name of the file after moving or renaming.

<directory1>

Specifies the name of a directory to be moved (renamed).

<directory2>

Specifies the name of a directory after moving (renaming).

<names>

Indicates the names of one or more source files or directories.

<dir>

Indicates the name of the destination directory.

Example and display items

None

Impact on communication

None

Notes

None

rm

Deletes a specified file.

Syntax

```
rm [<option>] <file name>
rm mc-file <mc file name>
```

Input mode

User mode and administrator mode

Parameters

<option>

-r: Deletes all files in the specified directory and its subdirectories.

Behavior when this parameter is omitted:

Only the specified file is deleted.

<file name>

Specifies a file name or directory name to be deleted.

mc-file <mc file name>

Specifies the name of the file to be deleted from a memory card.

The maximum number of characters that can be specified is 255 characters.

Wildcards cannot be used to specify file names on a memory card.

Example

Deletes a file called file1 on the memory card.

```
>rm mc-file file1
```

Display items

None

Impact on communication

None

Notes

1. The mc-file parameter cannot be used when a memory card is not inserted. In addition, the parameter cannot be used with the -r option.
2. If file names or directory names include special characters, an error such as a command invalid error might occur. In this case, specify an asterisk wildcard (*) for <file name>, and individually confirm target files, to delete files named with special characters. Special characters are characters other than alphanumeric characters listed in "List of character codes" of "1. Reading the Manual".
3. If an error occurs when no memory card is installed, you may see "A:" instead of "C:".

rmdir

Deletes a specified directory.

Syntax

```
rmdir <directory>
rmdir mc-dir <directory>
```

Input mode

User mode and administrator mode

Parameters

<directory>

Specifies the name of the directory to be deleted.

mc-dir <directory>

Deletes a directory on the memory card.

Wildcards cannot be used to specify directory names on a memory card.

Example

Deletes a directory, deldir, on the memory card.

```
>rmdir mc-dir deldir
```

Display items

None

Impact on communication

None

Notes

1. The mc-dir parameter cannot be used when a memory card is not inserted.
2. If an error occurs when no memory card is installed, you may see "A:" instead of "C:".

delete

Deletes files on the internal flash memory used by the Switch in a recoverable way. Note that the maximum number of files that can be deleted is 64 files.

Syntax

```
delete <file name>
```

Input mode

User mode and administrator mode

Parameters

<file name>

Specifies the name of a file to be deleted.

Example

Deletes a file in a recoverable way.

Figure 4-4: Executing delete on a file

```
> delete userfile
>
```

Display items

None

Impact on communication

None

Notes

1. This command can operate only on files in internal flash memory. Files on RAM disk (memory) cannot be deleted.
2. If there is not enough free space on internal flash memory to store files in a recoverable way, this command cannot be used for deletion.
3. To recover files deleted by this command, use the "undelete" command.
4. To completely erase files deleted by this command, use the "squeeze" command.
5. To list files deleted by this command, use the "dir" command.

undelete

Recovers deleted files that are recoverable on the internal flash memory used by the Switch.

Syntax

```
undelete <index>
```

Input mode

User mode and administrator mode

Parameters

<index>

Specifies the index number of a file to be recovered. An index number is a unique number assigned to each deleted file and displayed when file lists are displayed using the "dir /all" command or "dir /deleted" command.

Example

Recovers files deleted by the "delete" command.

Figure 4-5: Recovering a file

```
> dir /all

Directory of ./:
 - -rw-r--r-- user     user       123117 Jan 27 14:18 userfile1
 - -rw-r--r-- user     user          344 Jan 27 14:55 userfile2
 - -rw-r--r-- user     user        22310 Jan 27 17:38 userfile3
 6 -rw-r--r-- user     user           16 Jan 27 17:57 [userfile4]
> undelete 6
>
```

Display items

None

Impact on communication

None

Notes

1. This command can operate only on internal flash memory files that have been deleted by the "delete" command. Files deleted by the "rm" command or other commands cannot be recovered.
2. If there is no directory in internal flash memory to store a file to be recovered, the file cannot be recovered.
3. To check the indexes of deleted files to be recovered by this command, use the "dir" command.
4. If files are completely erased by the "squeeze" command, they cannot be recovered by this command.
5. If the current root directory is not internal flash memory, this command will fail.

squeeze

Completely erases files on internal flash memory used by the Switch that have been deleted in a recoverable way by the "delete" command.

Syntax

```
squeeze
```

Input mode

User mode and administrator mode

Parameters

None

Example

Completely erases files deleted by the "delete" command.

Figure 4-6: Executing squeeze on files

```
> squeeze
All deleted files will be erased.
 (y/n)?:y
Squeezing...
Done
>
```

Display items

None

Impact on communication

None

Notes

1. This command can operate only on files in internal flash memory.
2. Files completely erased by this command cannot be recovered by the "undelete" command.

5 Login Security and RADIUS/ TACACS+

adduser

Adds an account for a new login user.

Syntax

```
adduser <user name> [no-flash]
```

Input mode

Administrator mode

Parameters

<user name>

Specifies a user name for a new account. The user name is 1 to 16 characters in length. For the user name, alphabetic characters can be used for the first character, and alphanumeric characters, hyphens (-), and underscores (_) can be used for the second and subsequent characters.

In addition, the following characters used within the device cannot be specified:

root, daemon, bin, sys, sync, nobody, systemd-timesync, systemd-bus-proxy, messagebus, remote_user, admin, and script

no-flash

Creates the home directory of a new account in memory, rather than internal flash memory.

Behavior when this parameter is omitted:

The home directory of a new account is created in internal flash memory.

Example

1. Add a new login user "user1".

   ```
   # adduser user1
   ```

   A new login user account with no password is added, and then the following message is output:

   ```
   User(empty password) add done. Please setting password.
   ```

2. Next, enter a password.

   ```
   Changing local password for newuser.
   New password:********
   ```

   If you press only the Enter key at this time, a new login user with no password is created.

3. Re-type the password for confirmation.

   ```
   Retype new password:********
   # quit
   >
   ```

Display items

None

Impact on communication

None

Notes

1. You cannot cancel the password setup process midway. Check the password settings before executing the command.
2. A login user name that has already been registered cannot be added. In addition, names such as root or admin cannot be used as a login user name because they are used inside the Switch.
3. We recommend that you use at least six characters for a password. If fewer than six characters are entered, an error is displayed. Note, however, that if you re-enter the same password, it will be accepted. Also, the maximum number of characters that can be used for a password is 128. If you enter 129 or more characters, only the first 128 characters are registered for the password.
   Specifiable characters are alphanumeric characters and special characters. For details, see "List of character codes". We recommend that you use upper-case alphabetic characters, numbers, and symbols in addition to lower-case alphabetic characters. If a password consists of only lower-case alphabetic characters, an error is displayed. Note, however, that if you re-enter the same password, it will be accepted.
4. If an account is added with the no-flash parameter specified, do not create any files under the home directory of the added account.
5. If you create an account with the "adduser" command and specify the no-flash parameter then configure settings using the "set exec-timeout", "set terminal help", or "set terminal pager" commands, they revert to the default settings, and logs of commands of the history function are cleared when the device is restarted.

rmuser

Deletes a user login account registered by the "adduser" command.

Syntax

```
rmuser <user name>
```

Input mode

Administrator mode

Parameters

<user name>

Specifies a login user name registered in the password file.

Example

1. Delete the user registration of the login user named "operator".
   ```
   # rmuser operator
   ```
2. If the specified login user name has been registered, a confirmation message is displayed as follows:
   ```
   Delete user 'operator'? (y/n): _
   ```
   If "y" is entered, the account is deleted.

   If "n" is entered, the user is returned to the command prompt without deleting the account.

Display items

None

Impact on communication

None

Notes

1. The account of the user executing this command cannot be deleted. For example, the account "operator" cannot be deleted by this command while the account user "operator" is logged in.
2. The default user ("operator") provided during the initial installation can be deleted.
3. If a user is deleted, the home directory of the user is also deleted. Therefore, before deleting a user, back up user files that need to be saved.
4. If the specified user is logged in, the user is forcibly logged out. Therefore, the deletion target user should be logged out by the "logout" command or "exit" command beforehand.

password

Changes the password of a login user. The command works differently depending on the command input mode as follows:

1. In user mode, only the password of the current login user can be changed.
2. In administrator mode, the password of all users and the password for enable mode can be changed.

Syntax

```
password [<user name>]
password enable-mode
```

Input mode

User mode and administrator mode

Parameters

<user name>

Specifies the login user name. In administrator mode, other users can also be specified for the login user name.

Behavior when this parameter is omitted:

The password of the current login user is changed.

enable-mode

In administrator mode, a password for enable mode can be set.

Example

- Change the password of the login user name operator.

```
# password operator
Changing local password for operator
New password:******** ... Enter a new password.
Retype new password:******** ... Re-enter the new password.
#
```

- Change the password of the current login user (with no parameters).

```
> password
Changing local password for xxxxxxx ... The login user name is displayed.
Old password:******** ... Enter the current password.
New password:******** ... Enter a new password.
Retype new password:******** ... Re-enter the new password.
>
```

Display items

None

Impact on communication

None

Notes

1. The password of other login users cannot be changed in modes other than administrator mode. When the password of other login users is changed, the prompt (Old password:) is not displayed. Start the procedure by entering the new password at the prompt (New password:).
2. You cannot cancel the password setup process midway. Check the password settings before executing the command.
3. We recommend that you use at least six characters for a password. If fewer than six characters are entered, an error is displayed. Note, however, that if you re-enter the same password, it will be accepted. Also, the maximum number of characters that can be used for a password is 128. If you enter 129 or more characters, only the first 128 characters are registered for the password.
   Specifiable characters are alphanumeric characters and special characters. For details, see "List of character codes". We recommend that you use upper-case alphabetic characters, numbers, and symbols in addition to lower-case alphabetic characters. If a password consists of only lower-case alphabetic characters, an error is displayed. Note, however, that if you re-enter the same password, it will be accepted.

clear password

Deletes the password of a login user. The command works differently depending on the command input mode as follows:

1. In user mode, only the password of the current login user can be deleted.
2. In administrator mode, the password of any users and the password for enable mode can be deleted.

Syntax

```
clear password [<user name>]
clear password enable-mode
```

Input mode

User mode and administrator mode

Parameters

<user name>

Specifies the login user name. In administrator mode, other users can also be specified for the login user name.

Behavior when this parameter is omitted:

The password of the current login user is cleared.

enable-mode

In administrator mode, a password for enable mode can be deleted.

Example

Clear the password of the current login user.

```
> clear password
Changing local password for xxxxxxx ... The login user name is displayed.
Old password:******** ... Enter the current password.
Password cleared.
>
```

Display items

None

Impact on communication

None

Notes

1. The password of other login users cannot be deleted in modes other than administrator mode.

show sessions (who)

Displays the users currently logged in to the Switch.

Syntax

```
show sessions
who
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 5-1: Displaying users currently logged in to the Switch

```
> show sessions
Date 20XX/06/16 12:00:00 UTC
operator console  -----  0   Jun 15 14:16                    <-1
operator pts/0    admin  2   Jun 15 14:16 (192.168.0.1)      <-2
operator pts/1    -----  3   Jun 15 14:17 (192.168.0.1)      <-3
staff    pts/2    -----  4   Jun 15 15:52 (192.168.0.1)      <-4
>
```

1. Login from CONSOLE
2. Login from a remote operation terminal (administrator mode)
3. Login from a remote operation terminal
4. Login from a remote operation terminal

Display items

The following information is displayed:

- Login user name
- tty name
- Command input mode: "admin" (administrator mode) or "-----" (user mode)
- Login number
- Date and time
- Terminal IP address (displayed only when the user has logged in from a remote operation terminal)

Impact on communication

None

Notes

1. The login number might be used to forcibly log out a login user.

show whoami (who am i)

Shows only the user, logged in to the Switch, who executed this command. If the command is restricted, the contents of the command list, class, and situation authenticated by TACACS+, RADIUS, and local password authentication are displayed on an extended display.

Syntax

```
show whoami
who am i
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 5-2: Displaying the login name of the current login user

```
> show whoami
Date 20XX/01/07 12:00:00 UTC
operator pts/0    -----  2   Jan  6 14:17 (192.168.0.1)
>
```

If command authorization is set by the TACACS+ server, RADIUS server, or local (configuration), an extended display appears, as follows.

- When staff1 is authenticated by a TACACS+ server

  The following result is displayed when nothing is set for the class, "show" is set in the authorized command list, and "enable, inactivate, reload, config, and show ip" are set in the rejected command list:

  ```
  > show whoami
  Date 20XX/01/07 12:00:00 UTC
  staff1 pts/0    -----  2   Jan  6 14:17 (192.168.0.1)

  Home-directory: /usr/home/staff1
  Authentication: TACACS+ (Server 10.10.10.10)
  Class: -----
  Command-list:
      Allow: "show"
      Deny : "enable,inactivate,reload,config,show ip"
  >
  ```

- When staff2 is authenticated by the RADIUS server

  The following result is displayed when nomanage is set for the class, and reload is set in the deny command list:

  ```
  > show whoami
  Date 20XX/01/07 12:00:00 UTC
  staff2 pts/0    -----  2   Jan  6 14:17 (192.168.0.1)

  Home-directory: /usr/home/remote_user
  Authentication: RADIUS (Server 10.10.10.10)
  Class: nomanage
      Allow: -----
      Deny : "adduser,rmuser,clear password,password,killuser"
  Command-list:
      Allow: -----
      Deny : "reload"
  >
  ```

- When staff3 is authenticated by local password authentication

  The following result is displayed when allcommand is set for the class, and no command list is set:

```
> show whoami
Date 20XX/01/07 12:00:00 UTC
staff3 pts/0    -----  2   Jan  6 14:17 (192.168.0.1)

Home-directory: /usr/home/staff3
Authentication: LOCAL
Class: allcommand
    Allow: "all"
    Deny : -----
Command-list: -----
>
```

Display items

Table 5-1: Information displayed by the show whoami command

Item		Displayed information
User information		Displays information about the user who executed the command. • Login user name • tty name • Command input mode: "admin" (administrator mode) or "**-----**" (user mode) • Login number • Date and time • Terminal IP address (displayed only when the user has logged in from a remote operation terminal)
Home-directory		Displays the home directory.
Authentication		Authentication type (RADIUS, TACACS+, or LOCAL) It displays the address authentication information of the remote authentication server only when the user is authenticated by RADIUS or TACACS+.
Authorization		Command authorization type (TACACS+ or LOCAL) If command authorization is set, this item is displayed instead of the Authentication item when this command is executed using the commandline module from a Python script. If command authorization is set by TACACS+, the address of the command authorization server is also displayed.
Class	Class	Displays a class name. If no class is set, ----- is displayed. If the invalid class name is set, a comment (Invalid Class) is displayed next to the class name. If the invalid class name includes characters that cannot be displayed such as non-ASCII characters, they are replaced by "." in the display.
	Allow	If a class is set, the contents of the authorized command list of the class are displayed. If the class is "root", there are no command restrictions. The message (Command unlimited) is displayed. If an authorized command list is not specified for the applicable class, ----- is displayed.
	Deny	If a class is set, the contents of the rejected command list of the class are displayed. If the class is "root", there are no command restrictions. The message (Command unlimited) is displayed. If a rejected command list is not specified for the applicable class, ----- is displayed.

Item		Displayed information
Command list	Command-list	If a command list is not specified, or the class is "root", ----- is displayed.
	Allow	If an authorized command list is set, the contents of the list are displayed. If the authorized command list is not set, ----- is displayed. If the command list includes characters that cannot be displayed such as non-ASCII characters, they are replaced by "." in the display.
	Deny	If a rejected command list is set, the contents of the list are displayed. If the rejected command list is not set, ----- is displayed. If the command list includes characters that cannot be displayed such as non-ASCII characters, they are replaced by "." in the display.

Impact on communication

None

Notes

1. The login number might be used to forcibly log out a login user.
2. If the class name or command list includes characters that cannot be displayed such as non-ASCII characters, they are replaced by "." in the display.

killuser

Forcibly logs out a login user.

Syntax

```
killuser <login no.>
```

Input mode

User mode and administrator mode

Parameters

<login no.>

Specifies the login number of the forced logout target. The login number can be checked by the "show sessions" command.

Example

Use the "show sessions" command to check the login number of a user you want to get logged out. Execute this command with the login number specified.

Figure 5-3: Executing the command with the user's login number specified

```
> show sessions
Date 20XX/01/07 12:00:00 UTC
operator console  -----  0   Jan  6 14:16               <-1
staff    pts/0    admin  2   Jan  6 14:16 (192.168.0.1) <-2
staff    pts/1    -----  3   Jan  6 14:17 (192.168.0.1) <-3
operator pts/2    -----  4   Jan  6 14:20 (localhost)   <-4
>
> killuser 2                                            <-5
```

1. Login number 0
2. Login number 2
3. Login number 3
4. Login number 4
5. The user who is executing the command, staff (login number 3), specified login number 2 to force this user to log out.

Display items

None

Impact on communication

None

Notes

1. This command is prepared for forcibly logging out a login user who remains logged in due to a network failure or terminal failure occurring while the user is logged in. Use the "logout" command or "exit" command for normal logout. Do not use this command except in an emergency. Even if a user remains logged in, the user will eventually be logged out by the auto-logout function.

2. The user who is executing this command cannot specify himself as the forced logout target. If such a user is specified as described above, an error occurs. However, a user can specify himself as logout target when logged in from the console.
3. Only users who have the same account as the user who is executing this command can be forcibly logged out by using this command and specifying the applicable login number. In the above example 1, "staff" with login number 3 can forcibly log out "staff" with login number 2, but not "operator" with login number 4. However, when this command is executed from the console, users with different accounts can be forcibly logged out.
4. If a failure occurs, such as a cable disconnection when the command execution results are being displayed, a forced logout might not be able to be performed. In this case, a forced logout is performed after the recovery from the failure. If the failure recovery is not successful, a forced logout is performed after the TCP protocol times out. Although the timeout period of the TCP protocol varies depending on the line speed or line quality, the protocol usually times out after 10 minutes.

show accounting

Displays accounting information.

Syntax

```
show accounting
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 5-4: Displaying accounting information

```
>show accounting
Date 20XX/09/26 10:52:49 UTC
Since 20XX/09/26 10:45:00 UTC

Event
    Login  :         15          Logout :         10
    Command:          -          Config :          -
    Total  :         25

    InQueue:         10
    Discard:          5

[RADIUS]
    Host: RADIUS111
      Event Counts:         10                (Timeout: 30  Retransmit: 15)
      Request Information                  Response Information
        Send             :          0        Success          :          0
        Communicate Error:          0        Failure          :          0
        Timeout          :         10        Invalid          :          0

    Host: 192.168.111.111
      Event Counts:         10                (Timeout: 30  Retransmit: 15)
      Request Information                  Response Information
        Send             :          4        Success          :          4
        Communicate Error:          5        Failure          :          0
        Timeout          :          1        Invalid          :          0


>show accounting
Date 20XX/09/26 10:52:49 UTC
Since 20XX/09/26 10:45:00 UTC

Event
    Login  :          6          Logout :          6
    Command:          0          Config :      60000
    Total  :      60012

    InQueue:        512 (Congestion)
    Discard:      55000

[TACACS+]
    Host: 192.168.111.112
      Event Counts:        500                              (Timeout:  0)
      Request Information                  Response Information
        Send             :        500        Success          :        400
```

```
Communicate Error:          0         Failure          :        100
Timeout          :          0         Invalid          :          0
```

Display items

Table 5-2: Display items for the accounting information

Item	Meaning	Displayed detailed information
Since	Statistics start time	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second
Event	Displays the status of accounting events.	
Login	Number of login events	Displays "-" when target event accounting is not set in the system configuration.
Logout	Number of logout events	Displays "-" when target event accounting is not set in the system configuration.
Command	Number of execution events for operation commands	Displays "-" when target event accounting is not set in the system configuration.
Config	Number of execution events for configuration commands	Displays "-" when target event accounting is not set in the system configuration.
Total	Total number of accounting events	Indicates the total number of the above events.
InQueue	Number of transmission queue events	• Displays the number of transmission queue accounting events when a large volume of accounting events to be transmitted occurs. • Displays (Congestion) when a device log is output and a congested state occurs.
Discard	Number of discarded events	When the congesting of an accounting event transmission occurs, the number of discarded events is counted.
[RADIUS]	• This item is displayed when a RADIUS server is set to be used by the system accounting configuration. • The following accounting statistics are displayed for each RADIUS server. (Not configured) is displayed in the following items when the RADIUS server configuration is not set or all RADIUS servers are for logon authentication only, not accounting.	
Timeout	Reply timeout time	1 to 30 (seconds)
Retransmit	Number of re-transmissions	0 to 15 (times)
Host	Target host name or IP address	It is displayed in order of server priority.
Event Counts	Number of accounting events	Displays the number of events to be reported to the target RADIUS server.
Request Information	Displays accounting request information.	
Send	Number of accounting request transmissions	• The number of times the Switch sent accounting requests to servers. • It is counted as a response timeout (Timeout), but not as a transmission error (Communicate Error).
Communicate Error	Number of accounting request transmission errors	This item is counted when communication to servers is not successful, such as when the address corresponding to the host name is not found, or a route to the server does not exist.

Item	Meaning	Displayed detailed information
Timeout	Number of accounting response timeouts	This item is counted when a response from a server times out.
Response Information	Displays accounting response information.	
Success	Number of successful accounting responses	This item is counted when an accounting response is received from a server.
Failure	Number of failed accounting responses	This item is counted when a response other than an accounting response is received from a server.
Invalid	Number of invalid message responses	This item is counted when an invalid message is received from a server.
[TACACS+]	• This item is displayed when a TACACS+ server is set to be used by the system accounting configuration. • The following accounting statistics are displayed for each TACACS+ server. A term (Not configured) is displayed in the following items when the TACACS+ server configuration is not set or all TACACS+ servers are for logon authentication only, not accounting.	
Timeout	Reply timeout time	1 to 30 (seconds)
Host	Target host name or IP address	It is displayed in order of server priority.
Event Counts	Number of accounting events	Displays the number of events to be reported to the target TACACS+ server.
Request Information	Displays accounting request information.	
Send	Number of accounting request transmissions	• The number of times the Switch sent accounting requests to servers. • It is not counted as a response timeout (Timeout) or as a transmission error (Communicate Error).
Communicate Error	Number of connection errors	This item is counted when communication to servers is not successful, such as when the address corresponding to the host name is not found, or a route to the server does not exist.
Timeout	Number of timeouts of accounting connections and responses	This item is counted when a connection or communication to a server times out.
Response Information	Displays accounting response information.	
Success	Number of successful accounting responses	This item is counted when an accounting success is received from a server.
Failure	Number of failed accounting responses	This item is counted when an accounting failure is received from a server.
Invalid	Number of invalid message responses	This item is counted when an invalid message is received from a server.

Impact on communication

None

Notes

None

clear accounting

Clears accounting statistics.

After accounting events that were being sent to or received from each server when this command was executed have been successfully transmitted, the service will start recording statistics about the accounting events.

Syntax

```
clear accounting
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 5-5: Clearing accounting information

```
>clear accounting
Date 20XX/09/26 10:52:49 UTC
>
```

Display items

None

Impact on communication

None

Notes

After accounting events that were being sent to or received from each server when this command was executed have been successfully transmitted, the service will start recording statistics about the accounting events.

restart accounting

Restarts the accounting program.

Syntax

```
restart accounting [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the accounting program without outputting a restart confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file when the program is restarted.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

Restarts the accounting program after outputting a restart confirmation message.

Example

Figure 5-6: Example of restating the accounting program

```
> restart accounting
accounting program restart OK? (y/n):y
Date 20XX/12/26 11:02:42 UTC
>

> restart accounting -f
Date 20XX/12/26 11:12:42 UTC
>
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of the core file are as follows:

Storage directory: /usr/var/core/

Core file name: acctd.core

If the file has already been output, the existing file is unconditionally overwritten. If the existing file is necessary, back it up before executing the command.

dump protocols accounting

Outputs to a file detailed event trace information and control table information collected for the accounting program.

Syntax

```
dump protocols accounting
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 5-7: Example of taking an accounting dump

```
> dump protocols accounting
Date 20XX/09/26 11:03:19 UTC
>
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of the output dump file are as follows.

Storage directory: /usr/var/accounting/

File name: accounting_dump.gz

If the file has already been output, the existing file is unconditionally overwritten. If the existing file is necessary, back it up before executing the command.

6 SSH

ssh

Provides the secure remote login function and secure command execution function.

Syntax

```
ssh [{-4 | -6}] [-v <version>] [-l <user>] [-c <cipher>] [-m <mac>]
    [-b <source address>] [-p <port>] [-t] [<user>@]<host> [<command>]
```

Input mode

User mode and administrator mode

Parameters

{-4 | -6}

If you specify -4, the connection is established over IPv4 only, and if you specify -6, the connection is established over IPv6 only.

Behavior when this parameter is omitted:

A connection is established via IPv4 or IPv6.

-v <version>

Specifies to use a designated version of the protocol for connection.

You can specify 1 or 2 for <version>. If you specify 1, the connection is established over SSHv1 only, and if you specify 2, the connection is established over SSHv2 only.

Behavior when this parameter is omitted:

A connection is established via SSHv1 or SSHv2.

-l <user>

Specify the user name to be authenticated with 16 or fewer characters.

Behavior when this parameter is omitted:

The current login user name is used. However, if the <user>@ parameter is specified, that user name is used.

-c <cipher>

Specify the name of the common key cryptosystem or authenticated encryption to be used for connection. You can specify 3des or blowfish for SSHv1, and one of the following cryptosystems for SSHv2. (The number indicates the priority in SSHv2.)

1. aes128-gcm@openssh.com
2. aes256-gcm@openssh.com
3. aes128-ctr
4. aes192-ctr
5. aes256-ctr
6. aes128-cbc
7. aes192-cbc
8. aes256-cbc
9. 3des
10. blowfish

11. arcfour256
12. arcfour128
13. arcfour

Behavior when this parameter is omitted:

In SSHv1, the command works in the same way as when 3des is specified. In SSHv2, all of the above are valid. The order of precedence above is followed.

-m <mac>

Specifies the name of the message authentication code method used for connection. You can specify one of the message authentication code method names listed below. (The number indicates the priority in SSHv2.) Note that this parameter does not take effect for SSHv1 connection, even if specified.

1. hmac-sha2-256
2. hmac-sha2-512
3. hmac-sha1
4. hmac-md5
5. hmac-sha1-96
6. hmac-md5-96

Behavior when this parameter is omitted:

The above methods are all valid. The order of precedence above is followed.

-b <source address>

Specifies the source address for SSH connection. An IPv4 or IPv6 address can be specified.

Behavior when this parameter is omitted:

The source address is selected automatically.

-p <port>

Specifies the port number of the destination SSH server. The value ranges from 1 to 65535.

Behavior when this parameter is omitted:

Port number 22 is used.

-t

Forcibly allocates a virtual terminal at execution of the command specified by the <command> parameter. This must be specified in a secure command execution on the Switch.

Behavior when this parameter is omitted:

A virtual terminal is not forcibly allocated to .

<user>@

Specifies the user name for authentication. Specifiable characters are alphanumeric characters and special characters. For details, see "Table 1-9: List of character codes". If the -l <user> parameter is specified together with this parameter, the specified value of this parameter takes precedence.

Behavior when this parameter is omitted:

The current login user name is used. However, if the -l <user> parameter is specified, that user name is used.

<host>

Specifies the SSH server to connect to. The host name, IPv4 address, or IPv6 address can be specified.

<command>

Specifies the command to be executed on the destination SSH server.

Behavior when this parameter is omitted:

The user is remotely logged in to the destination SSH server.

Behavior when all parameters are omitted:

The command works as described in each "Behavior when this parameter is omitted" section.

Example

Figure 6-1: Remotely logging in to host hostA.example.jp using an SSH client

```
> ssh hostA.example.jp
operator@hostA.example.jp's password: ******
```

Figure 6-2: Remotely logging in to host hostA.example.jp with user name staff using an SSH client

```
> ssh staff@hostA.example.jp
staff@hostA.example.jp's password: ******
```

Figure 6-3: Executing the show ip arp command securely on host hostA.example.jp using an SSH client

```
> ssh -t staff@hostA.example.jp show ip arp
staff@hostA.example.jp's password: ******
Date 20XX/04/17 16:59:12 UTC
Total: 2 entries
 IP Address       Linklayer Address  Netif            Expire     Type
 192.168.0.1      0000.0000.0001     VLAN0001         3h55m56s   arpa
 192.168.0.2      0000.0000.0002     VLAN0001         3h58m56s   arpa
Connection to hostA.example.jp closed.
>
```

Display items

None

Impact on communication

None

Notes

1. If you want to specify a user name that cannot be specified with the -l <user> parameter, use the <user>@ parameter.

sftp

Transfers files by secure FTP. With this command, a connection can be established over SSHv2 only.

Syntax

```
sftp [{-4 | -6}] [-l <user>] [-c <cipher>] [-m <mac>] [-P <port>] [<user>@]<host>
```

Input mode

User mode and administrator mode

Parameters

{-4 | -6}

If you specify -4, the connection is established over IPv4 only, and if you specify -6, the connection is established over IPv6 only.

Behavior when this parameter is omitted:

A connection is established via IPv4 or IPv6.

-l <user>

Specify the user name to be authenticated with 16 or fewer characters.

Behavior when this parameter is omitted:

The current login user name is used. However, if the <user>@ parameter is specified, that user name is used.

-c <cipher>

Specify the name of the common key cryptosystem or authenticated encryption to be used for connection. You can specify one of the encryption method names listed below. (The number indicates the priority in SSHv2.)

1. aes128-gcm@openssh.com
2. aes256-gcm@openssh.com
3. aes128-ctr
4. aes192-ctr
5. aes256-ctr
6. aes128-cbc
7. aes192-cbc
8. aes256-cbc
9. 3des
10. blowfish
11. arcfour256
12. arcfour128
13. arcfour

Behavior when this parameter is omitted:

The above methods are all valid. The order of precedence above is followed.

-m <mac>

Specifies the name of the message authentication code method used for connection. You can specify one of the message authentication code method names listed below. (The number indicates the priority in SSHv2.)

1. hmac-sha2-256
2. hmac-sha2-512
3. hmac-sha1
4. hmac-md5
5. hmac-sha1-96
6. hmac-md5-96

Behavior when this parameter is omitted:

The above methods are all valid. The order of precedence above is followed.

-P <port>

Specifies the port number of the destination SSH server. The value ranges from 1 to 65535.

Behavior when this parameter is omitted:

Port number 22 is used.

<user>@

Specifies the user name for authentication. Specifiable characters are alphanumeric characters and special characters. For details, see "Table 1-9: List of character codes". If the -l <user> parameter is specified together with this parameter, the specified value of this parameter takes precedence.

Behavior when this parameter is omitted:

The current login user name is used. However, if the -l <user> parameter is specified, that user name is used.

<host>

Specifies the SSH server to connect to. The host name, IPv4 address, or IPv6 address can be specified.

Behavior when all parameters are omitted:

The command works as described in each "Behavior when this parameter is omitted" section.

Example

Figure 6-4: Transferring the staff.conf file through the sftp connection

```
> sftp staff@hostA.example.jp
*** SSHv2 authentication ***
sftp> ls
staff.conf                          test.conf
sftp> get staff.conf
Fetching /usr/home/staff/staff.conf to staff.conf
/usr/home/staff/staff.conf          100% 4115     4.0KB/s   00:01
sftp> quit
>
```

The "sftp" command can be used with the same operation interface as the conventional FTP program. While the "sftp>" prompt is displayed after this command is executed, the following commands are available:

quit

exit

bye

Exits the application and then ends the sftp prompt.

cd <path>

Changes the current directory on the remote host.

lcd <path>

Change the current directory on the local host.

pwd

Displays the current directory on the remote host.

lpwd

Displays the current directory on the local host.

ls [ls-options [<path>]]

Displays the list of files in <path> on the remote host. If <path> is not specified, the list of files in the current directory is displayed. With the -l option, file permissions, the owner, the size, and the modification time are displayed.

lls [ls-options [<path>]]

Displays the list of files in <path> on the local host. For details, see the "ls" command above.

get <remote path> [<local path>]

Transfers a file from the remote host to the local host. You can also transfer multiple files by specifying "get *.txt".

You can also enter the "mget" command instead of the "get" command. The parameters that can be specified and its functions are the same.

put <local path> [<remote path>]

Transfers a file from the local host to the remote host. You can also transfer multiple files by specifying "put *.txt".

You can also enter the "mput" command instead of the "put" command. The parameters that can be specified and its functions are the same.

rm <path>

Deletes <path> on the remote host.

mkdir <path>

Creates a directory on the remote host.

lmkdir <path>

Creates a directory on the local host.

rmdir <path>

Deletes a directory on the remote host.

rename <old path> <new path>

Renames <old path> to <new path> on the remote host. However, if <new path> exists, the name is not changed.

progress

Enables or disables the progress display during transfer.

?

help

Displays the help message for the command.

Display items

None

Impact on communication

None

Notes

1. Before transferring a file to the Switch with this command, make sure that the capacity available on the Switch is larger than the size of the file to be transferred.
2. Do not use this command to transfer and overwrite files on the local host.
3. Use this command to check the permissions of the directory to which the file is to be transferred, and then transfer the file.
4. If you want to specify a user name that cannot be specified with the -l <user> parameter, use the <user>@ parameter.

scp

Transfers files by secure copy. A connection can be established via SSHv2 or SSHv1.

Syntax

```
scp [{-4 | -6}] [-v <version>] [-l <user>] [-c <cipher>] [-m <mac>]
    [-p] [-r][-P <port>] [<user>@][<host>:]<directory/file>
    [<user>@][<target host>:]<directory/file>
```

Input mode

User mode and administrator mode

Parameters

{-4 | -6}

If you specify -4, the connection is established over IPv4 only, and if you specify -6, the connection is established over IPv6 only.

Behavior when this parameter is omitted:

A connection is established via IPv4 or IPv6.

-v <version>

Specifies to use a designated version of the protocol for connection.

You can specify 1 or 2 for <version>. If you specify 1, the connection is established over SSHv1 only, and if you specify 2, the connection is established over SSHv2 only.

Behavior when this parameter is omitted:

A connection is established via SSHv1 or SSHv2.

-l <user>

Specify the user name to be authenticated with 16 or fewer characters.

Behavior when this parameter is omitted:

The current login user name is used. However, if the <user>@ parameter is specified, that user name is used.

-c <cipher>

Specify the name of the common key cryptosystem or authenticated encryption to be used for connection. You can specify 3des or blowfish for SSHv1, and one of the following cryptosystems for SSHv2. (The number indicates the priority in SSHv2.)

1. aes128-gcm@openssh.com
2. aes256-gcm@openssh.com
3. aes128-ctr
4. aes192-ctr
5. aes256-ctr
6. aes128-cbc
7. aes192-cbc
8. aes256-cbc
9. 3des
10. blowfish

11. arcfour256
12. arcfour128
13. arcfour

Behavior when this parameter is omitted:

In SSHv1, the command works in the same way as when 3des is specified. In SSHv2, all of the above are valid. The order of precedence above is followed.

-m <mac>

Specifies the name of the message authentication code method used for connection. You can specify one of the message authentication code method names listed below. (The number indicates the priority in SSHv2.) Note that this parameter does not take effect for SSHv1 connection, even if specified.

1. hmac-sha2-256
2. hmac-sha2-512
3. hmac-sha1
4. hmac-md5
5. hmac-sha1-96
6. hmac-md5-96

Behavior when this parameter is omitted:

The above methods are all valid. The order of precedence above is followed.

-p

Preserves file attributes and timestamps.

Behavior when this parameter is omitted:

The file attributes and timestamps are not inherited from the copy source.

-r

Copies subdirectories recursively.

Behavior when this parameter is omitted:

The subdirectories are not copied recursively.

-P <port>

Specifies the port number of the destination SSH server. The value ranges from 1 to 65535.

Behavior when this parameter is omitted:

Port number 22 is used.

<user>@

Specifies the user name for authentication. Specifiable characters are alphanumeric characters and special characters. For details, see "Table 1-9: List of character codes". If the -l <user> parameter is specified together with this parameter, the specified value of this parameter takes precedence.

Behavior when this parameter is omitted:

The current login user name is used. However, if the -l <user> parameter is specified, that user name is used.

<host>

<target host>

Specifies the SSH server to connect to. The host name, IPv4 address, or IPv6 address can be specified. Specify an IPv6 address enclosed in square brackets [and].

Example of a specified IPv6 address: scp aaa.txt [2001:db8::10]:aaa.txt

<directory/file>

Specifies a directory and a file name.

Behavior when all parameters are omitted:

The command works as described in each "Behavior when this parameter is omitted" section.

Example

Figure 6-5: Transferring the local staff.cnf file to the remote server

```
> scp staff.conf staff@backup.example.jp:/usr/home/staff/staff.conf
staff@backup.example.jp's password: ******
staff.conf                          100%   89     0.1KB/s   00:00
>
```

A relative path can also be used for the transfer destination. In this case, the path is relative to the user's login directory (home directory).

Display items

None

Impact on communication

None

Notes

1. Before transferring a file to the Switch with this command, make sure that the capacity available on the Switch is larger than the size of the file to be transferred.
2. Use the "ssh" command to check the directory and file permissions of the directory to which the file is to be copied, and then copy the file.
3. Copying from one remote server to another is not supported, and the command is therefore not available for that purpose. Doing so causes an error.
4. If you want to specify a user name that cannot be specified with the -l <user> parameter, use the <user>@ parameter.

show ssh hostkey

Displays the SSHv1/SSHv2 host public key and fingerprint of the Switch.

Syntax

```
show ssh hostkey
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 6-6: Displaying the SSHv1/SSHv2 host public keys and fingerprints

```
> show ssh hostkey
Date 20XX/01/20 12:00:00 UTC
******* SSHv1 Hostkey *******
1024 65537 143208397557440082468455829280312741777235381400368300748962897902811470971617190681
303299617646858883514346610569754524665086092084705971929768474663873473514273709088747193256 45
964193723193907055708167608860751013667295765744933251420901184326738697523138805658247435623 23
389073122546245060001109650904748 47 1024-bit rsa1 hostkey

Fingerprint for key:
SHA256:iCalHPVQ8MeBHBff0RJDWgu/M9G6HYVoWgeguw1Mw1g
MD5:dc:9b:cb:8b:3e:a0:b1:02:87:f7:06:cd:da:63:52:c2

******* SSHv2 DSA Hostkey *******
ssh-dss AAAAB3NzaC1kc3MAAACBAOr87zOuq09Vyu1wVdMfysK5CEcXfHPzJMyA786MdRhk9Fr7ch8u65QHzjM+4/IGe7X
EMU6SggxcNRhllal3b5Oep66UC0EtoAGg9WFmsZvhf784zEIluzZd0ZqyqqfIsqQNmlZhM8nqcVhYH5uDlU8M/89j1B7l2U
+pjcJ6SRjFAAAAFQCXanImCvKAUF46GF+I6UdZXaBeFwAAAIEAyj/pHnizaQWLTi4A8MwMmUFduqy1KqgyE6vPpG2JKNpIi
uqm2Szk9nla5SjJiAR5kqCdeT/Wr4rdjOYqKdcrW18XoW1xvSOi/l9NY6+45ePDMlParW6uPIk75q37vNqSaLMcCKrv+75Y
DDv3tob4HU5/qvy7ZJv31Pu2bUrabasAAACAQz7TOf5KeDcLIZsYv3lVXTwvF9l0sjlaJcOaiKn90OaRrdRUOLmeC0IddTV
VlF/5oyFEXaz8V4EHWA7ul+iEeeksYR8Lnr5UQRboXJ9b/dAXMnqt4z39tekuwP1XxNI7vhEkfn7iLwEh+fUcTobP8yYcQc
9StPeiin3nwn+cQXw= 1024-bit dsa hostkey

Fingerprint for key:
SHA256:O+GPxz5QtjOD8wCEK2HhhHDkjocEY3IEIeF+ltuwJU4
MD5:e8:f8:71:1b:31:ba:c0:21:ee:ce:88:0f:78:e4:d7:09

******* SSHv2 RSA Hostkey *******
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCxHWN1j0PsRnDNTPiUbxbjhm8HyMkTFcAEe9EqPU1/ppp8j73cHJBuL6c
ZDok6cGH1FBrCspE+yj+CFDhNaLRjjoJoBwfpCCkTNJZjT7sDCKjiF4vuPIfpiTEzYQmkG7bfZdmhKIwtB8BhnpyO5trInZ
pafaa7Hght5hkmtJ6YgBuA5fOhVYJiTuFitESPxpt6LkuMpUcV+6Gg8gMkDCdTEaakXPcKFVBy3GHlfDyMy1mWrx4NNYktf
T7ilPafpJMtXQjWzsFQd1mALVKE8uRM5h9wPsqzq6zGqMLNrw6ETFAEJ63JZ1nT20m6yCfGSIREo7OAPNwZQUbZCtOSLJr1
 2048-bit rsa hostkey

Fingerprint for key:
SHA256:Nj/kt3eeKAlO/LnkIgdPKoD31RvAH3jW2cRPw0UABlg
MD5:45:f7:41:10:6d:7f:33:88:f7:94:d5:60:d8:9f:99:c4

******* SSHv2 ECDSA Hostkey *******
ecdsa-sha2-nistp521 AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBAA0d75zwWM0yX+naTVzlSP
wiEuZMZ6jh5nwTF8KyUEDX2QKWmJViW5TYLIaniokERSYnMPWQZGSkNPuMavl9VH9YwCJ8YEdtrOgneei4VjvtOq1iOiOwZ
5sXNNUlKO9LE3rvGoGevywMxOfWYP1jdurUz7NsgHcVmWmZEgVyg9ukloEEQ== 521-bit ecdsa hostkey

Fingerprint for key:
SHA256:jTz5rFJlA6oIrYrWKb6EueKvHcyCQXA1jYU1N+orgqg
MD5:0c:c1:c4:8a:38:b0:46:66:2e:ff:f2:44:3c:57:88:4e
```

Display items

None

Impact on communication

None

Notes

1. As different clients support different fingerprint hash algorithms, the Switch displays both the SHA256 algorithm and the MD5 algorithm.

set ssh hostkey

Creates an SSH host key pair (public and private keys) for the Switch.

Syntax

```
set ssh hostkey [{rsa1 | dsa | rsa {1024 | 2048 | 3072 | 4096} | ecdsa {256 | 384 | 521}}]
```

Input mode

Administrator mode

Parameters

{rsa1 | dsa | rsa {1024 | 2048 | 3072 | 4096} | ecdsa {256 | 384 | 521}}

Specifies the type of host key pair to be created.

rsa1

Creates an RSA host key pair for SSHv1.

dsa

Creates an DSA host key pair for SSHv2.

rsa {1024 | 2048 | 3072 | 4096}

Creates an RSA host key pair for SSHv2. The host key length can be selected from 1024 bits, 2048 bits, 3072 bits, and 4096 bits.

ecdsa {256 | 384 | 521}

Creates an ECDSA host key pair for SSHv2. The host key length can be selected from 256 bits, 384 bits, and 521 bits.

Behavior when this parameter is omitted:

An RSA host key pair for SSHv1 and an RSA host key pair for SSHv2 are created.

Example

Figure 6-7: Changing an SSHv1/SSHv2 host key pair

```
# set ssh hostkey

WARNING!!
Would you wish to generate SSHv1 RSA and SSHv2 RSA hostkeys? (y/n): y
Generating public/private rsa1 key pair.
The key fingerprint is:
SHA256:nxeQpjv+aQOQXo6Wqg0Q9BklwosYJ7K3kkUCXgXwwBg
MD5:a6:7e:c8:3c:0a:d7:ae:e8:78:58:66:8e:9e:be:e8:3a

Generating public/private rsa key pair.
The key fingerprint is:
SHA256:fDIqAY5v/ybGewFybchsJ1r3gMCnYkGTdKJr0TwAtkc
MD5:42:06:3d:06:50:3a:29:4a:2a:79:2f:3c:d4:cc:ea:48

The hostkey generation is completed.
#
```

Figure 6-8: Changing an ECDSA host key pair

```
# set ssh hostkey ecdsa 521

WARNING!!
Would you wish to generate the SSHv2 ECDSA hostkey? (y/n): y
Generating public/private ecdsa key pair.
```

```
The key fingerprint is:
SHA256:jTz5rFJlA6oIrYrWKb6EueKvHcyCQXA1jYU1N+orgqg
MD5:0c:c1:c4:8a:38:b0:46:66:2e:ff:f2:44:3c:57:88:4e

The hostkey generation is completed.
#
```

Display items

None

Impact on communication

None

Notes

1. Basically, you do not need to change the RSA host key pair for SSHv1 and the RSA host key pair for SSHv2 because they are automatically generated on the device at initial startup.

erase ssh hostkey

Deletes an SSHv2 host key pair (public and private keys) of the Switch.

Syntax

```
erase ssh hostkey {dsa | rsa | ecdsa}
```

Input mode

Administrator mode

Parameters

{dsa | rsa | ecdsa}

Specifies the type of the host key pair you delete.

dsa

Deletes the SSHv2 DSA host key pair.

rsa

Deletes the SSHv2 RSA host key pair.

ecdsa

Deletes the SSHv2 ECDSA host key pair.

Example

Figure 6-9: Deleting an SSHv2 RSA host key pair

```
# erase ssh hostkey rsa

WARNING!!
Would you wish to erase the SSHv2 RSA hostkey? (y/n): y

The hostkey was erased successfully.
#
```

Display items

None

Impact on communication

None

Notes

1. An SSHv1 host key pairs cannot be deleted. If you do not use SSHv1, use the "ip ssh version" configuration command to configure it.

show ssh logging

Displays trace logs in operating state on the SSH server.

Syntax

```
show ssh logging
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 6-10: Displaying trace logs on the SSH server

```
> show ssh logging
Date 20XX/12/04 15:30:38 UTC
20XX/12/04 15:30:35 sshd[4021] Disconnected from 192.0.2.1 port 34506
20XX/12/04 15:30:35 sshd[4021] Received disconnect from 192.0.2.1 port 34506:11: disconnected b
y user
20XX/12/04 15:29:36 sshd[4021] Starting session: shell on ttyp0 for sshusr from 192.0.2.1 port
34506 id 0
20XX/12/04 15:29:36 sshd[4021] Entering interactive session for SSH2.
20XX/12/04 15:29:36 sshd[4021] Accepted publickey for sshusr from 192.0.2.1 port 34506 ssh2: RS
A SHA256:EurqlJf/
yKwixDk8bNiCSGi+aVmgFVLx+PyrXQV6dxQ
20XX/12/04 15:29:36 sshd[4021] Postponed publickey for sshusr from 192.0.2.1 port 34506 ssh2
20XX/12/04 15:29:36 sshd[4021] Failed none for sshusr from 192.0.2.1 port 34506 ssh2
20XX/12/04 15:29:34 sshd[4021] kex: server->client cipher: aes128-ctr MAC: hmac-sha2-256 compre
ssion: none
20XX/12/04 15:29:34 sshd[4021] kex: client->server cipher: aes128-ctr MAC: hmac-sha2-256 compre
ssion: none
20XX/12/04 15:29:34 sshd[4021] Client protocol version 2.0; client software version OpenSSH_7.3
20XX/12/04 15:29:34 sshd[4021] Connection from 192.0.2.1 port 34506 on 192.0.2.100 port 22
```

Display items

The following shows the display format of a trace log:

```
yyyy/mm/dd hh:mm:ss sshd[process number] message
        1                2             3
```

1. Time: Sampling year, month, day, hour, minute, and second
2. Process number: Process number of the process on the server
3. Message: Message of the trace log

The following table shows the trace log messages and their descriptions.

Table 6-1: Trace log messages and their descriptions

Message	Description
<authentication method> authentication disabled.	<authentication method> cannot be used. <authentication method>: User authentication method

Message	Description
<function>: <message>	An event was detected. <function>: Function name <message>: Notification description
[/usr]/home/<user>/.ssh/authorized_keys, line <number>: non ssh1 key syntax	A non-SSHv1 public key was found in the registered user public keys. It is not used in SSHv1 public key authentication. <user>: User name <number>: Line number of the line in the public key file
Accepted <authentication method> for <user> from <host> port <port> <ssh version>[: <key type> <fp>]	User authentication was successful with <authentication method>. <authentication method>: User authentication method <user>: User name <host>: Remote host <port>: Port of the remote host <ssh version>: SSH protocol version (ssh1 or ssh2) In public key authentication, the following information is also displayed: <key type>: Type of the user public key <fp>: Fingerprint of the user public key
Bad protocol version identification '<string>' from <host> port <port>	An invalid version identifier was received from <host>. <string>: Version identifier received <host>: Remote host or UNKNOWN <port>: Port of the remote host or 65535
Client protocol version <version>; client software version <software version>	Displays the protocol version and software version of the client. <version>: Protocol version <software version>: Software version
Closing connection to <host> port <port>	The connection with <host> was closed. <host>: Remote host <port>: Port of the remote host
Closing session: usr <user> from <host> port <port> id <session id>	The SSH session will be closed. <user>: User name <host>: Remote host <port>: Port of the remote host <session id>: Session ID
Connection closed by <host> port <port>	The connection with <host> was lost. <host>: Remote host <port>: Port of the remote host
Connection from <host> port <port> on <local host> port <local port>	A connection was established from <port> on <host>. <host>: Remote host <port>: Port of the remote host <local host>: Local host <local port>: Port of the local host
Connection reset by <host> port <port>	A connection with <host> was disconnected. <host>: Remote host <port>: Port of the remote host

Message	Description
Could not write ident string to <host> port <port>	The version identifier could not be sent to <host>. <host>: Remote host <port>: Port of the remote host
Did not receive identification string from <host> port <port>	The version identifier could not be received from <host>. <host>: Remote host <port>: Port of the remote host
Disabling protocol version 1. Could not load host key	The SSHv1 host key could not be loaded. Re-create the host key with the "set ssh hostkey" command.
Disabling protocol version 2. Could not load host key	The SSHv2 host key could not be loaded. Re-create the host key with the "set ssh hostkey" command.
Disconnected from <host> port <port>	A connection with <host> was disconnected. <host>: Remote host <port>: Port of the remote host
Disconnecting: crc32 compensation attack detected	Disconnected because a CRC32 attack was detected.
Disconnecting: deattack denial of service detected	Disconnected because a DoS attack was detected.
Disconnecting: deattack error	Disconnected because some kind of attack was detected.
Disconnecting: Too many authentication failures	Disconnected because an authentication attempt failed many times.
Encryption type: <cipher>	The <cipher> common key cryptosystem is used. <cipher>: Common key cryptosystem name
Entering interactive session for SSH2.	An SSHv2 session has started.
Entering interactive session.	An SSHv1 session has started.
error: <function>: <reason>	An error was detected. <function>: Function name <reason>: Cause
error: auth_rsa_verify_response: RSA modulus too small: <size> < minimum 512 bits	The RSA key length used for public key authentication is too small. <size>: Key length
error: buffer_get_bignum2_ret: <reason>	There is an error in the public key. <reason>: Reason for the error
error: buffer_get_ret: <reason>	There is an error in the public key. <reason>: Reason for the error
error: buffer_get_string_ret: <reason>	There is an error in the public key. <reason>: Reason for the error
error: key_from_blob: <reason>	There is an error in the public key. <reason>: Reason for the error

Message	Description
error: maximum authentication attempts exceeded for [invalid user] <user> from <host> port <port> <ssh version>	The maximum number of authentication attempts was exceeded by <user>. invalid user: Displayed if the user name is invalid. <user>: User name <host>: Remote host <port>: Port of the remote host <ssh version>: SSH protocol version (ssh1 or ssh2)
Exec command '<command>'	The command was executed. <command>: Command
Failed <authentication method> for [invalid user] <user> from <host> port <port> <ssh version>	User authentication with <authentication method> failed. <authentication method>: User authentication method password: Password authentication publickey: Public key authentication none: No authentication invalid user: Displayed if the user name is invalid. <user>: User name <host>: Remote host <port>: Port of the remote host <ssh version>: SSH protocol version (ssh1 or ssh2)
fatal: <function>: <reason>	Terminated forcibly because the function can no longer be continued due to the detected error. <function>: Function name <reason>: Cause
fatal: auth_rsa_verify_response: <reason>	The RSA key used for public key authentication has an error. <reason>: Reason for the error
fatal: decode blob failed: <reason>	The key used for public key authentication has an error. <reason>: Reason for the error
fatal: Login refused for too many sessions.	The connection was refused because there are many sessions connected with the SSH server. Check the terminal from which the connection is established. Use the "clear tcp" command of the Switch to disconnect unnecessary sessions, or wait until the connection times out.
fatal: Timeout before authentication for <host> port <port>	A login authentication attempt timed out. <host>: Remote host <port>: Port of the remote host
fatal: uudecode failed.	The key used for public key authentication has an error.
Generating 1152 bit RSA key.	An RSA server key is being generated.
input_userauth_request: invalid user <user>	An invalid user name was specified. <user>: User name

Message	Description
kex: client->server <cipher> <mac> <compression>	Key exchange negotiation is in progress from the client to the server. <cipher>: Common key cryptosystem name <mac>: Message authentication code method name <compression>: Compression method name
kex: server->client <cipher> <mac> <compression>	Key exchange negotiation is in progress from the server to the client. <cipher>: Common key cryptosystem name <mac>: Message authentication code method name <compression>: Compression method name
Postponed <authentication method> for [invalid user] <user> from <host> port <port> <ssh version>	User authentication with <authentication method> was suspended. <authentication method>: User authentication method invalid user: Displayed if the user name is invalid. <user>: User name <host>: Remote host <port>: Port of the remote host <ssh version>: SSH protocol version (ssh1 or ssh2)
probed from <host> port <port> with <id>. Don't panic.	There is no problem although probing by <id> from <host> was detected. <host>: Remote host <port>: Port of the remote host <id>: Version identifier
Protocol major versions differ for <host> port <port>: <server id> vs. <client id>	There is a difference in the SSH protocol version on <host>: <server id> and<client id>. <host>: Remote host <port>: Port of the remote host <server id>: Version identifier of the server <client id>: Version identifier of the client
Read error from remote host <host> port <port>: <message>	An error occurred when data is received from the remote host. <host>: Remote host <port>: Port of the remote host <message>: Error description
Received disconnect from <host> port <port>: <message>	Disconnected by the remote host. <host>: Remote host <port>: Port of the remote host <message>: Message from the remote host
Received disconnect from <host> port <port>:<code>: <message>	Disconnected by the remote host. <host>: Remote host <port>: Port of the remote host <code>: Identification code notified by the remote host <message>: Message from the remote host
RSA key generation complete.	An RSA server key was generated.
scanned from <host> port <port> with <id>. Don't panic.	There is no problem although searching by <id> from <host> was detected. <host>: Remote host <port>: Port of the remote host <id>: Version identifier

Message	Description
Sent 1152 bit server key and 1024 bit host key.	The server key and host key were sent.
sshd: no hostkeys available -- exiting.	Exiting due to no valid host key. Re-create the host key with the "set ssh hostkey" command.
Starting session: <session type> [on <tty>] for <user> from <host> port <port> id <session id>	An SSH session is started. <session type>: Type of the SSH session (such as shell, command, subsystem 'sftp') <tty>: Terminal information <user>: User name <host>: Remote host <port>: Port of the remote host <session id>: Session ID
subsystem request for <subsystem> failed, subsystem not found	<subsystem> was requested but the request failed. (<subsystem> that is applicable does not exist.) <subsystem>: Name of the subsystem requested
subsystem request for sftp	An sftp connection was requested.
Transferred: sent <tx>, received <rx> bytes	The following data was transmitted: <tx>: Size of the data sent (bytes) <rx>: Size of the data received (bytes)
trying public RSA key file [/usr]/home/<user>/.ssh/authorized_keys	An SSHv1 public key authentication attempt is being made. <user>: User name
Unable to negotiate with <host> port <port>: <reason>: Their offer: <offer>	Cannot be negotiated with <host>. <host>: Remote host <port>: Port of the remote host <reason>: Cause <offer>: Request from the remote host
Unknown packet type received after authentication: <type>	Incorrect packet type <type> was received after authentication. <type>: Type of the SSH client message
User <user> not allowed because <message>	The specified user cannot log in. <user>: User name <message>: Reason for refusal
User uucp not allowed because shell /usr/libexec/uucp/uucico does not exist	The specified user (uucp) cannot log in.
Warning: keysize mismatch for client_host_key: actual <size1>, announced <size2>	The lengths of the client host keys do not match. <size1>: Actual key length <size2>: Advertised key length
Wrong response to RSA authentication challenge.	A wrong response was made to an RSA authentication request.

Impact on communication

None

Notes

1. Up to 64 Kbytes of logs can be stored. If this limit is exceeded, the oldest log is deleted automatically.
2. The SSH server logs are cleared when the Switch is powered off or restarted.

clear ssh logging

Clears trace logs in operating state on the SSH server.

Syntax

```
clear ssh logging
```

Input mode

Administrator mode

Parameters

None

Example

Figure 6-11: Clearing trace logs on the SSH server

```
# clear ssh logging
Would you wish to CLEAR the SSH server's log? (y/n): y

Clear Complete.
```

Display items

None

Impact on communication

None

Notes

None

7 Time Settings and NTP

show clock

Shows the current date and time.

Syntax

```
show clock
```

Input mode

User mode and administrator mode

Parameters

None

Displays the current time.

Example

Enter the following command to display the current time.

```
> show clock
Wed Jun 22 15:30:00 UTC 20XX
>
```

Display items

None

Impact on communication

None

Notes

None

set clock

Shows and sets the date and time.

Syntax

```
set clock <[[[[yy]mm]dd]hh]mm[.ss]>
```

Input mode

User mode and administrator mode

Parameters

yy

Specifies the last two digits of the year. The specifiable values are from 21 to 37.

mm

Specifies the month in the range 1 to 12.

dd

Specifies the day of the month in the range 1 to 31.

hh

Specifies the hour in the range 0 to 23.

mm

Specifies the minute in the range 0 to 59.

ss

Specifies the second in the range 0 to 59.

Behavior when all parameters are omitted:

You can omit the year, month, day, hour, and seconds, but cannot omit the minutes. These elements must be specified in sequence without skipping any. For example, you cannot specify just the day of the month and the minutes (but skip the hour).

Example

To set the date and time as September 01, 2021 at 15:30, enter the following command:

```
> set clock 2109011530
Wed Sep 1 15:30:00 UTC 2021
>
```

Impact on communication

Use of Web authentication or MAC-based authentication might affect communication. See "Configuration Guide Vol. 2, 5.4.1 Notes on changing the Switch configuration and status".

Notes

1. Statistics on CPU usage collected by the Switch will be cleared to zero when the time is changed.

show ntp associations

Shows the running status of the connected NTP server.

Syntax

```
show ntp associations
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 7-1: Displaying the running status of the NTP server

```
> show ntp associations
Date 20XX/01/23 12:00:00 UTC
  remote         refid      st t when poll reach   delay   offset    disp
==============================================================================
*timesvr    192.168.1.100    3 u    1   64  377     0.89   -2.827    0.27
>
```

Display items

Table 7-1: Information displayed by the show ntp associations command

Item	Meaning
remote	Indicates the name of the NTP server. If a local time server is specified, "LOCAL(1)" is displayed. [Meaning of the code at the beginning of the NTP server name] "x": An NTP server rejected by the intersection algorithm (falseticker) " ": An NTP server that is treated as invalid because the activity cannot be checked, or the stratum value is high. "+": An NTP server remaining as an available choice. "#": A selected, synchronized NTP server. However, the upper limit of the distance is exceeded. "*": A selected, synchronized NTP server. Other symbols: NTP servers that are found to be invalid as a result of testing.
refid	The destination NTP server to which the NTP server is synchronized.
st	The stratum value of the NTP server
t	Indicates a server type. [Meaning of displayed server types] "u": Unicast server "b": Broadcast server "l": Local server

Item	Meaning
when	When the Switch is connected to the NTP server, this item indicates the time elapsed since the last packet was received from the NTP server. If the Switch is disconnected from the NTP server, this item indicates the time elapsed since the NTP server was last synchronized. "-" is displayed when the elapsed time is 0 seconds or less. [Meaning of the symbol at the end of a displayed number] "m": In minutes (for 2049 seconds or more) "h": In hours (for 301 minutes or more) "d": In days (for 97 hours or more) If only a number is displayed with no symbol, the displayed value is in seconds.
poll	Indicates the NTP server polling interval (in seconds).
reach	Indicates reachability in octal notation.
delay	Indicates the total both-way delay time from the reference source to the synchronized subnet (in milliseconds).
offset	Indicates the offset value (in milliseconds).
disp	Indicates the latency (variation) in the time from the reference source to the synchronized subnet (in milliseconds).

Impact on communication

None

Notes

None

restart ntp

Restarts the local NTP server.

Syntax

```
restart ntp
```

Input mode

Administrator mode

Parameters

None

Example

Figure 7-2: Restarting the NTP server

```
# restart ntp
#
```

Display items

None

Impact on communication

None

Notes

None

8 Utilities

diff

Compares two specified files and displays their differences.

Syntax

```
diff [<option>] <file name1> <file name2>
diff [<option>] <directory1> <directory2>
```

Input mode

User mode and administrator mode

Parameters

<option>

-i: Ignores the difference between upper-case and lower-case letters.

-r: Applies the command to common subdirectories recursively (when directories are specified).

Behavior when this parameter is omitted:

The specified files are compared, with upper-case and lower-case letters distinguished.

<file name1> <file name2>

Specifies the names of files to be compared.

<directory1> <directory2>

Specifies the names of directories to be compared.

Example and display items

```
# diff aaa.txt bbb.txt
3d2           <---------------1
< Test 3
6c5           <---------------2
< Test 6
---
> Test 66
7a7           <---------------3
> Test 8
#
```

1. It indicates that "Test3" on the third line of aaa.txt is deleted in bbb.txt.
2. It indicates that "Test6" on the sixth line of aaa.txt is different from "Test66" on the fifth line of bbb.txt.
3. It indicates that "Test8" was added to the seventh line of bbb.txt.

Impact on communication

None

Notes

If a text file that is 4 MB or larger is specified using this command, a message (/usr/bin/diff: memory exhausted) is displayed and the command execution might be aborted on the way.

grep

Retrieves a specified file and outputs lines containing a specified pattern.

Syntax

```
grep[<option>] <pattern> [<file name>]
```

Input mode

User mode and administrator mode

Parameters

<option>

-n: Inserts the line number at the beginning of each line in the retrieved result.

-i: Retrieves a file without distinguishing between upper-case and lower-case letters.

Behavior when this parameter is omitted:

Retrieves the specified file while distinguishing between upper-case and lower-case letters and outputs the result with no line numbers.

<pattern>

Specifies the search string.

<file name>

Specifies the file name.

Behavior when this parameter is omitted:

Searches the standard input for specified <pattern>.

Behavior when all parameters are omitted:

Searches the standard input for specified <pattern>.

Example and display items

None

Impact on communication

None

Notes

None

more

Shows one page of the contents of a specified file.

Syntax

```
more [<option>] <file name>
```

Input mode

User mode and administrator mode

Parameters

<option>

-N: Displays the line number at the beginning of each line.

Behavior when this parameter is omitted:

Line numbers are not displayed.

<file name>

Specifies the file name.

Example and display items

None

Impact on communication

None

Notes

None

less

Shows one page of the contents of a specified file.

Syntax

```
less [<option>] <file name>
```

Input mode

User mode and administrator mode

Parameters

<option>

-m: Always displays a percentage representing the current line in the prompt.

-N: Displays the line number at the beginning of each line.

Behavior when this parameter is omitted:

The percentage and line number of the current line are not displayed.

<file name>

Specifies the file name.

Example and display items

None

Impact on communication

None

Notes

None

tail

Outputs the contents of a specified file from a specified point.

Syntax

```
tail [<option>] <file name>
```

Input mode

User mode and administrator mode

Parameters

<option>

-n: Outputs n lines from the end.

Behavior when this parameter is omitted:

10 lines from the end are output.

<file name>

Specifies the file name.

Example and display items

None

Impact on communication

None

Notes

None

hexdump

Shows a hexadecimal dump.

Syntax

```
hexdump [<option>] <file name>
```

Input mode

User mode and administrator mode

Parameters

<option>

-b: Displays a dump in octal notation for every byte.

-c: Displays a dump in characters for every byte.

Behavior when this parameter is omitted:

A dump is displayed in hexadecimal notation every one byte.

<file name>

Specifies the file name.

Example and display items

None

Impact on communication

None

Notes

None

9 Device Management

show version

Shows information about the Switch software and the board installed.

Syntax

```
show version [software]
```

Input mode

User mode and administrator mode

Parameters

software

Only the software information is displayed.

Behavior when this parameter is omitted:

Displays information about the Switch software and the boards installed.

Example

Figure 9-1: Displaying the software version only

```
> show version software
Date 20XX/04/01 02:54:45 UTC
S/W: OS-L2N Ver. 1.0
>
```

Figure 9-2: Displaying information about the Switch software and the boards installed

```
> show version
Date 20XX/04/01 02:56:29 UTC
Model: AX2340S-24P4X
S/W: OS-L2N Ver. 1.0
H/W: Main board
       AX-2340-24P4X-B [PA023424P4X0S0000LBH004]
>
```

Display items

Table 9-1: Information displayed by the show version command

Item	Displayed information	Displayed detailed information
Model	Device model	—
S/W	Software information	Software type, version
H/W		
Main board	Information about the main board	AX-xxxx-xxxxxx: Abbreviation of the model name [ssss….ssss]: Serial information

Impact on communication

None

Notes

None

show system

Shows the operating status.

Syntax

```
show system
```

Input mode

User mode and administrator mode

Parameters

None

Example 1

Figure 9-3: Displaying the result of executing the show system command

```
> show system
Date 20XX/01/16 17:53:12 UTC
System: AX2340S-48P4X, OS-L2N Ver.1.0
Node : Name=
    Contact=
    Locate=
    Elapsed time : 00:45:03
    Chassis MAC address : 0012.e23e.b20f
    MC Configuration mode : disabled
    Zero-touch-provisioning status : enabled(no change)
    PS1 : active
        Fan  : active No = Fan1(1) Speed normal, Direction = F-to-R
    PS2 : notconnect
    Fan : active
        Fan  : active no = Fan3(1) , Fan3(2)
               Speed = normal, Direction = F-to-R
    Main board : active
        Boot : 20XX/01/16 17:08:19 , operation reboot
        Boot device : primary
        Fatal restart : System 0 times ,  SW 0 times
        Lamp : Power LED=green , Status LED1=green , Status LED2=green
        Board : CPU=1600MHz , Memory=1,808,284KB(1765MB)
        Temperature : normal(26degree)
        Flash :
                  user area   config area     dump area    area total
            used    7,872KB         172KB          32KB       8,076KB
            free  498,220KB     114,620KB      99,368KB     712,208KB
            total 506,092KB     114,792KB      99,400KB     720,284KB
        MC  : enabled
            Manufacture ID : 00001683
            257,824KB used
            3,612,960KB free
            3,870,784KB total
                   :
                   :
                   :
```

Display items in Example 1

Table 9-2: Information displayed by the show system command

Item	Displayed information	Displayed detailed information
System	Device model	—
	Software information	Software type, version
Node	Node information	—
Name	System name	Identification name set by the user
Contact	Contact information	Contact information set by the user
Locate	Installation location	Installation location set by the user
Elapsed time	Elapsed time	The time elapsed since the device started
Chassis MAC address	Chassis MAC address	—
MC configuration mode	Running status of the memory card operation mode	enabled: Enabled disabled: Disabled
Zero-touch-provisioning status	Start-up status of the zero-touch provisioning running mode	enabled(<status>): The device is started in zero-touch provisioning running mode. <status>: Whether changes in the device information are available • no change: No update is available. • change: Update is available.
		disabled(<reason>): The device is started in normal running mode. <reason>: Reason for which the device was started in normal running mode • no configuration: Zero-touch provisioning is not enabled. • linkdown: The interface with zero-touch provisioning enabled is in link-down state. • no ip address: Failed to obtain an IP address. • file get failed: Failed to get a file. • file read failed: Failed to read a file. • file write failed: Failed to write to a file.
PS	Power supply	—
	Status of the power supply	active: Supplied normally fault: No supply/voltage fault notconnect: Not installed
Fan	Fan running status[#1]	Fan number of an active fan
Speed	The rotational speed of the fan	normal: Normal rotation high: High-speed rotation stop: Stopped rotation
Direction	Direction of the fan	F-to-R: Front air intake and rear air exhaust
Fan	Status of the fan	active: Supplied normally fault: Failure occurred notconnect: Not installed

Item	Displayed information	Displayed detailed information
Fan	Fan running status[#1]	Fan number of an active fan
Speed	The rotational speed of the fan	normal: Normal rotation high: High-speed rotation stop: Stopped rotation
Direction	Direction of the fan	F-to-R: Front air intake and rear air exhaust
Main board	Information about the main board	—
	Behavior status of the main board	active: Running fault: Failure occurred initialize: Initializing
Boot	Startup time of CPU	Startup time of CPU
	Cause of CPU startup	-: The power switch was turned ON or the device was restarted unexpectedly. operation reboot: Reboot command fatal: Restart (a failure occurs)
Boot device	Boot device	primary: Normal boot from internal flash memory secondary: Boot from the backup software in the internal flash memory MC: Boot from a memory card
Fatal restart	Number of times a restart is performed due to a failure	System: Number of times the device restarts due to a failure SW: Number of times the switching processor is restarted due to a failure Note: The CPU value is initialized one hour after the device is restarted. The SW value is initialized one hour after the device is restarted or after the first failure occurs.
Lamp	LED indication	light off: The LED is off. green blink: The LED is green and blinking. green: The LED is on and green. orange blink: The LED is orange and blinking. orange: The LED is on and orange.
Board	CPU information	Clock speed of the CPU
	Amount of memory installed on the main board	Amount of memory installed on the main board
Temperature	Temperature information inside the device	normal: Normal (higher than 5°C and lower than 75°C) caution: Caution (below 5°C or above 75°C and below 80°C) Note: If the sensor detects a temperature of 80°C or higher, the software stops.
Flash	Used capacity[#2, #3]	Capacity in use by the file system in the internal flash memory user area: Used capacity in the user area config area: Used capacity in the configuration area dump area: Used capacity in the dump area area total: Total of each used capacity in the user area, configuration area, and dump area

Item	Displayed information	Displayed detailed information
	Unused capacity[#2, #3]	Capacity not being used by the file system in the internal flash memory user area: Unused capacity in the user area config area: Unused capacity in the configuration area dump area: Unused capacity in the dump area area total: Total of each unused capacity in the user area, configuration area, and dump area
	Total capacity[#2, #3]	Total of capacity being used and capacity not being used for the file system in the internal flash memory user area: Total of used and unused capacity in the user area config area: Total of used and unused capacity in the configuration area dump area: Total of used and unused capacity in the dump area area total: Total capacity being used and not being used by the file system in the internal flash memory
MC	Memory card status	enabled: The memory card can be accessed. notconnect: The memory card is not inserted. --------: Another process is accessing the memory card.[#4]
	Type[#2, #3]	Manufacture ID: Memory card manufacturer number
	Used capacity[#2, #3]	Capacity in use in the memory card file system
	Unused capacity[#2, #3]	Capacity not in use in the memory card file system
	Total capacity[#2, #3]	Total of capacity in use and capacity not in use for the memory card file system

#1

The fan location is indicated in FANx(y) format. The following table describes the correspondence between information in operation log and names specified on the chassis. The right and left sides described in Location on the chassis represent the positional relation as viewed from the back of the device.

Table 9-3: Correspondences between fan numbers, operation log data, and chassis

Command and operation log display	Location on the chassis
FAN1(1)	Power supply on the right in the rear
FAN2(1)	Power supply on the left in the rear
FAN3(1)	On the right in the rear of the chassis 1
FAN3(2)	On the right in the rear of the chassis 2

#2

The item is displayed when the memory card is enabled.

#3

These items indicate the amount of space used and the space available for the file system on the internal flash memory or the memory card.

#4

Another process is accessing the memory card. Wait a while, and then re-execute the command.

Example 2

The following is an example of displayed resource information.

Figure 9-4: Displaying resource information

```
> show system
Date 20XX/06/17 15:09:34 UTC
System: AX2340S-24T4X, OS-L2N Ver.1.0
Node : Name=System Name
 :
 :
    Device resources
        MAC-Address table entry : current number=1014 , max number=16384
        System Layer2 Table Mode : mode=0
        Flow detection mode : layer2-1
          Used resources for filter (Used/Max)
                    MAC      IPv4      IPv6
               256/ 256       n/a       n/a
          Used resources for QoS(Used/Max)
                    MAC      IPv4      IPv6
                 0/ 128       n/a       n/a
```

Display items in Example 2

Table 9-4: Information displayed by the show system command (resource information)

Item	Displayed information	Displayed detailed information
Device resources	Hardware entry information	—
MAC-Address table entry	Number of MAC address table entries set on the hardware	current number: Number of MAC address table entries currently set on the hardware. max number: Maximum number of MAC address table entries that can be set on the hardware. Note: A hyphen (-) is displayed if the status of the Main board item is Fault.
System Layer2 Table Mode	Search method for the Layer 2 hardware table	mode= x: Value set by the "system l2-table mode" configuration command If the mode is not set by using the "system l2-table mode" configuration command, 0 is displayed for x.
Flow detection mode	Receiving-side flow detection mode for the filters and QoS function	For details, see the description of the "flow detection mode" configuration command.
Used resources for filter (Used/Max)	Number of entries currently registered as filter conditions on the target interface, and the maximum number of specifiable entries The number of the setting entries is the total of the implicit discard entries and the filtering condition entries set during configuration.	
	Applicable interface#	The interfaces are not displayed because there is no limit on the number of entries for each interface.
	Target access list type	MAC: MAC access lists
		IPv4: IPv4 access lists, standard IPv4 access lists, and extended IPv4 access lists

Item	Displayed information	Displayed detailed information
		IPv6: IPv6 access lists
	Number of entries that have been set and the maximum number of entries that can be set	In the flow detection mode, access lists marked n/a are not subject to detection.
Used resources for QoS(Used/Max)	The number of entries for QoS flow detection conditions and the action information that are currently registered on the target interface, and the maximum number of specifiable entries	
	Applicable interface#	The interfaces are not displayed because there is no limit on the number of entries for each interface.
	Target QoS flow list type	MAC: MAC QoS flow lists
		IPv4: IPv4 QoS flow lists
		IPv6: IPv6 QoS flow lists
	Number of entries that have been set and the maximum number of entries that can be set	In the flow detection mode, QoS flow lists marked "n/a" are not subject to detection.

#

There is no capacity limit of each target port.

Impact on communication

None

Notes

None

clear control-counter

Resets the following counters to zero:

- Number of times the device restarts due to a failure
- Number of times the switching processor is restarted
- Number of times a restart is performed due to a port failure

Syntax

```
clear control-counter
```

Input mode

User mode and administrator mode

Parameters

None

Example

Reset to zero the number of restarts due to a failure:

```
> clear control-counter
```

Display items

None

Impact on communication

None

Notes

None

show environment

Displays the status of the fan, power supply unit, and the temperature of the chassis and the total operating hours.

Syntax

```
show environment [temperature-logging]
```

Input mode

User mode and administrator mode

Parameters

temperature-logging

Displays the temperature history of the target device.

Behavior when this parameter is omitted:

The environmental status of the device is displayed.

Example 1

The following shows an example of displaying the operating status.

Figure 9-5: Result of executing the show environment command

```
> show environment
Date 20XX/01/01 12:00:00 JST
Module slot 1 : PS-M(AC), Direction = F-to-R
Module slot 2 : notconnect

Fan environment
    PS1 : Fan1(1) = active
          Speed = normal
    PS2 : Fan2(1) = notconnect
    Fan : Fan3(1) = active
          Fan3(2) = active
          Speed = normal
    Fan mode     : 1 (silent)

Power environment
    PS1 : active
    PS2 : notconnect

Temperature environment
    Main  :  30 degrees C
    Warning level : normal

Accumulated running time
    Main         :  total    : 36 days and 6 hours.
                    critical : 0 days and 0 hours.
>
```

Display items in Example 1

Table 9-5: Information displayed by the show environment command

Item	Displayed information	Displayed detailed information
Module slot	Type of the unit installed in the module slot[#1]	PS-M(AC): AC power supply notconnect: Not installed
	Direction: Direction of the fan[#2]	F-to-R: Front air intake and rear air exhaust
Fan environment		
PS	Power supply number	—
Fan[#3]	Fan behavior status	active: Running fault: A failure has occurred. notconnect: Not installed
Speed	The rotational speed of the fan	normal: Normal rotation high: High-speed rotation stop: Stopped rotation --------: Not installed
Fan		
Fan[#3]	Fan behavior status	active: Running fault: A failure has occurred. notconnect: Not installed
Speed	The rotational speed of the fan	normal: Normal rotation high: High-speed rotation stop: Stopped rotation --------: Not installed
Fan mode	Fan operating mode	1 (silent): Reducing switch noise takes priority 2 (cool): Keeping the switch cool takes priority
Power environment		
PS	Status of the input power supply unit	active: Supplied normally fault: No supply/voltage fault notconnect: Not installed
Temperature environment		
Main	Temperature inside the device	Displays temperature information for a device.
Warning level[#4]	Operating condition level	normal: Normal caution: Caution (High or low temperature)
Accumulated running time[#5]		
Main	total: Cumulative operating time of the device critical: Cumulative operating time of the device when the temperature inside the device is at 75°C or higher	During normal operation, total is displayed. fault: The operating time could not be loaded. ****: The operating time is being loaded.

#1: If power is not being supplied to the power supply, "---------" may be displayed.

#2: The information is displayed only when a power supply is installed.

#3

The fan location is indicated in FANx(y) format. The x value indicates the fan unit number, and the y value indicates the fan number. The following table describes the correspondence between information in operation log and names specified on the chassis. The right and left sides described in Location on the chassis represent the positional relation as viewed from the back of the device.

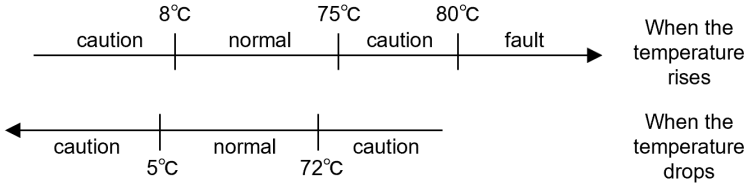
Table 9-6: Correspondences between fan numbers, operation log data, and chassis

Command and operation log display	Location on the chassis
FAN1(1)	Power supply on the right in the rear
FAN2(1)	Power supply on the left in the rear
FAN3(1)	On the right in the rear of the chassis 1
FAN3(2)	On the right in the rear of the chassis 2

#4: Warning level is displayed as a result of evaluating the changes in the temperature inside the device.

If the sensor detects a temperature of 80℃ or higher, the software stops.

Figure 9-6: Operating environment level and temperature values



#5

The cumulative operating time information in each board is updated every six hours. Therefore, if the operating time is less than six hours, the information in each board is not updated and the operating time recorded in each board will not be correct.

At power-up (cumulative operating time = 0)

4 hours later (cumulative operating time = 4 hours, time written in the board = 0 hours)

8 hours later (cumulative operating time = 8 hours, time written in the board = 6 hours)

13 hours later (cumulative operating time = 13 hours, time written in the board = 12 hours)

Example 2

The following shows an example of displaying the average temperature information.

Figure 9-7: Displaying average temperature information

```
> show environment temperature-logging
Date 20XX/11/30 12:00:00 UTC
Date         0:00  6:00 12:00 18:00
20XX/11/30   24.3  24.2  26.0
20XX/11/29   21.8  25.1  26.0  24.0
20XX/11/28   25.6     -  26.0  24.0
20XX/11/27   21.0     -  26.0  24.0
20XX/11/26   24.0  23.5  26.0  24.0
20XX/11/25   22.2  24.9  26.0  24.0
20XX/11/24      -     -  26.0  24.0
>
```

Display items in Example 2

Table 9-7: Information displayed by the show environment temperature-logging command

Item	Displayed information	Displayed detailed information
Date	Date	—
0:00	Average temperature of the time range	Average temperature of the period from 18:00 (previous day) to 0:00
6:00		Average temperature of the period from 0:00 to 06:00
12:00		Average temperature of the period from 6:00 to 12:00
18:00		Average temperature of the period from 12:00 to 18:00
"-"	Hyphen (-)	The device was not running. (Power was off or the history could not be held because the system time was changed.)
" "	Blank	Temperature aggregation not yet performed

Impact on communication

None

Notes

- The temperature history display is refreshed at the fixed times (0:00, 6:00, 12:00, and 18:00). The times might slightly change depending on the environment of the device. Also, if the device is restarted at the same time when the temperature log data is updated, part of the temperature log data might be lost.
- For the display of temperature history, if the date of the device is changed, the change is applied at 0:00 on the next day. Because the information items are displayed in the order they are collected, they are not displayed chronologically.
- If the device is restarted while the cumulative running time records are being updated, the cumulative running time might return to zero.

reload

Restarts the device, and then collect logs. As the default behavior, memory dump information is collected.

Syntax

```
reload [stop] [{no-dump-image | dump-image}] [-f]
```

Input mode

User mode and administrator mode

Parameters

stop

Stops without restarting.

{no-dump-image | dump-image }

no-dump-image

Disables the collection of memory dump information.

dump-image

Enables the collection of memory dump information.

Behavior when this parameter is omitted:

The command works in the same way as when dump-image is selected.

-f

Executes the command without displaying a confirmation message. A memory dump is collected if it is not specified whether or not to collect a memory dump.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example

1. Restart the device:

   ```
   >reload
   ```

2. Display a confirmation message for memory dump collection when the "reload" command is started:

   ```
   Dump information extracted?(y/n):_
   ```

   If "y" is entered here, the system displays a message indicating that the request to restart the switch was accepted, writes memory dump information to the internal flash memory, and then restarts the switch.

3. If memory dump information has already been collected, the following message is displayed:

   ```
   old dump file delete OK? (y/n):_
   ```

   If "y" is entered, the existing memory dump is deleted.

   If "n" is entered, the system displays the command prompt without restarting the switch.

   If "n" is entered in step 2, the system displays the following confirmation message without restarting the switch:

   ```
   Restart OK? (y/n):_
   ```

   If "y" is entered here, the system displays a message indicating that the request to restart the switch was accepted, and restarts the switch without writing memory dump information to the internal flash mem-

ory. If "n" is entered, the system displays the command prompt without restarting the switch.

Display items

None

Impact on communication

Communication is interrupted while the device is being restarted.

Notes

- The Switch boots from the memory card if a memory card that contains the software image file k.img is inserted. When you use this method, the account and configuration information reverts to the factory defaults and you cannot save your own settings. Avoid using this method under normal circumstances.
- This command cannot be executed while the "ppupdate" or "restore" command is executed by another user. If you attempt to do so, a message is displayed saying "another user is executing update command", and the command terminates abnormally. Wait a while, and then re-execute the command. If the command still terminates abnormally, execute "rm /tmp/ppupdate.exec" to delete files, and then re-execute the command.

show tech-support

Collects hardware and software status information required for technical support.

Syntax

```
show tech-support [page] [<password>] [no-config] [ftp]
```

Input mode

User mode and administrator mode

Parameters

page

Displays a page of the collected information on the console terminal screen. Pressing the Space key displays the next page of information, and pressing the Enter key displays the next line of information. Note that this parameter has no effect when the ftp parameter is also specified.

Behavior when this parameter is omitted:

Pages are displayed continuously without.

<password>

Enters the password if the password for administrator mode is specified. If the password includes a special character, the password needs to be enclosed in " " (double quotation marks).

This parameter can be omitted if the password for administrator mode has not been set. Note that in the configuration where the password for administrator mode has been set, if the password is omitted, then a prompt requesting the password appears. If an incorrect password is specified, the results of executing commands that require administrator mode such as the "show running-config" command are not collected.

Behavior when this parameter is omitted:

The password is not specified. In the configuration where the password for administrator mode has been set, if the password is omitted, then a prompt requesting the password appears.

no-config

The configuration is not collected.

Behavior when this parameter is omitted:

The configuration is collected.

ftp

Saves a text file of collected information, and the dump file and core file from the internal flash memory to a remote FTP server. The dump file and core file are combined into one binary file. When this parameter is specified, collected information is not displayed. Additionally, when this parameter is specified, enter connection setting information for the FTP server as per the prompts.

Behavior when this parameter is omitted:

The collected information is output to the console terminal screen.

Behavior when all parameters are omitted:

The command works as described in each "Behavior when this parameter is omitted" section.

Example

- Example of executing the "show tech-support" command:

Collect basic information that shows the hardware and software status, and display the information on the console terminal screen.

Figure 9-8: Displaying collected information on the screen

```
> show tech-support
########## Tech-Support Log ##########
Tue Nov  8 18:54:46 UTC 20XX

  :                         :
  :         (Omitted)          :
  :                         :

Tue Nov  8 19:28:15 UTC 20XX
########## End of Tech-Support Log ##########
```

- Example of executing the "show tech-support ftp" command:

  Collect basic information that shows the hardware and software status, and save it with a dump file and core file from the internal flash memory to an FTP server. Specify the file name as "support".

  Figure 9-9: Storing the collected information in the FTP server

```
> show tech-support ftp
Enter the host name of the FTP server.            : ftpserver.example.com
Enter the user name for the FTP server connection.: user1
Enter the password for the FTP server connection. : <password for user1>
Enter the path name of the FTP server.            : /usr/home/user1
Enter the file name for the log and dump files.   : support
Mon Dec 18 20:42:58 UTC 20XX
Transferred support.txt .
Executing.
...
File transfer ended successfully.
########## Dump files' Information ##########
***** ls -l /dump *****
-rw-rw-rw-    1 root     root      12527537 Feb 17 11:34 osdump
-rw-r--r--    1 root     root        320658 Feb 17 11:33 rmdump
***** ls -l /usr/var/hardware *****
total 1368
-rwxrwxrwx    1 root     root        738699 Dec 27 11:56 ni00.000
########## End of Dump files' Information ##########
########## Core files' Information ##########
***** ls -l /usr/var/core *****
No Core files
########## End of Core files' Information ##########
Transferred support.tgz .
Executing.
...
File transfer ended successfully.
>
```

Display items

Table 9-8: Information displayed by the show tech-support command

Item	Displayed information
########## <Information Type> ##########	A separator indicating the beginning of each type of collected information. <Information Type> indicates the type of information. The following describes the contents of <Information Type>: Dump files' Information: List of existing dump files Core files' Information: List of existing core files Tech-Support Log: Basic information that shows the hardware and software status

Item	Displayed information
########## End of <Information Type> ##########	A separator indicating the end of each type of collected information. <Information Type> indicates the type of information.
########## <Command Name> ##########	<Command Name> indicates the name of the command executed to collect the information. The execution result of the indicated command is displayed after this separator.
########## End of<Command Name> ##########	A separator that indicates the end of the execution result of the indicated command. <Command Name> indicates the name of the command executed to collect the information.

Impact on communication

None

Notes

1. When the collected information is displayed on the screen (without the ftp parameter), the display interval is as follows:
   - When the information is displayed on the console terminal screen connected to RS232C, the display interval with no parameters specified is five minutes.
   - When the information is displayed on the remote operation terminal screen, the display interval with no parameter is 30 seconds.
2. When a dump file, core file, and collected information are stored in an FTP server (with the ftp option), the time for transferring the files to the FTP server is as follows:
   - When only the dump file and core file for the active system are transferred, the transfer time is one to three minutes.
3. If an IP address is set for the device itself by the "ip address(loopback)" configuration command, the IP address is used as the source IP address during communication with the FTP server.
4. Only dump files and core files in the following directories can be saved to an FTP server when the ftp parameter is specified:
   - Storage directory for dump files

     /dump0 or /usr/var/hardware
   - Storage directory for core files

     /usr/var/core

backup

Saves device information and information about active applications to the internal flash memory, a memory card, or a remote FTP server. The device information includes the password information, configuration, and license information.

Syntax

```
backup {mc | ftp <ftp-server> | flash} <filename> [no-software]
```

Input mode

Administrator mode

Parameters

mc

Specifies the memory card as the backup destination.

ftp <ftp-server>

Specifies a remote FTP server as the backup destination. A host name, IPv4 address, IPv6 address, or IPv6 address with an interface name (only a link-local address) can be specified for <ftp-server>.

flash

Specifies the internal flash memory as the backup destination.

<filename>

Specifies the path and name of the storage-destination file.

Alphanumeric characters, hyphens (-), underscores (_), and periods (.) can be used for a file path and file name specified by the "backup mc" or "backup flash" command. Note that file names which end with a period (.) cannot be used with the "backup mc" command.

The maximum number of characters that can be specified for a file name in the "backup mc" and "backup flash" commands is 255 characters.

no-software

No software is backed up.

Behavior when this parameter is omitted:

Backup, including software information, is performed.

Example 1

Save the current device information to the MCBackup.dat file on the memory card.

```
> enable
# backup mc MCBackup.dat
Backup information to MC (MCBackup.dat).
Copy file to MC...
Backup information success!
```

Example 2

Save the current device information to the MCBackup.dat file on the FTP server.

```
> enable
# backup ftp ftpserver MCBackup.dat
```

```
Backup information to MCBackup.dat in FTP(ftpserver).
Input username: guest
Input password:
ftp transfer start.
ftp transfer succeeded.
Backup information success!
```

Example 3

Save the current device information (excluding software information) to the MCBackup.dat file on the internal flash memory.

```
> enable
# backup flash MCBackup.dat no-software
Backup information to flash memory (MCBackup.dat).
Copy file to flash memory...
Backup information success!
```

Display items

None

Impact on communication

When the mc parameter is specified, if the monitoring time or sending interval of the Layer 2 protocol is set shorter than the initial value on neighboring devices, communication might be interrupted when the connection over the Layer 2 protocol is disconnected.

Notes

- If you want to back up running software as well, the output destination may have to have approximately 150 MB of free space.
- The files under /usr/home/ are not backed up.
- The device information saved by this command can be restored to the Switch by using the "restore" command. If you specify the no-software parameter in this command, also specify the no-software parameter in the "restore" command.
- Perform backup and restoration between the same models.
- Do not allow other users to log in while this command is being executed.
- Do not remove or insert the memory card while the "backup mc" command is backing up data to the memory card.

restore

Restores the device information saved in the internal flash memory, a memory card, or a remote FTP server to the Switch.

Syntax

```
restore {mc | ftp <ftp-server> | flash} <filename> [no-software]
```

Input mode

Administrator mode

Parameters

mc

Specifies a memory card as the location where the image is stored.

ftp <ftp-server>

Specifies a remote FTP server as the location where the image is stored. A host name, IPv4 address, IPv6 address, or IPv6 address with an interface name (only a link-local address) can be specified for <ftp-server>.

flash

Specifies the internal flash memory as the location where the image is stored.

<filename>

Specifies the path and name of the file where the image is stored.

The maximum number of characters that can be specified for a file name in the "restore mc" and "restore flash" commands is 255 characters.

no-software

No software is restored.

Behavior when this parameter is omitted:

All the backup data is restored.

Example 1

Restore the device information from the MCBackup.dat file saved in the memory card.

```
> enable
# restore mc MCBackup.dat
Restore information from MC (MCBackup.dat).
Copy file from MC...
Restore software.
```

Example 2

Restore the device information from the MCBackup.dat file saved in the FTP server.

```
> enable
# restore ftp ftpserver MCBackup.dat
Restore information from FTP(ftpserver) MCBackup.dat.
Input username: guest
Input password:
ftp transfer start.
ftp transfer succeeded.
Restore software.
```

Example 3

Restore the device information (excluding software information) from the MCBackup.dat file on the internal flash memory.

```
> enable
# restore flash MCBackup.dat no-software
Restore information from flash memory (MCBackup.dat).
Copy file from flash memory...
Restore finished.
```

Display items

None

Impact on communication

When the device information has been restored, the device restarts automatically. During the restart, communication is temporarily suspended. When the mc parameter is specified, if the monitoring time or sending interval of the Layer 2 protocol is set shorter than the initial value on neighboring devices, communication might also be interrupted when the connection over the Layer 2 protocol is disconnected.

Notes

- Do not allow other users to log in while this command is being executed.
- Do not remove or insert the memory card while the "restore mc" command is restoring data from the memory card.
- Perform backup and restoration between the same models.
- This command cannot be executed while the "ppupdate" or "restore" command is executed by another user. If you attempt to do so, the command terminates abnormally, and the following message is displayed: another user is executing now. Wait a while, and then re-execute the command. If the command still terminates abnormally, execute "`rm /tmp/ppupdate.exec`" to delete files, and then re-execute the command.
- If you want to restore the device information without software information, execute the command with the no-software parameter specified. Otherwise, the command deletes "`/usr/var/update/k.img`".

10 Checking Internal Memory and Memory Cards

show mc

Shows the memory card format and card usage.

Syntax

```
show mc
```

Input mode

User mode and administrator mode

Parameters

None

Example

```
>show mc
Date 20XX/12/13 06:35:27 UTC
MC  : enabled
     Manufacture ID : 00001683
      257,828KB used
      3,612,956KB free
      3,870,784KB total
>
```

Display items

Table 10-1: Information displayed by the show mc command

Item		Displayed information	Displayed detailed information
MC	—	Memory card status	enabled: The memory card can be accessed. notconnect: The memory card is not inserted. --------: Another process is accessing the memory card.#1
	Manufacture ID	Production ID number#2	Production ID number of the memory card
	used	Used capacity#2	Capacity in use in the memory card file system
	free	Unused capacity#2	Capacity not in use in the memory card file system
	total	Total capacity#2	Total of capacity in use and capacity not in use for the memory card file system

#1: Another process is accessing the memory card. Wait a while, and then re-execute the command.
#2: The item is displayed when the memory card is enabled.

Impact on communication

None

Notes

This command shows both the used and the unused capacity for the file system on the memory card.

format mc

Formats the memory card for use by the Switch.

Syntax

```
format mc [-f]
```

Input mode

User mode and administrator mode

Parameters

-f

Executes the command without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example

1. Insert the memory card to be initialized into the slot, and then enter the following command:
   ```
   >format mc
   ```
2. A message asking for confirmation is displayed after the "format" command is executed.
   ```
   MC initialize OK?  (y/n):_
   ```
   If "y" is entered, the memory card will be initialized.

   If an error occurs, an error message is displayed.

   If "n" is entered, the memory card will not be initialized, and you will be returned to administrator mode.

Display items

None

Impact on communication

None

Notes

- Note that executing this command deletes all the data in the memory card.

show flash

Shows internal flash memory usage.

Syntax

```
show flash
```

Input mode

User mode and administrator mode

Parameters

None

Example

```
> show flash
Date 20XX/12/21 17:53:11 UTC
Flash :
          user area   config area     dump area    area total
    used  377,987KB         102KB           0KB     378,089KB
    free   90,469KB     116,960KB     131,008KB     338,437KB
    total 468,456KB     117,062KB     131,008KB     716,526KB
>
```

Display items

Table 10-2: Information displayed by the show flash command

Item		Displayed information	Displayed detailed information
Flash	—	—	—
	used	Used capacity	Capacity in use by the file system in the internal flash memory user area: Used capacity in the user area config area: Used capacity in the configuration area dump area: Used capacity in the dump area area total: Total of each used capacity in the user area, configuration area, and dump area
	free	Unused capacity	Capacity not being used by the file system in the internal flash memory user area: Unused capacity in the user area config area: Unused capacity in the configuration area dump area: Unused capacity in the dump area area total: Total of each unused capacity in the user area, configuration area, and dump area
	total	Total capacity	Total of capacity being used and capacity not being used for the file system in the internal flash memory user area: Total of used and unused capacity in the user area config area: Total of used and unused capacity in the configuration area dump area: Total of used and unused capacity in the dump area area total: Total capacity being used and not being used by the file system in the internal flash memory

Impact on communication

None

Notes

- This command shows the used and unused capacity secured by the file system in the internal flash memory.
- Even if the devices have the same model names, the used capacity of their internal flash memory might be different.

11 Resource Information

show cpu

Shows CPU usage.

Syntax

```
show cpu { days [hours] [minutes] [seconds]
                        | hours [days] [minutes] [seconds]
                        | minutes [days] [hours] [seconds]
                        | seconds [days] [hours] [minutes] } [detail]
```

Input mode

User mode and administrator mode

Parameters

{ days [hours] [minutes] [seconds] | hours [days] [minutes] [seconds] | minutes [days] [hours] [seconds] | seconds [days] [hours] [minutes] }

days

Displays statistics collected daily. Statistics for the past month are displayed.

hours

Displays statistics collected hourly. Statistics for the past day are displayed.

minutes

Displays statistics collected by the minute. Statistics for the past hour are displayed.

seconds

Displays statistics collected by the second. Statistics for the past minute are displayed.

Behavior when each parameter is omitted:

This command displays only the information that meets the condition of the specified parameters. If you do not specify a parameter, information for the conditions specified by the parameter will not be displayed.

Behavior when all parameters are omitted:

You cannot omit all of the parameters.

detail

Displays statistics for each CPU core.

Behavior when this parameter is omitted:

Statistics on all cores of each CPU are collected and displayed altogether on a CPU basis.

Example and display items

Figure 11-1: Specifying the days parameter

```
> show cpu days
Date 20XX/12/13 14:15:37 UTC
*** day ***
date    time              cpu average
Dec 10  16:00:00-23:59:59     5
Dec 11  00:00:00-23:59:59     4
Dec 12  00:00:00-23:59:59    25
>
```

Figure 11-2: Specifying the days parameter (with the detail parameter specified)

```
> show cpu days detail
Date 20XX/04/01 00:34:12 UTC
*** day ***
                              cpu average
date    time                  CPU[0]  CPU[1]
Mar 13  09:20:18-23:59:59        5       4
Mar 14  00:00:00-23:59:59        4       4
Mar 15  00:00:00-23:59:59       25      30
     :
Mar 29  00:00:00-23:59:59        3       4
>
```

Table 11-1: Information displayed when the days parameter is specified

Item	Displayed information
cpu average	The average CPU utilization within the time range indicated under time

Figure 11-3: Specifying the hours parameter

```
> show cpu hours
Date 20XX/09/13 14:15:37 UTC
*** hour ***
date    time              cpu average
Dec 13  15:00:00-16:59:59     6
                    :
Dec 13  23:00:00-23:59:59     7
Dec 13  00:00:00-00:59:59    10
Dec 13  01:00:00-01:59:59    20
                    :
                    :
Dec 13  14:00:00-14:59:59     3
>
```

Table 11-2: Information displayed when the hours parameter is specified

Item	Displayed information
cpu average	The average CPU utilization within the time range indicated under time

Figure 11-4: Specifying the minutes parameter

```
> show cpu minutes
Date 20XX/12/13 14:15:37 UTC
*** minute ***
date    time              cpu average
Dec 13  14:42:00-14:42:59     6
Dec 13  14:43:00-14:43:59    20
                    :
                    :
Dec 13  15:41:00-15:41:59    10
>
```

Table 11-3: Information displayed when the minutes parameter is specified

Item	Displayed information
cpu average	The average CPU utilization within the time range indicated under time

Figure 11-5: Specifying the seconds parameter

```
> show cpu seconds
Date 20XX/12/13 14:44:15 UTC
*** second ***
date    time                  cpu average
Dec 13  14:43:14-14:43:23    20  10   5   4  70   9  80  30   7  50
```

```
Dec 13  14:43:24-14:43:33    10   9  40  40   7   4   6  10   7   4
Dec 13  14:43:34-14:43:43    20  10   5   4  52   9  80  30   7  50
Dec 13  14:43:44-14:43:53    10   9  40  40   7   4   6  10   7   4
Dec 13  14:43:54-14:44:03    20  10   5   4  63   9  80  30   7  50
Dec 13  14:44:04-14:44:13    10   9  40  40   7   4   6  10   7   4
>
```

Figure 11-6: Specifying the seconds parameter (with the detail parameter specified)

```
> show cpu seconds detail
Date 20XX/04/01 00:34:12 UTC
*** second ***
                    cpu average
date    time        CPU[0]  CPU[1]
Mar 13  14:43:14       5       4
Mar 13  14:43:15       4       4
Mar 13  14:43:16      25      30
     :
Mar 13  14:44:13       3       4
>
```

Table 11-4: Information displayed when the seconds parameter is specified

Item	Displayed information
cpu average	The CPU utilization per second within the time range indicated under time

Impact on communication

None

Notes

None

show processes

Shows information about processes being executed by the device.

Syntax

```
show processes memory
show processes cpu
```

Input mode

User mode and administrator mode

Parameters

memory

Shows the memory usage of processes with a higher priority that are being executed by the device.

cpu

Shows the CPU usage of processes with a higher priority that are being executed by the device.

Example 1

Show memory usage of processes with a higher priority.

Figure 11-7: Displaying the memory usage of processes

```
> show processes memory
Date 20XX/01/01 12:00:00 UTC
  PID From                              Text   Data Stack  Real Process
 2493 ??                                1432  28240   180 24696 nimd
 5676 console                            788    712   132  3024 sh
 6101 console                           4412    548   132  3896 cli
 6105 console                             16    504   132   360 process
      :
      :
      :
>
```

Display items in Example 1

Table 11-5: Descriptions on the memory-related items displayed when the show processes command is executed

Item	Displayed information	Displayed detailed information
PID	Process number	Displays the process management number for each process.
From	Input terminal	console Management terminal connected to the serial port on the device IP address IP address of a remotely connected terminal ?? No terminal associated with this process
Text	Text size	Shows the text size of each running process in KB.
Data	Data size	Shows the size of the data area for each running process in KB.

Item	Displayed information	Displayed detailed information
Stack	Stack size	Shows the amount of stack usage for each running process in KB.
Real	Real memory usage	Shows the size of real memory usage for each running process in KB.
Process	Function name	Shows the function name of each running process.

Example 2

Show CPU usage of processes with a higher priority.

Figure 11-8: Displaying the CPU usage of processes

```
> show processes cpu
Date 20XX/01/01 12:00:00 UTC
  PID  LWP CPUID   %CPU Runtime(ms) Process(lwp)
    1    1     1  6.56%         2405 systemd
    2    2     1     0%            0 kthreadd
    3    3     0     0%            1 ksoftirqd/0
    5    5     0     0%            0 kworker/0:0H
    6    6     0     0%            2 kworker/u4:0
    7    7     1     0%            2 rcu_sched
    :
    :
    :
>
```

Display items in Example 2

Table 11-6: Descriptions on the CPU-related items displayed when the show processes command is executed

Item	Displayed information	Displayed detailed information
PID	Process number	Displays the process management number for each process.
LWP		
CPUID	Core number	Shows the core number of the core for each running process.
%CPU	CPU usage	Shows the CPU usage of each running process in percentages.
Runtime(ms)	Actual run time of CPU	Shows actual CPU run time for each running process in milliseconds.
Process(lwp)	Function name	Shows the function name of each running process.

Impact on communication

None

Notes

None

show memory

Shows information about the amount of memory being used by the device.

Syntax

```
show memory
```

Input mode

User mode and administrator mode

Parameters

None

Example

Display the installed capacity, used capacity, and free capacity of the physical memory of the device.

Figure 11-9: Displaying the information about the physical memory being used

```
> show memory
Date 20XX/01/23 12:00:00 UTC
    physical memory = 2,020,398KB( 1,973MB)
    used     memory     652,148KB(   636MB)
    free     memory = 1,368,250KB( 1,336MB)
>
```

Display items

Table 11-7: Information displayed by the show memory command

Item	Displayed information
physical memory	Displays the installed capacity of physical memory in KB and MB.
used memory	Displays the used capacity of physical memory in KB and MB.
free memory	Displays the free capacity of physical memory in KB and MB.

Impact on communication

None

Notes

None

df

Shows the available disk space.

Syntax

```
df [<option>] [<file name>]
```

Input mode

User mode and administrator mode

Parameters

<option>

-t: Specifies the type of file system.

<file name>

Displays information about the file system in which this file or directory exists.

Example and display items

None

Impact on communication

None

Notes

None

du

Shows the amount of space being used by the files in a directory.

Syntax

```
du [<option>] [<file name>]
```

Input mode

User mode and administrator mode

Parameters

<option>

-s: Displays only the total number of blocks.

<file name>

Displays information about this file or directory.

Example and display items

None

Impact on communication

None

Notes

None

12 Dump Information

erase dumpfile

Deletes dump files stored in the dump file storage directory.

The dump file storage directory is "/dump" and "/usr/var/hardware".

Syntax

```
erase dumpfile { all | <file name> }
```

Input mode

User mode and administrator mode

Parameters

all

Specifies all dump files.

<file name>

Specifies the name of a file to be deleted. The permissible format of the file name is shown below. # represents a number in the range from 0 to 9.

- "rmdump": Memory dump file
- "osdump": OS dump file
- "ni##.###": NIF failure dump file

Example

Figure 12-1: Deleting all the dump files

```
> erase dumpfile all
```

Figure 12-2: Deleting the memory dump file (rmdump)

```
> erase dumpfile rmdump
```

Impact on communication

None

Notes

None

show dumpfile

Lists the dump files stored in the dump file storage directory.

Syntax

```
show dumpfile
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 12-3: Displaying a dump file

```
> show dumpfile
Date 20XX/07/16 15:17:50 UTC
  [/dump]:
    File Name           osdump
    Date                20XX/07/16 13:57:03
    Version             1.0
    Serial No           xxxxxxxxxxxxxxxxx
    Factor              xxxx xxxxxxxx

    File Name           rmdump
    Date                20XX/07/16 13:57:03
    Version             1.0
    Serial No           xxxxxxxxxxxxxxxxx
    Factor              xxxx xxxxxxxx

  [/usr/var/hardware]:
    No dump file.

>
```

Display items

Table 12-1: Information displayed by the show dumpfile command

Item	Displayed information	Displayed detailed information
File Name	File name	Dump file name
Date	Dump collection date	Date and time of the dump file collection
Version	Version information	Software version
Serial No.	Serial number	Serial number
Factor	Reason for collecting dump	xxxx xxxxxxxx: Error description User operation: A dump is collected by user operation.

Note 1: If there is no dump information in the dump file storage directory, "No dump file." is displayed.

Note 2: If loading a dump file fails, a blank is displayed.

Impact on communication

None

Notes

When the displayed content is for rmdump or osdump, the dump collection date (Date) is displayed in UTC time. Instead, internal management information, which indicates software type, is displayed in the version information.

13 Memory Card Operation Mode

set mc-configuration

Enables or disables the memory card operation mode.

Syntax

```
set mc-configuration {enable | disable}
```

Input mode

Administrator mode

Parameters

{enable | disable}

enable

Enables the memory card operation mode.

disable

Disables the memory card operation mode.

Example

Figure 13-1: Enabling the memory card operation mode

```
# set mc-configuration enable
Do you wish to continue? (y/n): y
#
```

Display items

None

Impact on communication

None

Notes

1. When a memory card is inserted while the memory card operation mode is enabled, the "update mc-configuration" command is executed automatically.

update mc-configuration

Outputs device information and information about active applications to a memory card.

Syntax

```
update mc-configuration
```

Input mode

Administrator mode

Parameters

None

Example

Figure 13-2: Outputting device information and information about applications to the memory card

```
# update mc-configuration
#
```

Display items

None

Impact on communication

If the monitoring time or sending interval of the Layer 2 protocol is set shorter than the initial value on neighboring devices, communication might be interrupted when the connection over the Layer 2 protocol is disconnected.

Notes

1. Do not insert or remove the memory card while this command is being executed.
2. It may take several tens of seconds to several minutes for this command to complete.
3. This command cannot be executed concurrently by multiple users. If they attempt to do so, the command terminates abnormally, and the following message is displayed: MC is busy. Wait a while, and then re-execute the command. If the command still terminates abnormally, execute "`rm/tmp/updatemc.exec`" to delete the file, and then re-execute the command.

14 Software Management

ppupdate

Updates the current software in flash memory with new software, which is downloaded via FTP or a similar method.

Syntax

```
ppupdate [test] [no-display] [-f] [no-reload] <file-name>
```

Input mode

Administrator mode

Parameters

test

Performs a check by simulating command execution. The software is not actually updated.

no-display

Does not display the message output when the command is executed.

-f

Forces the processing without displaying confirmation messages when the command is executed.

Behavior when this parameter is omitted:

A confirmation message is displayed.

no-reload

When the update is complete, the device is not automatically restarted. Instead, the device starts up with the new software next time the device is restarted.

<file-name>

Specifies the update file name.

Example

List the current software version and the new software version, and display a confirmation message.

```
# ppupdate k.img

Software update start

Broadcast message from operator@ (somewhere) (Wed Jul 14 15:32:20 20XX):

*******************************************
** UPDATE IS STARTED.                    **
*******************************************

Current version is 1.0
New version is 1.1
Automatic reboot process will be run after installation process.
Do you wish to continue? (y/n) y
```

If you enter "y", the system starts update processing. After the processing finishes, the system automatically restarts the switch.
If you enter "n", the system displays the command prompt without starting update processing.

Display items

None

Impact on communication

If the test parameter or the no-reload parameter is not specified, the device is automatically restarted after the update finishes. During the restart, communication is temporarily suspended.

Notes

1. When updating is performed, the configuration in effect before the update is inherited. Note that, when the inherited configuration includes a configuration that is not supported by the updated software version, the unsupported configuration command is not inherited. At this time, the startup configuration and running configuration do not match. Therefore, a prompt indicating that the configuration has not been saved is displayed until a save operation is performed. In addition, unsupported configuration commands that are not inherited are output as operation log entries. For details, see "Message Log Reference, 2.5 CONFIG".
2. If many configurations are set and software is updated, device startup might take some time because the configurations are inherited to the new version.
3. Where a memory card that contains the software image file k.img is mounted in the device, the device boots from the memory card when it is restarted. If you do this, the account and configuration information revert to the factory defaults and you cannot save your own settings. Avoid using this method under normal circumstances.
4. This command cannot be executed while the "ppupdate" or "restore" command is executed by another user. If you attempt to do so, the command terminates abnormally, and the following message is displayed: another user is executing now. Wait a while, and then re-execute the command. If the command still terminates abnormally, execute "`rm /tmp/ppupdate.exec`" to delete files, and then re-execute the command.
5. When this command is executed while the memory card operation mode is enabled, the "update mc-configuration" command is also executed automatically (except for when the test parameter is specified). Therefore, the operation log of the "update mc-configuration" command is collected. For details about the operation log, see "Message Log Reference". Note that even if an error is detected in the "update mc-configuration" command, this command is ended successfully.
6. When you execute this command while the memory card operation mode is enabled, we recommend that you specify the no-reload parameter upon the command execution.

   If the no-reload parameter is not specified, the device will restart without updating the device information and information about applications in the memory card when an error occurs during processing of the "update mc-configuration" command. Therefore, the device will start with the states of the applications and the device as they were before this command was executed.

   If an error occurs while the "update mc-configuration" command is being processed during execution of this command with the no-reload parameter specified, execute the "update mc-configuration" command manually to update the device information and the information about applications in the memory card and then restart the device.
7. If the "hostname" configuration command is used to specify a device name of eight characters or more in length, you can only see up to the 79th character of the name in the Broadcast message item displayed on the user terminal when this command is executed.

set license

Registers an optional license onto the Switch.

Syntax

```
set license {key-file <file name> | key-code <license key>}
```

Input mode

Administrator mode

Parameters

key-file <file name>

Specifies the file for the optional license.

key-code <license key>

Specifies the license key for the optional license. The license key consists of 32 characters within the range from 0 to 9 and from a to f (lower-case letters), and a hyphen is placed between every 4 digits in the license key.

Example

- Example of specifying a file name (In this example, the file addopt.dat is specified as a license key file.)

```
# set license key-file addopt.dat
#
```

- Example of specifying a license key (In this example, 0123-4567-89ab-cdef-0123-4567-89ab-cdef is specified as a license key.)

```
Specifying a license key with hyphens as a delimiter:
#set license key-code 0123-4567-89ab-cdef-0123-4567-89ab-cdef

Specifying a license key without hyphens:
#set license key-code 0123456789abcdef0123456789abcedf
```

Display items

None

Impact on communication

None

Notes

The applied license key takes effect after the device is restarted.

show license

Shows optional licenses.

Syntax

```
show license
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 14-1: Showing the optional licenses

```
> show license
Date 20XX/01/23 12:00:00 UTC
  Available: OP-ULTG
    Serial Number        Licensed software
    1600-0001-0200-0000  OP-ULTG(AX-P2340-F21)
>
```

Display items

Table 14-1: Information displayed by the show license command

Item	Displayed information	Displayed detailed information
Available:	Abbreviated name of the optional license enabled	—
Serial Number	Serial number of the optional license registered	—
Licensed software	Abbreviated name of the optional license registered in the Switch (with the model name in parentheses)	"unknown(-----)" is displayed when the software name is unknown.

Impact on communication

None

Notes

None

erase license

Erases the specified optional license.

Syntax

```
erase license <serial no.>
```

Input mode

Administrator mode

Parameters

<serial no.>

Specifies the serial number to be deleted. The serial number consists of 16 characters within the range from 0 to 9 and from a to f (lower-case letters), and a hyphen is placed every 4 digits of the serial number.

Example

Figure 14-2: Deleting an optional license

```
# erase license 1600-0001-0200-0000


This serial number enable OP-ULTG
Erase OK? (y/n)

If you enter "y" here, the optional license is deleted.
If you enter "n" here, the optional license is not deleted, and the command prompt is displayed.
```

Display items

None

Impact on communication

None

Notes

The deleted license key is no longer valid when the device is restarted.

15 Power Saving Functions

show power

Shows the maximum power consumption information of the device.

Syntax

```
show power
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 15-1: Result of executing the show power command

```
>show power
Date 20XX/09/21 12:00:00 UTC
H/W       Maximum Wattage
Chassis           45.00 W
>
```

Display items

Table 15-1: Information displayed by the show power command

Item	Displayed information	Displayed detailed information
H/W	Parts information	Shows the information about the device.
Maximum Wattage	Maximum power consumption	Shows the maximum power consumption of the Switch. This is displayed in watts.

Impact on communication

None

Notes

- The power consumption information displayed by this command is equal to the result value of the command execution.

16 Log

show logging

Shows the log entries recorded by the Switch.

This command handles two types of logs, operation logs and reference logs, which are displayed or controlled independently. The operation logs consist of entered command strings, command response messages, and various event messages. The reference logs contain statistics obtained by compiling events that occurred for each code.

For details about the information displayed as a command execution result, see "Message Log Reference".

Syntax

```
show logging [<kind>] [<command classification>] [count <count>]
```

Input mode

User mode and administrator mode

Parameters

<kind>

reference

Specifies the reference log.

script-only

Displays operation log entries of message types SKY and SRS.

script-include

Displays operation log entries of all message types.

Behavior when this parameter is omitted:

Operation log entries, excluding message types SKY and SRS, are displayed.

<command classification>

-h

Displays log entries with no header information (System Information). System Information indicates the device model and software information.

Behavior when this parameter is omitted:

Log entries with header information (System Information) are displayed.

count <count>

Displays the specified number of operation log entries in the latest operation log. The specifiable value for <count> is from 1 to 12000. If the <kind> parameter is specified with the reference option together, this parameter will be ignored even if specified.

Behavior when this parameter is omitted:

Six-thousand (6000) operation log entries in the latest operation log are displayed.

Behavior when all parameters are omitted:

The command works as described in each "Behavior when this parameter is omitted" section.

Example

- Display the operation log entries for the device.

```
> show logging
```

Figure 16-1: Displaying operation logs

```
> show logging
Date 20XX/12/25 14:14:18 UTC
System Information
    AX2340S-48T4X, OS-L2N Ver. 1.0 (Build:xx)
Logging Information
KEY 20XX/12/24 12:37:30 operator(pts/0):# ping 192.111.214.10
     :
     :
     :
>
```

- Display the reference log entries for the device.

```
> show logging reference
```

Figure 16-2: Displaying reference logs

```
> show logging reference
Date 20XX/12/25 14:14:18 UTC
System Information
    AX2340S-48T4X, OS-L2N Ver. 1.0 (Build:xx)
Logging Information
E3 SOFTWARE 01900250 1001:000000000000
  20XX/12/23 14:12:10    20XX/12/23 14:12:10    1
     :
     :
     :
>
```

Display items

None

Impact on communication

None

Notes

- Log information is obtained at the UTC time immediately after the device is started.
- The operation log entries are displayed in reverse chronological order from the latest message or operation (the latest information is displayed at the top). Note that the reboot reason log entry of the device appears after the startup log entry, but its timestamp is earlier than that of the startup log entry. If several log entries are generated at the same time, those log entries might not be displayed in reverse chronological order.
- The reference log entries are collected for each event in chronological order. However, the order in which command execution results are displayed is not always in chronological order because the information about events that have occurred is grouped by event type.

clear logging

Erases the log entries recorded by the Switch.

Syntax

```
clear logging [<kind>]
```

Input mode

User mode and administrator mode

Parameters

<kind>

reference

Specifies the reference log.

Behavior when this parameter is omitted:

Specifies the operation log.

Example

Figure 16-3: Erasing operation logs

```
> clear logging
```

Figure 16-4: Erasing reference logs

```
> clear logging reference
```

Display items

None

Impact on communication

None

Notes

None

show logging console

Shows the event level at which screen displays are suppressed, set by the "set logging console" command. The command is applied to operation messages of message types ERR and EVT.

Syntax

```
show logging console
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 16-5: Enabling the display of operation messages on the screen

```
> show logging console
  Date 20XX/12/25 14:14:18 UTC
  System message mode : Display all
```

Figure 16-6: Suppressing the display of operation messages at event level E6 or lower

```
> show logging console
  Date 20XX/12/25 14:14:18 UTC
  System message mode : E6
```

Display items

None

Impact on communication

None

Notes

None

set logging console

Controls the display of operation messages by event level. The command is applied to operation messages of message types ERR and EVT. Low-priority operation messages that might be displayed frequently due to system configuration changes can be suppressed.

Syntax

```
set logging console { disable <event level> | enable }
```

Input mode

User mode and administrator mode

Parameters

{ disable <event level> | enable }

disable <event level>

Specifies an event level (E3 to E9); operation messages related to events at this specified level and lower levels will not be displayed. It also suppresses recovery operation messages corresponding to the specified event level.

enable

Specifies that all operation messages will be displayed.

Example

Figure 16-7: Enabling operation messages to be displayed on the screen

```
> set logging console enable
```

Figure 16-8: Suppressing the display of operation messages at event level E5 or lower

```
> set logging console disable E5
```

Display items

None

Impact on communication

None

Notes

None

17 SNMP

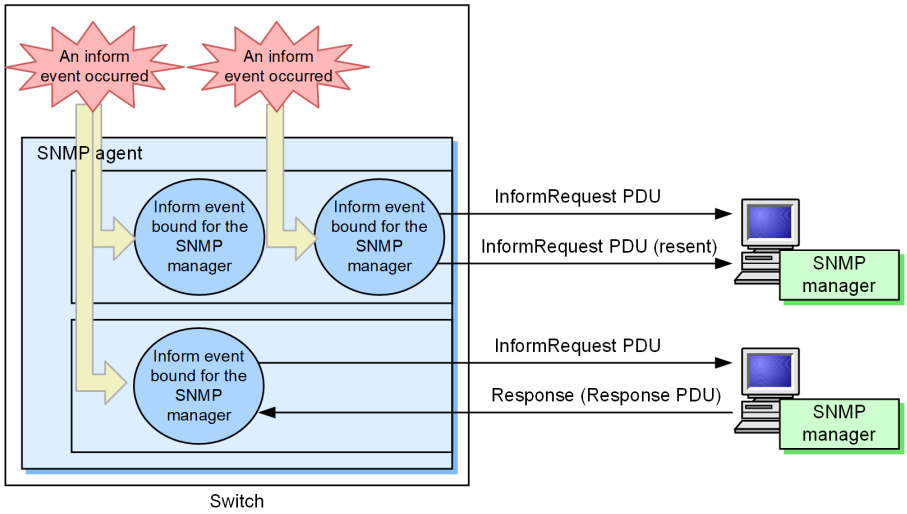
show snmp

Shows SNMP information.

For inform requests, information is displayed for each of the following units:

- Inform event
- Inform event bound for the SNMP manager
- InformRequest PDU

Figure 17-1: Informed request information



Syntax

```
show snmp
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 17-2: Example of executing the show snmp command

```
> show snmp
Date 20XX/12/27 15:06:08 UTC
Contact: Suzuki@example.com
Location: ServerRoom
SNMP packets input   : 137    (get:417 set:2)
    Get-request PDUs    : 18
    Get-next PDUs       : 104
    Get-bulk PDUs       : 0
    Set-request PDUs    : 6
    Response PDUs       : 3    (with error 0)
    Error PDUs          : 7
        Bad SNMP version errors: 1
        Unknown community name : 5
```

```
        Illegal operation      : 1
        Encoding errors        : 0

SNMP packets output : 185
    Trap PDUs           : 4
    Inform-request PDUs : 11
    Response PDUs       : 128    (with error 4)
        No errors              : 124
        Too big errors         : 0
        No such name errors    : 3
        Bad values errors      : 1
        General errors         : 0
    Timeouts            : 8
    Drops               : 0

[TRAP]
    Host: 192.168.0.1, sent:1
    Host: 192.168.0.2, sent:3

[INFORM]
    Timeout(sec)       : 10
    Retry              : 5
    Pending informs    : 1/25 (current/max)
    Host: 192.168.0.3
        sent    :8
        response:2          pending:1          failed:5          dropped:0
    Host: 192.168.0.4
        sent    :3
        response:0          pending:0          failed:3          dropped:0
    Host: 2001:db8::10
        sent    :1
        response:1          pending:0          failed:0          dropped:0
```

Display items

Table 17-1: Information displayed when the show snmp command is executed

Item	Meaning	Displayed detailed information
Contact	Indicates the contact information of the Switch.	Value set by the "snmp-server contact" configuration command
Location	Indicates the name of the location where the Switch is installed.	Value set by the "snmp-server location" configuration command
SNMP packets input	Indicates the snmpInPkts value (total number of received SNMP messages).	
get	Indicates the snmpInTotalReqVars value (total number of MIB objects for which a MIB was successfully collected).	—
set	Indicates the snmpInTotalSetVars value (total number of MIB objects for which a MIB was successfully configured).	—
Get-request PDUs	Indicates the snmpInGetRequests value (total number of received GetRequest PDUs).	—
Get-next PDUs	Indicates the snmpInGetNexts value (total number of received GetNextRequest PDUs).	—
Get-bulk PDUs	Indicates the total number of received GetBulkRequest PDUs.	0 to 4294967295

Item	Meaning	Displayed detailed information
Set-request PDUs	Indicates the snmpInSetRequests value (total number of received SetRequest PDUs).	—
Response PDUs	Indicates the snmpInGetResponses value (total number of received GetResponse PDUs).	—
with error	Indicates the number of PDUs of the received GetResponse PDUs whose error status is not noError.	0 to 4294967295
Error PDUs	Indicates the total number of errors that occurred in PDU reception processing.	0 to 4294967295
Bad SNMP version errors	Indicates the snmpInBadVersions value (total number of received messages whose version is not supported).	—
Unknown community name	Indicates the snmpInBadCommunityNames value (total number of received SNMP messages from unknown communities).	—
Illegal operation	Indicates the snmpInBadCommunityUses value (total number of received messages that indicate operations that are not permitted by the specified community).	—
Encoding errors	Indicates the snmpInASNParseErrs value (total number of received ASN.1 error messages).	—
SNMP packets output	Indicates the snmpOutPkts value (total number of sent SNMP messages).	
Trap PDUs	Indicates the snmpOutTraps value (total number of sent Trap PDUs).	—
Inform-request PDUs	Indicates the total number of sent Inform-request PDUs.	0 to 4294967295
Response PDUs	Indicates the snmpOutGetResponses value (total number of sent GetResponse PDUs).	—
with error	Indicates the number of PDUs of the sent GetResponse PDUs whose error status is not noError.	0 to 4294967295
No errors	Indicates the total number of sent PDUs whose error status is noError.	0 to 4294967295
Too big errors	Indicates the snmpOutTooBigs value (total number of sent PDUs whose error status is tooBig).	—
No such name errors	Indicates the snmpOutNoSuchNames value (total number of sent PDUs whose error status is noSuchName).	—
Bad values errors	Indicates the snmpOutBadValues value (total number of sent PDUs whose error status is badValue).	—
General errors	Indicates the snmpOutGenErrs value (total number of sent PDUs whose error status is genErr).	—
Timeouts	Indicates the total number of InformRequest PDUs for which a timeout occurred.	0 to 4294967295

Item	Meaning	Displayed detailed information
Drops	Indicates the total number of inform events that were bound for the SNMP manager but were discarded because, for example, the maximum number of inform events that can wait for a response was exceeded.	0 to 4294967295
[TRAP]	Indicates trap information.	
Host	Indicates the host to which the trap is sent.	Value set by the <manager address> parameter of the "snmp-server host" configuration command
sent	Indicates the number of times a trap was sent.	0 to 4294967295
[INFORM]	Indicates inform event information.	
Timeout(sec)	Indicates the timeout value (in seconds).	Value set by the timeout parameter of the "snmp-server informs" configuration command
Retry	Indicates the number of resending attempts that has been set.	Value set by the retries parameter of the "snmp-server informs" configuration command
Pending informs : <current>/<max>	Indicates the number of informs and the maximum number of them. An inform is held until the SNMP manager respond or a timeout occurs. <max> may be temporarily exceeded when the inform is sent for the first time.	<current>: Number of informs that are currently held. <max>: Value set by the pending parameter of the "snmp-server informs" configuration command.
Host	Indicates the inform event destination.	Value set by the <manager address> parameter of the "snmp-server host" configuration command
sent	Indicates the number of sent informs bound for the SNMP manager that sent InformRequest PDUs.	0 to 4294967295
response	Indicates the number of responses from the SNMP manager to informs bound for the SNMP manager.	0 to 4294967295
pending	Indicates the number of informs bound for the SNMP manager that is waiting for a response from another SNMP manager.	0 to 4294967295
failed	Indicates the number of times sending of an inform bound for the SNMP manager failed. Sending fails if there is no response after repeated resend attempts.	0 to 4294967295
dropped	Indicates the number of informs that were bound for the SNMP manager but were discarded because, for example, the maximum number of informs that can wait for a response was exceeded.	0 to 4294967295

Impact on communication

None

Notes

1. The Switch supports a set of snmp operation commands that have the functions equivalent to the SNMP

agent and SNMP manager. The statistics displayed by this command pertain to SNMP agents only, and do not pertain to snmp operation commands.

2. In the statistics displayed by this command, the number of messages and PDUs are counted in the same way as when MIBs are acquired from a network SNMP manager. This is true even when MIBs are acquired by using snmp operation commands.
3. If an inform event bound for the SNMP manager occur after a coldStart inform event is sent when the device starts, any inform events bound for the SNMP manager that occurred before the response to the coldStart inform event is received are held for a while without being sent soon. The inform events bound for SNMP manager that have not yet been sent are temporarily counted as sent and pending events.

show snmp pending

Displays inform events bound for the SNMP manager that is waiting for a response from the SNMP manager.

Syntax

```
show snmp pending
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 17-3: Example of executing the show snmp pending command

```
> show snmp pending
Date 20XX/12/27 15:06:10 UTC
Req ID: 48, Dest: 192.168.0.1, Remaining Retry: 2, Expires in seconds: 3
Req ID: 49, Dest: 192.168.0.2, Remaining Retry: 4, Expires in seconds: 3
Req ID: 50, Dest: 192.168.0.3, Remaining Retry: 2, Expires in seconds: 7
Req ID: 51, Dest: 192.168.0.4, Remaining Retry: 4, Expires in seconds: 7
Req ID: 52, Dest: 2001:db8::10, Remaining Retry: 10, Expires in seconds: 30
```

Display items

Table 17-2: Information displayed when the show snmp pending command is executed

Item	Meaning	Displayed detailed information
Req ID	Request ID	—
Dest	Destination SNMP manager	Value set by the <manager address> parameter of the "snmp-server host" configuration command
Remaining Retry	Remaining number of retries	0 to 100 If the value of this item is 0, whether a response is made is checked, but no resend attempts are performed.
Expires in seconds	Remaining time before the session times out	0 to 21474835 (seconds)

Impact on communication

None

Notes

If this command is executed when inform events bound for the SNMP manager time out simultaneously, the command might display 0 for all sessions as the remaining time before a timeout (as shown in the following example).

Example

```
> show snmp pending
Date 20XX/12/27 17:06:10 UTC
```

```
Req ID: 88, Dest: 192.168.0.1, Remaining Retry: 0, Expires in seconds: 0
Req ID: 89, Dest: 192.168.0.2, Remaining Retry: 0, Expires in seconds: 0
Req ID: 90, Dest: 192.168.0.3, Remaining Retry: 0, Expires in seconds: 0
```

snmp lookup

Shows supported MIB object names and object IDs.

Syntax

```
snmp lookup [<variable name>]
```

Input mode

User mode and administrator mode

Parameters

<variable name>

Specifies an object name, or an object in dot notation.

A list of object names that follow the specified object or objects in dot notation are displayed.

Behavior when this parameter is omitted:

All object names are listed in dot notation.

Example

Figure 17-4: Example of executing the snmp lookup command

```
> snmp lookup sysDescr
  sysDescr                                = 1.3.6.1.2.1.1.1

> snmp lookup
iso                                       = 1
org                                       = 1.3
dod                                       = 1.3.6
internet                                  = 1.3.6.1
mgmt                                      = 1.3.6.1.2
```

Display items

Supported MIB object names and object IDs are displayed in the <object name> = <object ID> format.

Impact on communication

None

Notes

None

snmp get

Shows the specified MIB value.

Syntax

```
snmp get <variable name>
```

Input mode

User mode and administrator mode

Parameters

<variable name>

Specifies an object name, or an object in dot notation.

The command searches for management information of the specified object instance to display it.

Example

Figure 17-5: Example of executing the snmp get command

```
> snmp get sysUpTime.0

Name: sysUpTime.0
Value: 1296584

> snmp get 1.3.6.1.2.1.1.3.0

Name: sysUpTime.0
Value: 1308889
```

Display items

Table 17-3: Information displayed when the snmp get command is executed

Item	Meaning	Displayed detailed information
Name	Object instance	—
Value	Object instance value	—

Impact on communication

None

Notes

1. For five minutes immediately after the power is turned on or the "copy" command is used to copy the backup configuration file to the startup configuration file, the No response message appears because the SNMP agent is being initialized.
2. If the "snmp-server community" configuration command is not set, the No response message appears and the MIB cannot be acquired.

snmp getnext

Shows the MIB value following the specified one.

Syntax

```
snmp getnext <variable name>
```

Input mode

User mode and administrator mode

Parameters

<variable name>

Specifies an object name, or an object in dot notation.

The command searches for the next management information of the specified object instance to display it.

Example

Figure 17-6: Example of executing the snmp getnext command

```
> snmp getnext sysObjectID.0

Name: sysUpTime.0
Value: 45300
> snmp getnext 1.3.6.1.2.1.1.2.0

Name: sysUpTime.0
Value: 47300
```

Display items

Table 17-4: Information displayed when the snmp getnext command is executed

Item	Meaning	Displayed detailed information
Name	Object instance following the specified one	—
Value	Object instance value following the specified one	—

Impact on communication

None

Notes

1. For five minutes immediately after the power is turned on or the "copy" command is used to copy the backup configuration file to the startup configuration file, the No response message appears because the SNMP agent is being initialized.
2. If there are too many interfaces on the Switch, it takes time to search for IP-related MIB information, and a timeout might occur. If that happens, use the "snmp get" command to acquire the information, or use the "snmp getnext" command to set the instance value and then acquire the information.
3. If the "snmp-server community" configuration command is not set, the No response message appears and the MIB cannot be acquired.

snmp walk

Shows the specified MIB tree.

Syntax

```
snmp walk <variable name>
```

Input mode

User mode and administrator mode

Parameters

<variable name>

Specifies an object name, or an object in dot notation.

The command searches for subsequent management information of the specified object instance, and then displays all instances of the applicable objects.

Example

Figure 17-7: Example of executing the snmp walk command

```
> snmp walk interfaces

Name: ifNumber.0
Value: 4

Name: ifIndex.1
Value: 1

Name: ifIndex.3
Value: 3

Name: ifIndex.10
Value: 10

Name: ifIndex.100
Value: 100

Name: ifDescr.1
Value: loopback

Name: ifDescr.3
Value: VLAN 1 (default) (VLAN0001)

Name: ifDescr.100
Value: GigabitEther 1/0/1
```

Display items

Table 17-5: Information displayed when the snmp walk command is executed

Item	Meaning	Displayed detailed information
Name	Object instance	—
Value	Object instance value	—

Impact on communication

None

Notes

1. For five minutes immediately after the power is turned on or the "copy" command is used to copy the backup configuration file to the startup configuration file, the No response message appears because the SNMP agent is being initialized.
2. If there are too many interfaces on the Switch, it takes time to search for IP-related MIB information, and a timeout might occur. If that happens, use the "snmp get" command to acquire the information, or use the "snmp getnext" command to set the instance value and then acquire the information.
3. If the "snmp-server community" configuration command is not set, the No response message appears and the MIB cannot be acquired.

snmp rget

Shows the MIB value for the specified remote device.

Syntax

```
snmp rget [version { 1 | 2 }] <ip address> <community> <variable name>
```

Input mode

User mode and administrator mode

Parameters

The command remotely accesses an SNMP agent, acquires and displays management information of the specified object instance.

version { 1 | 2 }

Specifies the SNMP version.

Behavior when this parameter is omitted:

The value of 1 is assumed.

<ip address>

Specifies the IP address of the device which is remotely accessed.

<community>

Specifies the community name of the remote device.

<variable name>

Specifies an object name of MIB or an object in dot notation.

Example

Figure 17-8: Example of executing the snmp rget command

```
> snmp rget version 2 192.168.11.35 public sysObjectID.0

Name: sysObjectID.0
Value: ax2340s
```

Display items

Table 17-6: Information displayed when the snmp rget command is executed

Item	Meaning	Displayed detailed information
Name	Object instance following the specified one	—
Value	Object instance value following the specified one	—

Impact on communication

None

Notes

None

snmp rgetnext

Shows the MIB value following the specified remote device.

Syntax

```
snmp rgetnext [version { 1 | 2 }] <ip address> <community> <variable name>
```

Input mode

User mode and administrator mode

Parameters

The command remotely accesses an SNMP agent, acquires and displays management information following the specified object instance.

version { 1 | 2 }

Specifies the SNMP version.

Behavior when this parameter is omitted:

The value of 1 is assumed.

<ip address>

Specifies the IP address of the device which is remotely accessed.

<community>

Specifies the community name of the remote device.

<variable name>

Specifies an object name of MIB or an object in dot notation.

Example

Figure 17-9: Example of executing the snmp rgetnext command

```
> snmp rgetnext version 2 192.168.11.35 public sysObjectID.0

Name: sysUpTime.0
Value: 27603450
```

Display items

Table 17-7: Information displayed when the snmp rgetnext command is executed

Item	Meaning	Displayed detailed information
Name	Object instance following the specified one	—
Value	Object instance value following the specified one	—

Impact on communication

None

Notes

If there are too many interfaces on the target device, it takes time to search for IP-related MIB information, and a timeout might occur. If that happens, use the "snmp rget" command to acquire the information, or use the "snmp rgetnext" command to set the instance value, and then acquire the information.

snmp rwalk

Shows information about the MIB tree for the specified remote device.

Syntax

```
snmp rwalk [version { 1 | 2 }] <ip address> <community> <variable name>
```

Input mode

User mode and administrator mode

Parameters

This command remotely accesses an SNMP agent, and acquires the management information following the specified object instance, and then displays all instances of the applicable object.

version { 1 | 2 }

Specifies the SNMP version.

Behavior when this parameter is omitted:

The value of 1 is assumed.

<ip address>

Specifies the IP address of the device which is remotely accessed.

<community>

Specifies the community name of the remote device.

<variable name>

Specifies an object name of MIB or an object in dot notation.

Example

Figure 17-10: Example of executing the snmp rwalk command

```
> snmp rwalk version 2 192.168.11.35 public ifDescr

Name: ifDescr.1
Value: loopback

Name: ifDescr.3
Value: VLAN 1 (default) (VLAN0001)

Name: ifDescr.10
Value: MGMT0

Name: ifDescr.100
Value: GigabitEther 1/0/1
```

Display items

Table 17-8: Information displayed when the snmp rwalk command is executed

Item	Meaning	Displayed detailed information
Name	Object instance following the specified one	—
Value	Object instance value following the specified one	—

Impact on communication

None

Notes

If there are too many interfaces on the target device, it takes time to search for IP-related MIB information, and a timeout might occur. If that happens, use the "snmp rget" command to acquire the information, or use the "snmp rgetnext" command to set the instance value, and then acquire the information.

18 Advanced Script

python

Starts Python.

Syntax

```
python [<option>] [-W {ignore | default | all | module | once | error}] [{-m <module name> | <f
ile name> | - } [<args>...]]
```

Input mode

Administrator mode

Parameters

<option>

-b (-bb)

Raises a warning when a comparison is made between a string and data in bytes. When the -bb option is specified, an error is caused.

-B

Is a reserved option. It does not take a particular effect on the Switch.

-d

Enables debug output.

-E

Ignores all Python-related environment variables (PYTHON*).

-h (--help)

Shows short descriptions on all command-line options.

-i

Specifies to move to interactive mode, if a script is specified in the first argument, after the script ends.

-O (-OO)

Is a reserved option. It does not take a particular effect on the Switch.

-q

Hides the version at startup in interactive mode.

-R

Specifies to use salt[#1] for hash value generation by hash() as a defense against denial of service attacks. The value set in the PYTHONHASHSEED environment variable is used as salt[#1]. If it is not set, a random value is used.

-s

Does not add the user's site directory to sys.path[#2].

-S

Disables the import of the site module to disable directory-specific sys.path[#2] operations performed by the module.

-u

Is a reserved option. It does not take a particular effect on the Switch.

-v (-vv)

Shows a message indicating where a module was loaded from (file name or built-in module) each time the module is initialized. If the -vv option is specified, a message is displayed for each file that is checked when modules are searched for. The information about module cleanup when the module ends is also displayed.

-V (--version)

Tells the command to show the version number of Python and then exit.

-x

Skips the first line of source code.

-X

Is a reserved option. It does not take a particular effect on the Switch.

Behavior when this parameter is omitted:

The command does not work as described in each parameter of <option>.

-W {ignore | default | all | module | once | error}

Specifies to control how often a warning is raised.

ignore

Ignores all warnings.

default

Explicitly requests the default behavior (to show a warning only once per source-code line).

all

Shows a warning each time it is raised. This option causes a large number of messages if a warning occurs repeatedly on the same source-code line, such as in a loop statement.

module

Shows the first warning that is raised in each module.

once

Shows the first warning that is raised in a program.

error

Raises an exception without showing any warning.

Behavior when this parameter is omitted:

A warning is displayed only once per source-code line.

{-m <module name> | <file name> | - } [<args>...]

-m <module name>

Searches sys.path[#2] for the specified module and executes the module.

<module name> can accept a maximum of 255 characters.

Alphanumeric characters, periods (.), hyphens (-), underscores (_), tildes (~), and carets (^) can be used for <module name>.

The current directory is not searched for display.

<file name>

Executes the specified script file. Specify the path to the file along with the file name. If you omit the file path, the current directory is searched.

<file name> can accept a maximum of 255 characters.

Alphanumeric characters, periods (.), hyphens (-), underscores (_), tildes (~), and carets (^) can be used for <file name>.

Script files that can be specified have the extension of ".py", ".pyc", or ".pyo".

-

Starts Python in interactive mode.

<args>

Specifies arguments to apply to at startup of the script file.

A single argument can accept a maximum of 63 characters.

Alphanumeric and special characters can be used for the argument. For special characters, see "List of character codes". However, double quotation marks ("), single quotation marks ('), semicolons (;), backslashes (\), and grave accent marks (`) cannot be used. Also, a dollar ($) cannot be used for the first character.

A maximum of 32 arguments can be specified. If you specify more than one argument, place a space between the arguments. If you specify a special character, such as a space, in an argument, enclose the argument in double quotation marks (").

Behavior when this parameter is omitted:

Python is started in interactive mode. However, if the -h (--help) option or -V (--version) option is specified for the <option> parameter, the command works as specified by the option.

Behavior when all parameters are omitted:

Python is started in interactive mode.

#1

Salt refers to a string added to the value from which a hash value is generated for the purpose of complicating the hash value.

#2

sys.path is a list of strings of paths that Python uses to search for a module.

Example

The following command shows an example of starting the script file (sample.py) in the current directory:

```
# python sample.py
       :
       :
       :
#
```

The following command shows an example of starting the script module (sample) installed on the device. At startup, pass test as the first argument and 1 as the second argument:

```
# python -m sample test 1
       :
       :
       :
#
```

The following command shows an example of starting Python in interactive mode. You exit the command after confirming Python has started.

```
# python
    Python 3.2.3 (default, Oct 29 20XX, 17:26:20)
    Type "help", "copyright", "credits" or "license" for more information.
    >>>
    >>> quit()
#
```

Display items

The result of executing the script is displayed.

Impact on communication

Running a script that controls communication can affect communication.

Notes

1. A maximum of four scripts can be executed concurrently.
2. Up to eight scripts can be started per second. If this upper limit is exceeded, an error occurs.

stop python

Stops a running Python script. A resident script restarts immediately after stopped.

Syntax

```
stop python [-f] [kill] <pid>
```

Input mode

Administrator mode

Parameters

-f

Executes the command without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

kill

Sends SIGKILL to the running script to forcibly stop it.

Behavior when this parameter is omitted:

The command makes an attempt to stop the script by sending SIGTERM.

<pid>

Specifies the process ID of the script to stop. You can check the process ID with the "show script running-state" command. The specifiable values are from 1 to 30000.

Behavior when all parameters are omitted:

The command works as described in each "Behavior when this parameter is omitted" section.

Example

Figure 18-1: Stopping a running script (PID: 12345)

```
# stop python 12345
Do you want to stop the specified script? (y/n): y
#
```

Display items

None

Impact on communication

None

Notes

None

pyflakes

Checks the syntax of a Python script file.

This command uses a syntax check tool that is available at PyPI (software repository website for Python scripts).

Syntax

```
pyflakes <file name>
```

Input mode

User mode and administrator mode

Parameters

<file name>

Checks the syntax of the specified script file. Specify the path to the file along with the file name.

Alphanumeric characters, periods (.), hyphens (-), underscores (_), tildes (~), and carets (^) can be used for <file name>.

A script file that can be specified has the extension of ".py".

Example

Figure 18-2: Checking the syntax of a script file (sample.py) created according to the Python version 3 syntax

```
> pyflakes ./sample.py
>
```

Figure 18-3: Checking the syntax of a script file (sample.py) created without conforming to the Python version 3 syntax

```
> pyflakes ./sample.py
  ./sample.py:1: invalid syntax
  print "Sample"
                ^
>
```

Display items

If there are no syntax error and warning, the command exits without outputting anything.

If there is a syntax error or warning, the command outputs the following error information:

- File name: Line number: error type
- Error location

Impact on communication

None

Notes

None

install script

Installs a created Python script file in the Switch. Resident scripts and event startup scripts start script files installed by this command.

An installed script file is copied to /config/script/script.file.

The maximum number of files and size limit of script files that can be installed are as follows:

- Number of files: 100 files
- Total size limit of all files: 4 MB
- Size limit per file: 512 KB

Syntax

```
install script <file name>
```

Input mode

Administrator mode

Parameters

<file name>

Installs the specified script file. Specify the path to the file along with the file name. If you omit the file path, the current directory is searched.

<file name>, including the path, can accept a maximum of 255 characters. The maximum number of characters that can be used for the file name of the script file is 99 characters, including the extension.

Alphanumeric characters, periods (.), hyphens (-), underscores (_), tildes (~), and carets (^) can be used for the file name of a script file.

Script files that can be specified have the extension of ".py", ".pyc", or ".pyo".

A script file that differs only in the extension from that of a script file that has already been installed cannot be installed.

Example: If test.py is already installed, both "test.pyc" and "test.pyo" cannot be installed.

Example

Figure 18-4: Installing a script file (testscript.py) in the current directory in the Switch

```
# install script testscript.py
#
```

Display items

None

Impact on communication

None

Notes

1. An already installed script file cannot be overwritten. If you want to change the script file, delete and then reinstall it.

uninstall script

Deletes a Python script file installed in the Switch. If you specify the script file of a running resident script or of a running script triggered by the occurrence of a monitoring event, the applicable process is stopped and then the file is deleted.

Syntax

```
uninstall script [-f] {all | <file name>}
```

Input mode

Administrator mode

Parameters

-f

Executes the command without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

{all | <file name>}

all

Deletes all script files installed in the Switch.

<file name>

Deletes the specified script file. Specify only the file name. A file path cannot be specified.

Alphanumeric characters, periods (.), hyphens (-), underscores (_), tildes (~), and carets (^) can be used for <file name>.

The current directory is not searched for display.

Example

Figure 18-5: Deleting a script file (testscript.py)

```
# uninstall script testscript.py
Do you want to delete the specified script file? (y/n): y
#
```

Display items

None

Impact on communication

None

Notes

None

show script installed-file

Shows information on a Python script file or script files installed in the Switch.

Syntax

```
show script installed-file [<file name>]
```

Input mode

User mode and administrator mode

Parameters

<file name>

Shows the information about the specified script file. Specify only the file name. A file path cannot be specified.

Behavior when this parameter is omitted:

The information about all installed script files is displayed.

Example

Figure 18-6: Displaying the information about all script files

```
> show script installed-file
Date 20XX/10/25 13:39:50 UTC
Total: 3 files, 129931 bytes

name: test1.py
size: 4014 bytes
MD5: 646da9ae6854565766abc96856857d67

name: test2.py
size: 125263 bytes
MD5: 8ef5b45e1f7bead446a5bfa1ebac1620

name: test3.py
size: 654 bytes
MD5: b5210a71ea7c7bcbcb7923a7d471e383
>
```

Figure 18-7: Displaying the information about a script file (test1.py)

```
> show script installed-file test1.py
Date 20XX/10/25 13:40:50 UTC

name: test1.py
size: 4014 bytes
MD5: 646da9ae6854565766abc96856857d67
>
```

Display items

Table 18-1: Information displayed by the show script installed-file command

Item		Displayed information
Total	<value> files	<value>: Number of installed files
	<value> bytes	<value>: Total size of files

Item	Displayed information
name	File name
size	File size
MD5	MD5 hash value

Impact on communication

None

Notes

None

show script running-state

Shows information on running Python scripts.

Syntax

```
show script running-state
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 18-8: Displaying the information about running scripts

```
>show script running-state
Date 20XX/10/25 13:39:50 UTC

[operation command]
  command line args: python /usr/home/operator/script1.py
  PID: 12345
  start time: 20XX/10/25 13:39:01 UTC

[applet]
  applet name: event-monitor
  action sequence: 1
  command line args: python script2.py "100"
  PID: 15432
  start time: 20XX/10/25 13:39:20 UTC

[resident]
  script id: 1
  command line args: python script3.py "abc"
  state: Running
  PID: 10987
  start time: 20XX/10/20 11:00:20 UTC

  script id: 2
  command line args: python script4.py
  state: Not Running(suppression)
  suppression time: 20XX/10/20 19:00:02 UTC

  script id: 3
  command line args: python script5.py
  state: Not Running(no file)
>
```

Display items

Table 18-2: Information displayed by the show script running-state command

Item	Displayed information	Displayed detailed information
[operation command]	Displays the information about command scripts. If there is no running script, "Not Running" is displayed.	
command line args	Command-line argument	Command-line arguments specified when the applicable script is started

Item	Displayed information	Displayed detailed information
PID	Process ID	—
start time	Startup time	—
[applet]	Displays the information about event startup scripts by the applet function. If there is no running script, "Not Running" is displayed.	
applet name	Applet name	—
action sequence	Action sequence number	Sequence number used to manage the execution order of the applicable script, which was set in the configuration
command line args	Command-line argument	Command-line arguments specified when the applicable script is started
PID	Process ID	—
start time	Startup time	—
[resident]	Displays the information about resident scripts. If the configuration has not been set, "Not Configured" is displayed.	
script id	Script ID	Script ID used to manage the applicable script, which was set in the configuration
command line args	Command-line argument	Command-line arguments specified when the applicable script is started
state	Startup status	Running: The script is running. Not Running(suppression): The script is in startup suppression status Not Running(no file): The file is not installed.
PID	Process ID	—
start time	Startup time	—
suppression time	Suppression time	Time when the script is started to be in startup suppression status.

Impact on communication

None

Notes

None

show event manager history

Shows the history of monitoring events occurred.

Syntax

```
show event manager history {applet | script}
```

Input mode

User mode and administrator mode

Parameters

{applet | script}

applet

Displays the history of events being monitored by the applet function.

script

Displays the history of monitoring events registered by a script.

Example 1

Figure 18-9: Displaying the history of events being monitored by the applet function

```
> show event manager history applet
Date 20XX/10/25 12:25:10 UTC
time(event occur)           time(action start)          applet name                type
--------------------------- --------------------------- -------------------------- ----------
20XX/10/25 12:00:00 UTC     20XX/10/25 12:00:00 UTC     every-one-hour             timer
20XX/10/25 11:34:33 UTC     20XX/10/25 11:34:34 UTC     SNMPlog                    sysmsg
20XX/10/25 11:00:00 UTC     20XX/10/25 11:00:00 UTC     every-one-hour             timer
20XX/10/25 10:00:00 UTC     20XX/10/25 10:00:00 UTC     every-one-hour             timer
20XX/10/25 09:00:00 UTC     20XX/10/25 09:00:01 UTC     every-one-hour             timer
20XX/10/25 08:00:00 UTC     20XX/10/25 08:00:01 UTC     every-one-hour             timer
20XX/10/25 07:00:00 UTC     20XX/10/25 07:00:01 UTC     every-one-hour             timer
20XX/10/25 06:12:57 UTC     20XX/10/25 06:12:57 UTC     OSPFlog                    sysmsg
                                 :
                                 :
>
```

Display items in Example 1

Table 18-3: Information displayed by the show event manager history applet command

Item	Displayed information	Displayed detailed information
time(event occur)	Event occurrence time	—
time(action start)	Action execution time	—
applet name	Applet name	—
type	Event type	timer: Timer monitoring sysmsg: Operation message monitoring

Example 2

Figure 18-10: Displaying the history of monitoring events registered by a script

```
> show event manager history script
Date 20XX/10/25 12:25:10 UTC
time                        name                       PID   event ID type
--------------------------- ---------------------- ----- ---------- ----------
20XX/10/05 13:12:57 UTC     sample1.py              2543   16777216 timer
20XX/10/04 23:01:55 UTC     sample1.py              2543   33554432 sysmsg
20XX/10/04 02:00:00 UTC     sample1.py              2543   16777216 timer
20XX/10/03 02:00:00 UTC     sample1.py              2543   16777216 timer
20XX/10/02 10:11:23 UTC     sample2.py             12345   33554433 sysmsg
20XX/10/02 02:00:00 UTC     sample1.py              2543   16777216 timer
20XX/10/01 02:00:00 UTC     sample1.py              2543   16777216 timer
                                :
                                :
>
```

Display items in Example 2

Table 18-4: Information displayed by the show event manager history script command

Item	Displayed information	Displayed detailed information
time	Event occurrence time	—
name	Script file name or module name	File name or module name of the script from which the applicable event is registered or to which the event is notified If the name has 24 characters or more in length, the first 23 characters of the name are shown here. (interactive): Interactive mode
PID	Process ID	Process ID of the script that requested the monitoring of the applicable event
event ID	Event ID	—
type	Event type	timer: Timer monitoring sysmsg: Operation message monitoring

Impact on communication

None

Notes

None

show event manager monitor

Shows monitoring event information.

Syntax

```
show event manager monitor {applet [name <applet name>] | script [pid <pid>]} [type {timer |
sysmsg}] [detail]
```

Input mode

User mode and administrator mode

Parameters

{applet [name <applet name>] | script [pid <pid>]}

applet [name <applet name>]

Displays the information of events being monitored by the applet function.

If name <applet name> is specified, the information of events being monitored by the specified applet is displayed. For <applet name>, specify an apple name with 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.

If name <applet name> is omitted, the information of events being monitored by all applets is displayed.

script [pid <pid>]

Displays the information of monitored events registered by a script.

If pid <pid> is specified, the information of monitored events registered by the script with the specified process ID is displayed. The specifiable value for <pid> is from 1 to 30000.

If pid <pid> is omitted, the information of monitored events registered by all scripts is displayed.

type {timer | sysmsg}

Displays the information of monitoring events of specified event type.

timer

Displays the information of monitoring events of timer monitoring.

sysmsg

Displays the monitoring of monitoring events of operation message monitoring.

Behavior when this parameter is omitted:

The information of monitoring events of all event types is displayed.

detail

Displays detailed information about monitoring events.

Behavior when this parameter is omitted:

Monitoring event information is displayed.

Behavior when all parameters are omitted:

All monitoring event information is displayed.

Example

Figure 18-11: Displaying the information of monitoring events registered using the applet function

```
> show event manager monitor applet
Date 20XX/10/25 12:15:15 UTC
3 event(timer:2, sysmsg:1)
applet name                     type         start time                    detection
------------------------------- ------------ ------------------------- ----------
monitor1                        timer        20XX/10/24 12:03:57 UTC             23
monitor2                        sysmsg       20XX/10/24 12:04:08 UTC              1
monitor3                        timer        (disable)                            0
>
```

Figure 18-12: Displaying the detailed information of monitoring events registered using the applet whose applet name is monitor1

```
> show event manager monitor applet name monitor1 detail
Date 20XX/10/25 12:25:10 UTC
applet name: monitor1
  type: timer
    condition
      cron: "0 * * * *"
    start time: 20XX/10/24 12:03:57 UTC
    statistics
      detection:         23
      discard:            0
  priority: normal
  action
    1 python start.py "monitor1" "timer"
    2 python test.py
    5 python end.py
>
```

Figure 18-13: Displaying the information of monitoring events registered using scripts

```
> show event manager monitor script
Date 20XX/10/25 12:25:10 UTC
3 event(timer:1, sysmsg:2)
  PID name                  event ID type         start time                  detection
----- ------------------- ---------- ------------ -------------------------- ----------
 2543 test1.py              16777216 timer        20XX/10/24 13:12:57 UTC             23
                            33554432 sysmsg       20XX/10/24 13:12:56 UTC              0
12345 test2.py              33554433 sysmsg       20XX/10/24 15:10:01 UTC              1
>
```

Figure 18-14: Displaying the detailed information of monitoring events registered using the script with its process ID of 2543

```
> show event manager monitor script pid 2543 detail
Date 20XX/10/25 12:25:10 UTC
2 event(timer: 1, sysmsg: 1)
PID: 2543
name: test1.py
  event ID: 33554432
    type: timer
    condition
      cron: "0 * * * *"
    notice priority: last
    start time: 20XX/10/24 13:12:57 UTC
    statistics
      detection:         23
      discard
          detector:       0
          script:         0

  event ID: 33554433
    type: sysmsg
    condition
      event level: E7 E8 E9
      event function: "PORT"
    notice priority: normal
    start time: 20XX/10/24 13:12:56 UTC
    statistics
      detection:          0
      discard
          detector:       0
```

```
          script:         0
>
```

Display items

Table 18-5: Information displayed by the show event manager monitor command

Item	Displayed information	Displayed detailed information
Warning	Warning	"System message was discarded before searching. (discard count: <count>, last time: <time>)" <count>: Number of discarded messages <time>: Last time when a message was discarded It is displayed when an operation message is discarded before the operation message is matched with monitoring conditions during operation message monitoring.
<value> event	Number of events	<value>: Number of monitoring events to be displayed[#1]
timer	Timer monitoring count	Number of timer monitoring events to be displayed[#1]
sysmsg	Operation message monitoring count	Number of operation message monitoring events to be displayed[#1]
applet name	Applet name	—
PID	Process ID	—
name	Script file name or module name	When the detail parameter is not specified, the first 19 characters of the name are shown here if the name has 20 characters or more in length.
event ID	Event ID	—
type	Event type	timer: Timer monitoring sysmsg: Operation message monitoring
condition	Monitoring condition[#2]	—
priority notice priority	Notification priority	high: High priority normal: Medium priority low: Low priority last: Lowest priority
start time	Monitoring start time	Time when event monitoring started "(disable)" is displayed when the "disable" configuration command is enabled for event monitoring of the applet function, and "-" is displayed when event monitoring is not started.
statistics	Statistics	—
detection	Event detection count	Number of events detected by the event management function
discard	Event discard count	—
detector	Event discard count details	Number of event occurrence notifications discarded by the monitoring program
script	Event discard count details	Number of event occurrence notifications discarded by a script
action	Registered action	Action sequence number and action registered by the applet

#1: If the number of monitoring events is changed while it is being displayed, it may not match the actual number displayed.

#2: The monitoring conditions shown in the table below are displayed according to the event type.

Table 18-6: Items displayed for the monitoring condition (condition) for each event type

Event type	Item	Displayed information	Displayed detailed information
timer	cron	cron-formatted timer monitoring	Displays the time when the event occurred, in cron format.
	interval	interval-formatted timer monitoring	Displays a time interval in seconds.
sysmsg	message type	Message type	—
	switch no.	Switch number	—
	event level	Event level	R8 to R5, E9 to E3: Event level of monitoring targets If multiple event levels are listed, it means that there are multiple monitoring targets.
	event function	Event location	—
	interface id	Event interface ID	—
	message id	Message ID	—
	additional info (upper)	Upper 4 digits of additional information	—
	additional info (lower)	Lower 12 digits of additional information	—
	message text	Message text	—

#: Items that are not specified as event monitoring conditions are not displayed.

Impact on communication

None

Notes

None

clear event manager

Clears the following information related to event management:

- Statistics and warning information output by the "show event manager monitor" command
- Event history output by the "show event manager history" command

Syntax

```
clear event manager [{applet | script}] [{statistics | history}]
```

Input mode

User mode and administrator mode

Parameters

{applet | script}

applet

Clears the information of events registered for monitoring by the applet function.

script

Clears the information of events registered for monitoring by a script.

Behavior when this parameter is omitted:

The information of events registered for monitoring by the applet function and scripts is cleared.

{statistics | history}

statistics

Clears statistics and warning information of monitored events.

history

Clears the event history.

Behavior when this parameter is omitted:

The statistics, warning information, and event history of events being monitored are cleared.

Behavior when all parameters are omitted:

The statistics, warning information, and event history of monitored events registered for monitoring by the applet function and scripts are cleared.

Example

Figure 18-15: Clearing the statistics held by the event management program

```
> clear event manager statistics
>
```

Display items

None

Impact on communication

None

Notes

None

restart script-manager

Restarts the script management program. At this time, running scripts are stopped and resident script files are restarted.

Syntax

```
restart script-manager [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the script management program without displaying a restart confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the script management program's core file (scriptManagerd.core) when the program is restarted.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

After the restart confirmation message is output, the script management program is restarted.

Example

Figure 18-16: Restarting the script management program

```
> restart script-manager
Do you want to restart the script management program (scriptManagerd)? (y/n): y
>
```

Display items

None

Impact on communication

None

Notes

1. If the core file already exists, it is overwritten unconditionally. Therefore, back up the file in advance, if necessary. The output destination and file name are as follows:
   - Directory: /usr/var/core/
   - File name: scriptManagerd.core

restart event-manager

Restarts the event management program.

Syntax

```
restart event-manager [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the event management program without displaying a restart confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the event management program's core file (eventManagerd.core) when the program is restarted.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

After the restart confirmation message is output, the event management program is restarted.

Example

Figure 18-17: Restarting the event management program

```
> restart event-manager
Do you want to restart the event management program (eventManagerd)? (y/n): y
>
```

Display items

None

Impact on communication

None

Notes

1. If the core file already exists, it is overwritten unconditionally. Therefore, back up the file in advance, if necessary. The output destination and file name are as follows:
   - Directory: /usr/var/core/
   - File name: eventManagerd.core

dump script-user-program

Outputs standard errors that are output by resident scripts and collected by the script management program, and that are output by event startup scripts, to a file.

Syntax

```
dump script-user-program
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 18-18: Outputting standard errors output by resident and event startup scripts to a file

```
> dump script-user-program
>
```

Display items

None

Impact on communication

None

Notes

1. If the specified file already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary. The output destination and file name are as follows:
   - Directory: /usr/var/scriptManager/
   - File name: smd_script_user.gz
2. smd_script_user.gz is a gzip compressed file. Here is an output example of the uncompressed file:

   [Output example]

```
########################################
##[resident script id 1 info]###########                  …1
## START(20XX/07/04 11:56:00 UTC) name=err.py pid=3758    …2
## 20XX/07/04 11:56:00 UTC                                …3
  File "/config/script/script.file/err.py", line 1       ┐
    print aaa                                            │4
          ^                                              │
SyntaxError: invalid syntax                              ┘
## END(20XX/07/04 11:56:00 UTC) name=err.py pid=3758      …5
########################################
## START(20XX/07/04 11:56:00 UTC) name=err.py pid=3418
## 20XX/07/04 11:56:00 UTC
  File "/config/script/script.file/err.py", line 1
    print aaa
          ^
SyntaxError: invalid syntax
## END(20XX/07/04 11:56:00 UTC) name=err.py pid=3418
########################################
## START(20XX/07/04 11:56:00 UTC) name=err.py pid=3815
## 20XX/07/04 11:56:01 UTC
```

```
  File "/config/script/script.file/err.py", line 1
    print aaa
            ^
SyntaxError: invalid syntax
## END(20XX/07/04 11:56:01 UTC) name=err.py pid=3815
########################################
## START(20XX/07/04 11:56:01 UTC) name=err.py pid=3980
## 20XX/07/04 11:56:01 UTC
  File "/config/script/script.file/err.py", line 1
    print aaa
            ^
SyntaxError: invalid syntax
## END(20XX/07/04 11:56:01 UTC) name=err.py pid=3980
########################################
########################################
##[resident script id 2 info]###########
## START(20XX/07/04 11:59:00 UTC) name=sample.py pid=1212
                 :
                 :
                 :
************************************                  …6
########################################
## [applet:testapplet,action:1]                       …7
## START(20XX/07/04 11:35:00 UTC) name=sample.py pid=1345 …2
## 20XX/07/04 11:36:00 UTC                            …3
  File "/config/script/script.file/sample.py", line 1     ┐
    print aaa                                             │4
            ^                                             │
SyntaxError: invalid syntax                               ┘
## END(20XX/07/04 11:36:47 UTC) name=sample.py pid=1345   …5
########################################
```

1. Heading about the resident script with the script ID of 1
2. Start time, file/module name, and process ID#
3. Time when the standard error was output#
4. Standard error text#
5. End time, file name, and process ID#
6. Display boundary between resident scripts and event startup scripts
7. Applet name and action sequence number

#: Data subject to be wrapped around

dump script-manager

Outputs control information collected by the script management program to a file.

Syntax

```
dump script-manager
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 18-19: Outputting control information of the script management program to a file

```
> dump script-manager
>
```

Display items

None

Impact on communication

None

Notes

1. If the specified file already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary. The output destination and file name are as follows:
   - Directory: /usr/var/scriptManager/
   - File name: smd_dump.gz
   - File name: smd_trace1.gz
   - File name: smd_trace2.gz

dump event-manager

Outputs control information collected by the event management program to a file.

Syntax

```
dump event-manager
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 18-20: Outputting the control information of the event management program to a file

```
> dump event-manager
>
```

Display items

None

Impact on communication

None

Notes

1. If the specified file already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary. The output destination and file name are as follows:
   - Directory: /usr/var/eventManager/
   - File name: emd_dump.gz
   - File name: emd_trace1.gz
   - File name: emd_trace2.gz

19 Python Extension Library

List of provided modules

This section contains the information about device-specific functions provided by the Switch. All the device-specific functions are offered as libraries in the extlib package.

■ commandline module

The commandline module provides the CommandLine class that is used to execute operation commands and configuration commands from scripts.

The CommandLine class has the following methods:

- CommandLine class
  - __init__ method
  - exec method
  - exit method
  - set_default_timeout method
  - set_default_logging method

■ sysmsg module

The sysmsg module is used to output operation messages from scripts.

The available function is as follows:

- send function

■ eventmonitor module

The eventmonitor module is used to notify running scripts of status changes (events) of monitored objects by linking with the monitoring of the status of devices and a network.

The available functions are as follows:

- regist_sysmsg function
- regist_cron_timer function
- regist_interval_timer function
- event_delete function
- event_receive function

The module also gets the trigger that started a script (for an event startup script, the event that started the script as a trigger).

The available function is as follows:

- get_exec_trigger function

__init__ method (commandline.CommandLine class)

This method is the constructor of the CommandLine class.

Method name

```
__init__()
```

Argument

None

Return value

Instance type

Instance generated

Exception

Table 19-1: List of exception classes of the __init__ method

Exception class name	Description
commandline.GenerateInstanceError	An attempt to generate an instance failed. Re-execute the command.
commandline.DuplicateInstanceError	An instance that can be used to execute commands has already been generated.

Details

The method creates an instance through which commands can be executed with the exec method.

The command input mode is in user mode immediately after an instance is generated. Also, the current directory is /opt/script immediately after an instance is generated.

Notes

1. Multiple instances of the CommandLine class cannot be generated for a single process. When regenerating the instance, first call the exit method for the existing instance.
2. If the TACACS+ command authorization function is enabled, this method retrieves command authorization information from the TACACS+ server. Therefore, if your network environment experiences timeouts due to failure to access the target server, you need to wait for the following period of wait time:

   Timeout period (1 to 30 seconds. initial value of 5 seconds) x number of servers configured (maximum 4)

Remarks

None

exec method (commandline.CommandLine class)

Executes a command specified in the argument.

Method name

```
exec(*tpl_command, logging = commandline.DEFAULT)
```

Argument

*tpl_command

Tuple type

First element

A string, along with a parameter string, of the operation command or configuration command to be executed

Second and subsequent elements

An inner tuple with two elements. The first element has a question string for an interactive command, and the second element has a response string.

Last element

Timeout period of the command response (unit: seconds). The specifiable values are from 0 to 86400. This element is optional.

logging

Sets whether the logs of commands executed by this method are to be displayed by the "show logging" command.

- commandline.ENABLE

  Specifies that the logs of commands executed by this method are displayed by the "show logging" command.

- commandline.DISABLE

  Specifies that the logs of commands executed by this method are not displayed by the "show logging" command. However, the logs are displayed if the script-only parameter or script-include parameter is specified at the execution of the "show logging" command.

The default value of this argument is commandline.DEFAULT. If commandline.DEFAULT is specified (or if this parameter is omitted), the value specified by the set_default_logging method is applied.

Return value

Dictionary type

Key value 'result'

- commandline.OK: Command execution was successful.
- commandline.TIMEOUT: A command response timed out.

Key value 'strings'

String that represents the result of command execution. If a command exits with a command response timeout, the value corresponding to this key contains the command execution results up to the timeout.

Exception

Table 19-2: List of exception classes of the exec method

Exception class name	Description
TypeError	The type of argument is incorrect.
ValueError	A value out of range is specified for the command response timer.
KeyboardInterrupt	The command was interrupted because the Ctrl + C keys were entered.
commandline.NoCommandError	No command string is specified for the argument.
commandline.ExecuteCommandError	The command execution failed. Generate an instance again, and then re-execute the command.

Details

The method executes the specified operation command or configuration command. For interactive commands, waits for a question string specified in and after the second element, and then executes the corresponding response command.

By specifying the timeout period of the command response in seconds as the last element, you can suspend the command when the specified time elapses. If the timeout period is not specified, the method is executed with the time specified by the set_default_timeout method (0 if not set). If the timeout period of the command response has the value of 0, the method waits indefinitely until the command is completed.

The method also returns the command execution result. The command execution result string to be returned contains strings stored in the standard output (stdout) and standard error output (stderr).

Notes

1. If response strings for an interactive command are specified more than the number of necessary interactions, the excess response strings are not used and the method ends normally.
2. If a commandline.ExecuteCommandError exception occurs, all the subsequent commands fail to be executed. To recover this situation, the instance must be regenerated.
3. The exec method executes commands under the user-for-scripts-only permissions.
4. Interactive commands such as telnet, which sends and receives strings to and from external devices, may not work properly even if you specify correct response strings.
5. When a timeout occurs, the exec method interrupts the running command when you enter the Ctrl + C keys. For commands that do not permit interruption of processing by the Ctrl + C keys (such as "more" and "less"), an exception (commandline.ExecuteCommandError) occurs because they cannot be terminated normally when a timeout occurs.
6. No password entry is required for executing the "enable" command (to enter the administrator mode) when enable password is set.

Remarks

None

exit method (commandline.CommandLine class)

Exits a command execution by a target instance.

Method name

```
exit()
```

Argument

None

Return value

None

Exception

None

Details

Command execution by the target instance is disabled, and another instance can be regenerated.

Notes

1. If an instance is generated by a local function within a process and the function is terminated without calling this method, or if the generated instance is deleted with the del statement before this method is called, regenerating the instance always causes an error. To recover from this situation, you need to re-start Python (restart the interactive mode or re-execute the script).

Remarks

None

set_default_timeout method (commandline.CommandLine class)

Sets the default timeout period for a command execution by a target instance.

Method name

```
set_default_timeout(timeout)
```

Argument

timeout

Specifies the default timeout period (in seconds) for command responses when the exec method is executed. The specifiable values are from 0 to 86400.

Return value

None

Exception

Table 19-3: List of exception classes of the set_default_timeout method

Exception class name	Description
TypeError	The type of argument is incorrect.
ValueError	A value out of range is specified for the argument.

Details

The method sets the default timeout period (in seconds) for command responses when the exec method is executed.

Notes

None

Remarks

None

set_default_logging method (commandline.CommandLine class)

Sets the default value for whether the logs of commands executed by a target instance are to be displayed by the "show logging" command.

Method name

```
set_default_logging(mode)
```

Argument

mode

- commandline.ENABLE

  Specifies that the logs of commands executed by this method are displayed by the "show logging" command.

- commandline.DISABLE

  Specifies that the logs of commands executed by this method are not displayed by the "show logging" command. However, the logs are displayed if the script-only parameter or script-include parameter is specified at the execution of the "show logging" command.

Return value

None

Exception

Table 19-4: List of exception classes of the set_default_logging method

Exception class name	Description
TypeError	The type of argument is incorrect.
ValueError	An invalid value is specified for the argument.
KeyboardInterrupt	The configuration was interrupted because the Ctrl + C keys were entered.
commandline.LoggingError	The configuration failed. Generate an instance again, and then re-execute the command.

Details

The method specifies whether the logs (of message type KEY or RSP) of commands executed by the applicable instance are to be displayed by the "show logging" command. If this method is not called, the log is displayed (default).

Notes

1. This setting is applied to the logs of commands executed after this method is called. Before it is called, the setting at the time when the logs are recorded is applied.
2. If you specify commandline.DISABLE for the mode argument, you might miss command errors that are important for operation. Therefore, we recommend the following actions:

- When executing an important command, execute it with commandline.ENABLE specified for the logging argument of the exec method.
- Create a script that outputs a message through the sysmsg module when command execution results in an error.

Remarks

- If you want to hide logs of commands (exit and end) that this module executes independently when the exit method is called or when the script terminates, use this method to hide them (by specifying commandline.DISABLE for the mode argument).
- If the script-only parameter or script-include parameter is specified in executing the "show logging" command, the logs that are hidden by this method (with commandline.DISABLE specified for the mode argument) are displayed with one of the message types listed in the following table.

Table 19-5: Message types of logs to be hidden

Target log	Message type
Command entered	SKY
Configuration error message and command response message	SRS

sysmsg.send

Outputs an operation message.

Function name

```
send(event_level, message_id_lower, additional_info_lower, message_text)
```

Argument

event_level

Specifies the event level of events to be output as a two-letter ASCII code string. The specifiable ranges of values are from E3 to E9 as well as from R5 to R8.

message_id_lower

Specifies the lower four digits of the message ID of the operation message to be output in hexadecimal notation. The specifiable range of values is from 0x0 to 0xffff.

Note that the upper four digits of the message ID are always 3e03.

additional_info_lower

Specifies the lower 12 digits of the additional information to be output in hexadecimal notation. The specifiable range of values is from 0x0 to 0xffffffffffff.

message_text

Specifies the text of the message text to be output as an ASCII code string. The maximum number of characters that can be specified is 196 characters.

Return value

None

Exception

Table 19-6: List of exception classes of sysmsg.send

Exception class name	Description
TypeError	The type of argument is invalid.
ValueError	The value specified for the argument is invalid.
sysmsg.MsgSendError	Failed to output an operation message.

Details

The function outputs an operation message. The event location is always SCRIPT.

Notes

1. A maximum of 10 operation messages per second can be output per device.
2. If a single process calls this function more than 10 times per second, the applicable process is forced to be in sleep mode for up to one second.
3. If multiple processes call this function at the same time and the total number of calls exceeds 10 times per second, an exception (sysmsg.MsgSendError) is returned if that situation persists.

Remarks

- Messages specified by this function are output in the following format:

```
kkk mm/dd hh:mm:ss www ee SCRIPT 3e03xxxx yyyy:yyyyyyyyyyy ttt...ttt
                       1            2         3           4
```

  1. The value specified in event_level
  2. The value specified in message_ id_lower
  3. The value specified in additional_info_lower
  4. The string specified in message_text

eventmonitor.regist_sysmsg

Monitors operation messages of specified message type or that contains specified message text. For operation message of message types ERR and EVT, you can also monitor the elements that make up operation messages, such as the switch number and event level.

For details on the elements of operation messages, see "Message Log Reference, 1.2.2 Format of operation logs".

Function name

```
regist_sysmsg( message_type = "",
               switch_no = eventmonitor.DEFAULT,
               event_level = "",
               event_function = ""
               interface_id = "",
               message_id = eventmonitor.DEFAULT,
               additional_info_upper = eventmonitor.DEFAULT,
               additional_info_lower = eventmonitor.DEFAULT,
               message_text = "",
               priority = eventmonitor.NORMAL)
```

Argument

message_type

Specifies the message type of operation messages to be monitored in three letters.

The default value of this argument is "". If "" is specified, all message types are monitored.

Note that even if you specify a string that is not defined in the Switch, an exception (ValueError) does not occur.

switch_no

Specifies the switch number in operation messages to be monitored as a numeric value. For the specifiable range of values, see the description of the <switch no.> value in "Specifiable values for parameters".

The default value of this argument is eventmonitor.DEFAULT. If eventmonitor.DEFAULT is specified, all switch numbers are monitored.

event_level

Specifies the event level of events to be monitored. Specify two letters if you monitor a single event level, or event levels of tuple type (E3 to E9 or R5 to R8). For example, messages at event levels of E3, E5, and R8 are monitored if you specify:

```
event_level = ("E3","E5","R8")
```

The default value of this argument is "". If "" is specified, all event levels are monitored.

event_function

Specifies the event location to be monitored in a maximum of 15 characters. Only the event location that exactly matches the specified string are monitored.

The default value of this argument is "". If "" is specified, all event locations are monitored.

Note that even if you specify a string that is not defined in the Switch, an exception (ValueError) does not occur.

interface_id

Specifies the event interface ID to be monitored as a regular expression string with a maximum of 32 characters. Only the event interface IDs that match the specified regular expression string are monitored.

This argument must be specified along with the event_function argument. If it is not specified (default value), an exception (ValueError) is returned.

The default value of this argument is "". If "" is specified, all event interface IDs are monitored.

The function supports the POSIX 1003.2 Extended Regular Expression syntax, in which periods (.), hyphens (-), asterisks (*), plus signs (+), question marks (?), carets (^), dollar signs ($), opening square brackets ([), closing square brackets (]), opening round brackets (), closing round brackets ()), pipes (|), and backslashes (\) are available.

message_id

Specifies message IDs to be monitored in hexadecimal notation. The specifiable range of values is from 0x0 to 0xffffffff.

The default value of this argument is eventmonitor.DEFAULT. If eventmonitor.DEFAULT is specified, all message IDs are monitored.

additional_info_upper

Specifies the upper four digits of the additional information to be monitored in hexadecimal notation. The specifiable range of values is from 0x0 to 0xffff.

The default value of this argument is eventmonitor.DEFAULT. If eventmonitor.DEFAULT is specified, upper four digits of all additional information are monitored.

additional_info_lower

Specifies the lower 12 digits of the additional information to be monitored in hexadecimal notation. The specifiable range of values is from 0x0 to 0xffffffffffff.

The default value of this argument is eventmonitor.DEFAULT. If eventmonitor.DEFAULT is specified, lower 12 digits of all additional information are monitored.

message_text

Specifies the message text to be monitored as an ASCII code string with a maximum of 128 characters. Only the message text that matches the specified regular expression string is monitored.

The default value of this argument is "". If "" is specified, all message text is monitored.

The function supports the POSIX 1003.2 Extended Regular Expression syntax, in which periods (.), hyphens (-), asterisks (*), plus signs (+), question marks (?), carets (^), dollar signs ($), opening square brackets ([), closing square brackets (]), opening round brackets (), closing round brackets ()), pipes (|), and backslashes (\) are available.

priority

Specifies the notification priority when this monitoring event occurs.

- eventmonitor.HIGH: High priority
- eventmonitor.NORMAL: Medium priority (default value)
- eventmonitor.LOW: Low priority
- eventmonitor.LAST: Lowest priority

Events with high-, medium-, and low-notification priorities are notified at the following rate:

HIGH:NORMAL:LOW = 6:3:1

An event with the lowest notification priority is notified after all high-, medium-, and low-priority events are notified.

Return value

Integer type

Monitoring event ID (unique value)

Exception

Table 19-7: List of exception classes of eventmonitor.regist_sysmsg

Exception class name	Description
TypeError	The type of argument is incorrect.
ValueError	An invalid value is specified for the argument.
SystemError	A system error occurred.
KeyboardInterrupt	The command was interrupted because the Ctrl + C keys were entered.
eventmonitor.RegisterMax	The number of registered events has reached the upper limit.
eventmonitor.RegistrationError	An attempt to register an event failed.

Details

The function monitors operation messages specified in the argument.

The monitoring of the operation messages is carried out with the AND condition of the message_type, switch_no, event_level, event_function, interface_id, message_id, additional_info_upper, additional_info_lower, and message_text arguments.

If the function exits successfully, it returns the value of the monitoring event ID (positive integer) as its return value. If it exits abnormality, it returns an exception.

A single device can have a maximum of 256 operation message monitoring entries registered. An exception (eventmonitor.RegisterMax) is returned if the number of records exceeds 256 entries.

Notes

1. Operation messages of following message types cannot be monitored:
   - KEY and SKY (command entered)
   - RSP and SRS (command response message)
2. An exception (ValueError) is returned if all the arguments, except for the priority argument, have their default value.

Remarks

- The arguments specified in this function corresponds to the operation messages as follows:

```
kkk mm/dd hh:mm:ss www ee kkkkkkkk [iii ... iii] xxxxxxxx yyyy:yyyyyyyyyyyy ttt...ttt
 1                  2 3 4    5         6               7       8        9          10
```

  1. message_type
  2. switch_no
  3. switch_status (This cannot be specified with an argument.)
  4. event_level
  5. event_function
  6. interface_id
  7. message_id

8. additional_info_upper
9. additional_info_lower
10. message_text

- If a large number of operation messages are output, it may take time to notify the messages of the scripts or the messages may be discarded, depending on the number of monitoring registrations or the monitoring conditions.

eventmonitor.regist_cron_timer

Registers a cron timer.

Function name

```
regist_cron_timer(cron, priority = eventmonitor.NORMAL)
```

Argument

cron

'<minute> <hour> <day> <month> <week>'

Raises an event at the specified time. The specifiable ranges of values are as follows:

<minute>

Specifies the minute. {0-59|*}

<hour>

Specifies the hour. {0-23|*}

<day>

Specifies the day of the month. {1-31|*}

<month>

Specifies the month. {1-12|*}

<week>

Specifies the day of the week. {0-7|*}

(0, 7 = Sunday, 1 = Monday, 2 = Tuesday, ..., 6 = Saturday)

For the rules on how to specify the date and time and setting examples, see Remarks.

priority

Specifies the notification priority when this timer runs.

- eventmonitor.HIGH: High priority
- eventmonitor.NORMAL: Medium priority (default value)
- eventmonitor.LOW: Low priority
- eventmonitor.LAST: Lowest priority

Events with high-, medium-, and low-notification priorities are notified at the following rate:

HIGH:NORMAL:LOW = 6:3:1

An event with the lowest notification priority is notified after all high-, medium-, and low-priority events are notified.

Return value

Integer type

Monitoring event ID (unique value)

Exception

Table 19-8: List of exception classes of eventmonitor.regist_cron_timer

Exception class name	Description
TypeError	The type of argument is incorrect.
ValueError	An invalid value is specified for the argument.
SystemError	A system error occurred.
KeyboardInterrupt	The command was interrupted because the Ctrl + C keys were entered.
eventmonitor.RegisterMax	The number of registered events has reached the upper limit.
eventmonitor.RegistrationError	An attempt to register an event failed.

Details

The function registers a cron timer specified in the argument.

If the function exits successfully, it returns the value of the monitoring event ID (positive integer) as its return value. If it exits abnormality, it returns an exception.

A single device can have a maximum of 256 cron timer monitoring entries registered, in combination with interval timer monitoring registration entries. An exception (eventmonitor.RegisterMax) is returned if the number of records exceeds 256 entries.

Notes

1. If the system time is changed across the event occurrence time of a cron timer (including system time changes due to the start or end of the daylight savings time), the event may not occur if the time is set forward across the occurrence time, and the event may occur twice if the time is set backward across the occurrence time.

Remarks

- The rules when the cron argument is specified are as follows:
  - Specifying an asterisk (*) means that all possible values (times) for that parameter are specified. For example, if you specify an asterisk (*) for minute, the event will be raised every minute of the system time.
  - You can specify multiple values by separating them with commas (,).
  - You can specify a time interval at which an event occurs by using a slash (/), followed by a numeric value.
  - You can specify a range by using a hyphen (-).
  - A cron setting string can have up to 511 characters.

  The following table shows examples of how to specify the cron argument.

  Table 19-9: Examples of how to specify the cron argument

Example	Description
* * * * *	An event is raised every minute.
43 23 * * *	An event is raised at 23:43 every day.

Example	Description
0 17 * * 1	An event is raised at 17:00 every Monday.
0,10 17 * * 0,2,3	An event is raised at 17:00 and 17:10 every Sunday, Tuesday, and Wednesday.
0-10 17 1 * *	An event is raised every minute from 17:00 to 17:10 on the first day of every month.
0 0 1,15 * 1	An event is raised at 0:00 on the 1st and 15th days of every month and on Mondays.
42 4 1 * *	An event is raised at 4:42 on the 1st day of every month.
0 21 * * 1-6	An event is raised at 21:00 every Monday through Saturday.
0,10,20,30,40,50 * * * *	An event is raised at 0, 10, 20, 30, 40, and 50 minutes every hour
*/10 * * * *	An event is raised every 10 minutes from every hour on the hour.
* 1 * * *	An event is raised every minute from 1:00 to 1:59 every day
0 */1 * * *	An event is raised every hour on the hour.
0 * * * *	An event is raised every hour on the hour.
2 8-20/3 * * *	An event is raised at 8:02, 11:02, 14:02, 17:02, 20:02 daily.
30 5 1,15 * *	An event is raised at 5:30 on the 1st and 15th of every month.

eventmonitor.regist_interval_timer

Registers an interval timer.

Function name

```
regist_interval_timer(interval, priority = eventmonitor.NORMAL)
```

Argument

interval

Generates an event at the specified cycle (in seconds). The specifiable values are from 1 to 4294967.

priority

Specifies the notification priority when this timer runs.

- eventmonitor.HIGH: High priority
- eventmonitor.NORMAL: Medium priority (default value)
- eventmonitor.LOW: Low priority
- eventmonitor.LAST: Lowest priority

Events with high-, medium-, and low-notification priorities are notified at the following rate:

HIGH:NORMAL:LOW = 6:3:1

An event with the lowest notification priority is notified after all high-, medium-, and low-priority events are notified.

Return value

Integer type

Monitoring event ID (unique value)

Exception

Table 19-10: List of exception classes of eventmonitor.regist_interval_timer

Exception class name	Description
TypeError	The type of argument is incorrect.
ValueError	An invalid value is specified for the argument.
SystemError	A system error occurred.
KeyboardInterrupt	The command was interrupted because the Ctrl + C keys were entered.
eventmonitor.RegisterMax	The number of registered events has reached the upper limit.
eventmonitor.RegistrationError	An attempt to register an event failed.

Details

The function registers an interval timer specified in the argument.

If the function exits successfully, it returns the value of the monitoring event ID (positive integer) as its return

value. If it exits abnormality, it returns an exception.

A single device can have a maximum of 256 interval timer monitoring entries registered, in combination with cron timer monitoring registration entries. An exception (eventmonitor.RegisterMax) is returned if the number of records exceeds 256 entries.

Notes

None

Remarks

None

eventmonitor.event_delete

Stops monitoring of an event.

Function name

```
event_delete(event_id= eventmonitor.EVENT_ALL_DEL)
```

Argument

event_id

Specifies the monitoring event ID of the event to be deleted.

The default value of this argument is eventmonitor.EVENT_ALL_DEL. If eventmonitor.EVENT_ALL_DEL is specified, the system stops monitoring all monitoring events registered by the caller.

Return value

Integer type

The function returns 0.

Exception

Table 19-11: List of exception classes of eventmonitor.event_delete

Exception class name	Description
TypeError	The type of argument is incorrect.
ValueError	An invalid value is specified for the argument.
SystemError	A system error occurred.
KeyboardInterrupt	The command was interrupted because the Ctrl + C keys were entered.
eventmonitor.DeleteError	An attempt to delete an event failed.

Details

This function stops event monitoring of the event with the monitoring event ID specified by the argument.

If the monitoring event ID specified by the argument has been registered by another script, eventmonitor.DeleteError is returned.

If the function exits successfully, it returns 0. If it exits abnormality, it causes an exception.

Notes

1. The function cannot stop monitoring of events with a monitoring event ID registered by a process other than the process of the function.
2. If a non-existent monitoring event ID is specified, the function returns 0.

Remarks

- If a script program terminates without stopping events registered by it, the event monitoring of the event registered by the terminated script program is stopped.

eventmonitor.event_receive

Receives an event.

Function name

```
event_receive(blocking_flg, timeout = 0)
```

Argument

blocking_flg

Enables the blocking mode.

- eventmonitor.BLOCK_ON: Blocking mode
- eventmonitor.BLOCK_OFF: Non-blocking mode

timeout

Specifies the reception wait time when the blocking mode is specified (in seconds). The specifiable values are from 0 to 86400.

The default value of this argument is 0.

Return value

Dictionary type

Key value 'result'

Stores a reception result.

- eventmonitor.OK: Successful
- eventmonitor.TIMEOUT: Timed out
- eventmonitor.NODATA: No data received

Key value 'event_type'

Stores the type of received event.

- eventmonitor.CRON_TIMER_EVT: cron timer
- eventmonitor.INTERVAL_TIMER_EVT: interval timer
- eventmonitor.SYSMSG_EVT: Operation message
- eventmonitor.NODATA: No data received

Key value 'event_id'

Stores a monitoring event ID. It is a unique value that is associated with a registered monitoring event.

Key value 'add_info' [additional information part]

If the received event is eventmonitor.SYSMSG_EVT, the key value stores the operation message that triggered the event.

For the data structure of the variable-length section in an operation message, see "Table 19-13: Data structure of the variable-length section in a trigger operation message".

Exception

Table 19-12: List of exception classes of eventmonitor.event_receive

Exception class name	Description
TypeError	The type of argument is incorrect.
ValueError	An invalid value is specified for the argument.
SystemError	A system error occurred.
KeyboardInterrupt	The command was interrupted because the Ctrl + C keys were entered.
eventmonitor.ReceiveError	An attempt to receive an event failed.

Details

The function receives a notification that an event occurred.

The relationship between the blocking_flg argument setting and the timeout argument is shown below:

- If BLOCK_OFF is specified, the timeout argument is ignored.
- If BLOCK_ON is specified, the timeout argument specifies the reception wait time.
- If BLOCK_ON is specified and 0 is specified for the timeout argument, the function waits until it receives an event.
- When BLOCK_ON is specified and a value greater than 0 is specified for the timeout argument, eventmonitor.TIMEOUT is set in the 'result' key of the return value, and the function returns to the caller if an event does not occur within the time (seconds) specified by timeout.

Notes

None

Remarks

- The data structure of the variable-length section in an operation message that triggered the event is shown below.

  Table 19-13: Data structure of the variable-length section in a trigger operation message

Tuple type (access value)	Description
eventmonitor.SYSMSG_TIME	Event occurrence time "<month>/<day> <hour>:<minute>:<second>"
eventmonitor.SYSMSG_MESSAGE_TYPE	Message type A string is stored in it.
eventmonitor.SYSMSG_SWITCH_NO	Switch number A numeric value is stored in it.
eventmonitor.SYSMSG_SWITCH_STATUS	Switch status • eventmonitor.M: Standalone (Fixed value)

Tuple type (access value)	Description
eventmonitor.SYSMSG_EVENT_LEVEL	Event level A string of two letters is stored in it. "E9" to "E3", "R8" to "R5"
eventmonitor.SYSMSG_EVENT_FUNCTION	Event location A string is stored in it.
eventmonitor.SYSMSG_INTERFACE_ID	Event interface ID A string is stored in it.
eventmonitor.SYSMSG_MSG_ID	Message ID A numeric value is stored in it.
eventmonitor.SYSMSG_ADD_HIGH	Upper 4 digits of additional information A numeric value is stored in it.
eventmonitor.SYSMSG_ADD_LOW	Lower 12 digits of additional information A numeric value is stored in it.
eventmonitor.SYSMSG_EVT_TEXT	Message text A string is stored in it.

eventmonitor.get_exec_trigger

Gets the trigger to start a script.

Function name

```
get_exec_trigger()
```

Argument

None

Return value

Dictionary type

Key value 'type'

Stores a startup trigger.

- eventmonitor.OPERATE_COMMAND: Command script
- eventmonitor.RESIDENT: Resident script
- eventmonitor.APPLET: Applet (event startup script)

Key value 'applet'

Stores detailed applet information if the startup trigger is eventmonitor.APPLET.

For details about applet information, see "Table 19-15: Detailed applet information".

Exception

Table 19-14: List of exception classes of eventmonitor.get_exec_trigger

Exception class name	Description
SystemError	A system error occurred.
KeyboardInterrupt	The command was interrupted because the Ctrl + C keys were entered.

Details

The function gets the trigger to start the script that called this function.

Notes

None

Remarks

- The following table lists and describes the detailed applet information.

  Table 19-15: Detailed applet information

Key value	Description
applet_name	Applet name A string is stored in it.

Key value	Description
type	Type of monitoring event that triggered the startup of the script • eventmonitor.TIMER_EVT: Timer monitoring • eventmonitor.SYSMSG_EVT: Operation message monitoring
condition	Detailed monitoring condition information about monitoring events It is stored as a value of tuple type. For timer monitoring: See "Table 19-16: Detailed monitoring condition information (timer monitoring)". For operation message monitoring: See "Table 19-17: Detailed monitoring condition information (operation message monitoring)".
trigger	Details of the event that triggered the startup of the script It is stored as a value of tuple type. For timer monitoring: This entry is invalid. For operation message monitoring: See "Table 19-18: Event cause information (operation message monitoring)".

Table 19-16: Detailed monitoring condition information (timer monitoring)

Tuple type (access value)	Description
eventmonitor.TIMER_TYPE	Type of timer monitoring • eventmonitor.CRON: cron timer • eventmonitor.INTERVAL: interval timer
eventmonitor.CRON	Value set for the cron timer A string is stored in it.
eventmonitor.INTERVAL	Value set for the interval timer A numeric value is stored in it.

Table 19-17: Detailed monitoring condition information (operation message monitoring)

Tuple type (access value)	Description
eventmonitor.SYSMSG_MESSAGE_TYPE	Message type A string is stored in it. If this value of tuple type is not specified as a monitoring condition, "" is stored.
eventmonitor.SYSMSG_SWITCH_NO	Switch number A numeric value is stored in it. If this value of tuple type is not specified as a monitoring condition, eventmonitor.DEFAULT is stored.
eventmonitor.SYSMSG_SWITCH_STATUS	Switch status eventmonitor.DEFAULT is stored.
eventmonitor.SYSMSG_EVENT_LEVEL	Event level A string of two letters is stored in it as a value of tuple type (for example, ['E3','R5','E5','R6','R7']). If this value of tuple type is not specified as a monitoring condition, [''] is stored.

Tuple type (access value)	Description
eventmonitor.SYSMSG_EVENT_FUNCTION	Event location A string is stored in it. If this value of tuple type is not specified as a monitoring condition, "" is stored.
eventmonitor.SYSMSG_INTERFACE_ID	Event interface ID A string is stored in it. If this value of tuple type is not specified as a monitoring condition, "" is stored.
eventmonitor.SYSMSG_MSG_ID	Message ID A numeric value is stored in it. If this value of tuple type is not specified as a monitoring condition, eventmonitor.DEFAULT is stored.
eventmonitor.SYSMSG_ADD_HIGH	Upper 4 digits of additional information A numeric value is stored in it. If this value of tuple type is not specified as a monitoring condition, eventmonitor.DEFAULT is stored.
eventmonitor.SYSMSG_ADD_LOW	Lower 12 digits of additional information A numeric value is stored in it. If this value of tuple type is not specified as a monitoring condition, eventmonitor.DEFAULT is stored.
eventmonitor.SYSMSG_EVT_TEXT	Message text A string is stored in it. If this value of tuple type is not specified as a monitoring condition, "" is stored.

Table 19-18: Event cause information (operation message monitoring)

Tuple type (access value)	Description
eventmonitor.SYSMSG_MESSAGE_TYPE	Message type A string is stored in it.
eventmonitor.SYSMSG_SWITCH_NO	Switch number A numeric value is stored in it.
eventmonitor.SYSMSG_EVENT_LEVEL	Event level A string of two letters is stored in it. "E9" to "E3", "R8" to "R5"
eventmonitor.SYSMSG_EVENT_FUNCTION	Event location A string is stored in it.
eventmonitor.SYSMSG_INTERFACE_ID	Event interface ID A string is stored in it.
eventmonitor.SYSMSG_MSG_ID	Message ID A numeric value is stored in it.
eventmonitor.SYSMSG_ADD_HIGH	Upper 4 digits of additional information A numeric value is stored in it.
eventmonitor.SYSMSG_ADD_LOW	Lower 12 digits of additional information A numeric value is stored in it.

Tuple type (access value)	Description
eventmonitor.SYSMSG_EVT_TEXT	Message text A string is stored in it.
eventmonitor.SYSMSG_TIME	Output time of the operation message "<month>/<day> <hour>:<minute>:<second>"

20 Ethernet

show interfaces

Shows Ethernet information.

Syntax

```
show interfaces <interface type> <interface number> [detail]
```

Input mode

User mode and administrator mode

Parameters

<interface type> <interface number>

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below.

For details, see "■How to specify an interface" in "Specifiable values for parameters".

- Ethernet interface

detail

Specifies that detailed statistics be displayed.

Behavior when this parameter is omitted:

Detailed information is not displayed.

Example

The following figure shows an example of executing the command with the 10BASE-T/100BASE-TX/1000BASE-T port specified.

Figure 20-1: Example of executing the command (10BASE-T/100BASE-TX/1000BASE-T port)

```
> show interfaces gigabitethernet 1/0/1
Date 20XX/01/14 12:34:36 UTC
NIF0: -
Port1: active up  1000BASE-T full(auto)    0012.e245.0405
        Time-since-last-status-change:0:08:24
        Bandwidth:1000000kbps  Average out:0Mbps  Average in:0Mbps
        Peak out:1Mbps at 10:59:06  Peak in:1Mbps at 10:59:19
        Output rate:         0bps           0pps
        Input  rate:         0bps           0pps
        Flow control send   :off
        Flow control receive:off
        EEE config:enabled  EEE status:operational
        EEE Tx-LPI:on
        EEE Rx-LPI:on
        TPID:8100
        Frame size:1522 Octets  retry:0  Interface name:geth1/0/1
        description:test lab area network
        <Out octets/packets counter>       <In octets/packets counter>
        Octets       :              27706  Octets       :              28994
        All packets  :                272  All packets  :                286
        Unicast packets        :      271  Unicast packets        :      272
        Multicast packets      :        0  Multicast packets      :       11
        Broadcast packets      :        1  Broadcast packets      :        3
        Pause packets          :        0  Pause packets          :        0
        <Out line error counter>
        Late collision         :        0  Defer indication       :        0
        Collisions             :        0  Excessive collisions   :        0
        Underrun               :        0  Error frames           :        0
        <In line error counter>
        CRC errors             :        0  Symbol errors          :        0
```

```
        Alignment              :        0  Fragments              :        0
        Short frames           :        0  Jabber                 :        0
        Long frames            :        0  Overrun                :        0
        Error frames           :        0
        <Line fault counter>
        Polarity changed       :        0
        Link down              :        0
        Link down in operational state                           :        0
>
```

The following figure shows an example of executing the command with the 10BASE-T/100BASE-TX/1000BASE-T port and the detail parameter specified.

Figure 20-2: Example of executing the command with the detail parameter specified

```
> show interfaces gigabitethernet 1/0/1 detail
Date 20XX/01/14 12:35:06 UTC
NIF0: -
Port1: active up  1000BASE-T full(auto)  0012.e245.0405
        Time-since-last-status-change:0:08:54
        Bandwidth:1000000kbps  Average out:0Mbps  Average in:0Mbps
        Peak out:1Mbps at 10:59:06  Peak in:1Mbps at 10:59:19
        Output rate:         0bps           0pps
        Input  rate:         0bps           0pps
        Flow control send   :off
        Flow control receive:off
        EEE config:enabled  EEE status:operational
        EEE Tx-LPI:on
        EEE Rx-LPI:on
        TPID:8100
        Frame size:1522 Octets  retry:0  Interface name:geth1/0/1
        description:test lab area network
        <Out octets/packets counter>       <In octets/packets counter>
        Octets       :              27706  Octets       :              28994
        All packets  :                272  All packets  :                286
        Unicast packets        :      271  Unicast packets        :      272
        Multicast packets      :        0  Multicast packets      :       11
        Broadcast packets      :        1  Broadcast packets      :        3
        Pause packets          :        0  Pause packets          :        0
        <Out/In packets counter>
        64 packets             :       14
        65-127 packets         :      542
        128-255 packets        :        1
        256-511 packets        :        1
        512-1023 packets       :        0
        1024-     packets      :        0
                   :
                   :
>
```

The following figure shows an example of executing the command with an SFP+/SFP shared port that enabled SFP+ specified.

Figure 20-3: Example of executing the command (on an SFP+/SFP shared port with SFP+ enabled)

```
> show interfaces tengigabitethernet 1/0/27
Date 20XX/01/14 12:41:55 UTC
NIF0: -
Port27: active up  10GBASE-LR    0012.e222.1d55
        SFP+ connect
        Time-since-last-status-change:0:05:33
        Bandwidth:10000000kbps  Average out:0Mbps  Average in:0Mbps
        Peak out:65Mbps at 11:43:21  Peak in:51Mbps at 11:43:21
        Output rate:         0bps           0pps
        Input  rate:         0bps           0pps
        Flow control send   :off
        Flow control receive:on
        TPID:8100
        Frame size:1522 Octets  retry:0  Interface name:tengeth1/0/27
        <Out octets/packets counter>
        Octets                                        :              18653
        All packets                                   :                190
        Unicast packets                               :                189
```

```
          Multicast packets                                :                0
          Broadcast packets                                :                1
          Pause packets                                    :                0
          <In octets/packets counter>
          Octets                                           :            19172
          All packets                                      :              189
          Unicast packets                                  :              189
          Multicast packets                                :                0
          Broadcast packets                                :                0
          Pause packets                                    :                0
          <Out line error counter>
          Underrun                                         :                0
          Error frames                                     :                0
          <In line error counter>
          CRC errors                                       :                0
          Alignment                                        :                0
          Fragments                                        :                0
          Jabber                                           :                0
          Symbol errors                                    :                0
          Short frames                                     :                0
          Long frames                                      :                0
          Overrun                                          :                0
          Error frames                                     :                0
          <Line fault counter>
          Link down              :         0
          TX fault               :         0
          Signal detect errors   :         0
          Transceiver notconnect :         0
          Link down in operational state                          :         0
          Signal detect errors in operational state               :         0
          Transceiver notconnect in operational state             :         0
>
```

Display items

Table 20-1: Information displayed about the Ethernet interface

Item	Displayed information	
	Detailed information	Meaning
NIF<nif no.>	NIF number	
<NIF status>	—	
Port<port no.>	Port number	
<port status>	active up	Active (up and running normally)
	active down	Active (A line failure occurred.)
	initialize	Currently initializing or waiting for establishment of negotiation (auto-negotiation function is active).
	test	A line test is in progress.
	fault	Failure occurred
	inactive	• Operation was stopped by the "inactivate" command. • The port has been deactivated by the standby link function of link aggregation. • The port has been deactivated by the BPDU guard function of the Spanning Tree Protocol.

Item	Displayed information	
	Detailed information	Meaning
		• The port has been deactivated by the unidirectional link failure detection function. • The port has been deactivated by the L2 loop detection function. • The port has been deactivated by storm control. • The port has been deactivated by port resetting of uplink redundancy.
	disable	Operation was stopped by using the "shutdown" configuration command.
<line type>	See "Table 20-2: List of line types".	
<MAC address>	MAC address of the applicable port	
<type of transceiver>	SFP	SFP or SFP-T
	SFP+	SFP+
	-	The transceiver type is unknown.
<transceiver status>	connect	Installed
	notconnect	Not installed
	not support	An unsupported transceiver is installed.
	-	The transceiver status is unknown. A hyphen is displayed in the following cases: • A port is in initialize state. • A port is in fault state.

Table 20-2: List of line types

Displayed item#	Displayed information
10BASE-T full	10BASE-T full duplex
10BASE-T half	10BASE-T half duplex
100BASE-TX full	100BASE-TX full duplex
100BASE-TX half	100BASE-TX half duplex
1000BASE-T full	1000BASE-T full duplex
1000BASE-LX full	1000BASE-LX full duplex
1000BASE-SX full	1000BASE-SX full duplex
1000BASE-LH full	1000BASE-LH full duplex
1000BASE-BX10-D full	1000BASE-BX-D (10km) full duplex
1000BASE-BX10-U full	1000BASE-BX-U (10km) full duplex
1000BASE-BX40-D full	1000BASE-BX-D (40km) full duplex

Displayed item#	Displayed information
1000BASE-BX40-U full	1000BASE-BX-U (40km) full duplex
2.5GBASE-T full	2.5GBASE-T full duplex
10GBASE-SR	10GBASE-SR
10GBASE-LR	10GBASE-LR
10GBASE-ER	10GBASE-ER
10GBASE-CU30CM	10GBASE-CU (30cm)
10GBASE-CU1M	10GBASE-CU (1m)
10GBASE-CU3M	10GBASE-CU (3m)
10GBASE-CU5M	10GBASE-CU (5m)
10GBASE-BR10-D	10GBASE-BR-D (10km)
10GBASE-BR10-U	10GBASE-BR-U (10km)
10GBASE-BR40-D	10GBASE-BR-D (40km)
10GBASE-BR40-U	10GBASE-BR-U (40km)
(auto)	Line type determined through auto-negotiation
-	The line type is unknown. A hyphen is displayed in the following cases: • Auto-negotiation is enabled but the port status is neither active up nor test. • A port is in initialize state. • A port is in fault state. • The transceiver status is not connect.

#: The connection interface is displayed.

Hereafter, the frame length indicates the length from the MAC header to the FCS field. For details about frame formats, see "Configuration Guide Vol. 1, 20.2.2 Frame format".

Table 20-3: Detailed Ethernet interface information

Item	Displayed information	
	Detailed information	Meaning
Time-since-last-status-change	Displays the elapsed time since the last change in status. hh:mm:ss (when the elapsed time is 24 hours or less: hh = hours, mm = minutes, ss = seconds) dd.hh:mm:ss (when the elapsed time is more than 24 hours: dd = number of days, hh = hours, mm = minutes, ss = seconds) Over 100 days (when the elapsed time is more than 100 days)	
Bandwidth:<bandwidth of line>kbps	Displays the bandwidth of the line in kbps. If the "bandwidth" configuration command has not been executed, the line speed of the port is displayed. If the "bandwidth" configuration command has been executed, the setting value is displayed. Note that this setting does not control the bandwidth of the port.	

Item	Displayed information	
	Detailed information	Meaning
Average out:<average bandwidth used on sending side>Mbps	Displays the average bandwidth (in Mbps) used on the sending side of the line for the one minute interval before the command was executed. 0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place. The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.	
Average in:<average bandwidth used on receiving side>Mbps	Displays the average bandwidth (in Mbps) used on the receiving side of the line for the one minute interval before the command was executed. 0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place. The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.	
Peak out	Displays the maximum bandwidth used on the sending side of the line for the 24-hour interval before the command was executed, and the relevant time. 0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place. The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.	
Peak in	Displays the maximum bandwidth used on the receiving side of the line for the 24-hour interval before the command was executed, and the relevant time. 0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place. The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.	
Output rate[#1]	Displays the send throughput of the line (in bps and pps) for the one second interval before the command was executed, rounded to two decimal places. The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.	
Input rate[#1]	Displays the receive throughput of the line (in bps and pps) for the one second interval before the command was executed, rounded to two decimal places. The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.	
Flow control send[#2]	on	Pause packets are sent.
	off	Pause packets are not sent.
Flow control receive[#2]	on	Pause packets are received.
	off	Pause packets are not received.
EEE config	enabled	The EEE function is enabled.
	disabled	The EEE function is disabled.

Item	Displayed information	
	Detailed information	Meaning
EEE status#3	operational	The EEE function is running.
	disagreed	The EEE function is disabled due to a disagreement in EEE auto-negotiation.
EEE Tx-LPI#3	on	The sending-side device is running in power saving mode.
	off	The sending-side device exited the power saving mode and is running in normal mode.
EEE Rx-LPI#3	on	The receiving-side device is running in power saving mode.
	off	The receiving-side device exited the power saving mode and is running in normal mode.
TPID	Displays a TagProtocolIDentifier value that is used on the port to identify the VLAN.	
Frame size#3	Displays the maximum frame length of a port in octets. The maximum frame length is calculated from the MAC header, through DATA and PAD fields, to the FCS field.	
retry:<Counts>	Displays the number of times the port was reactivated due to a failure.	
Interface name	Displays the name assigned to a port.	
description:<supplementary explanation>	Displays the contents of the description configuration. The description configuration can be used to set comments, such as a comment about the purpose of the port. This item is not displayed if the description configuration has not been set.	

#1: If the displayed value is smaller than 10000, the decimal point is not displayed.

If the displayed value is 10000 or larger, the display unit varies depending on the displayed value, as follows:

- If the displayed value is 10000 or larger, the unit is k.
- If the displayed value is 10000 K or larger, the unit is M.
- If the displayed value is 10000 M or larger, the unit is G.

In the above cases, one digit is displayed below the decimal point.

#2: This item is always off except when the status of the port is either active up or test.

#3: This item is always - except when the status of the port is either active up or test.

Table 20-4: List of statistical items

Item	Displayed information
<Out octets/packets counter>	Send statistics
<In octets/packets counter>	Receive statistics
Octets	Number of octets (receive statistics include statistics on error packets whereas send statistics do not)#1 Calculation of octet values is based on the range from the MAC header to the FCS field over the frame length.
All packets	Number of packets (receive statistics include statistics on error packets whereas send statistics do not)#1
Unicast packets	Number of unicast packets

Item	Displayed information
Multicast packets	Number of multicast packets
Broadcast packets	Number of broadcast packets
Pause packets	Number of pause packets
<Out/In packets counter>	Send and receive statistics (including statistics on error packets) #1
64 packets	The number of packets whose frame length is 64 octets.
65-127 packets	The number of packets whose frame length is from 65 to 127 octets.
128-255 packets	The number of packets whose frame length is from 128 to 255 octets.
256-511 packets	The number of packets whose frame length is from 256 to 511 octets.
512-1023 packets	The number of packets whose frame length is from 512 to 1023 octets.
1024- packets	The number of packets whose frame length is 1024 octets or longer#2.
<Out line error counter>	Send error statistics
Late collision	The number of collisions detected after the 512-bit time has elapsed (This item is displayed only for 10BASE-T/100BASE-TX/1000BASE-T ports and 100BASE-TX/1000BASE-T/2.5GBASE-T ports.)
Collisions	The number of collisions detected (This item is displayed only for 10BASE-T/100BASE-TX/1000BASE-T ports and 100BASE-TX/1000BASE-T/2.5GBASE-T ports.)
Defer indication	The number of times the initial transmission was delayed because the transmit line was busy (This item is displayed only for 10BASE-T/100BASE-TX/1000BASE-T ports and 100BASE-TX/1000BASE-T/2.5GBASE-T ports.)
Excessive collisions	The number of transfer failures due to excessive collisions (16 collisions) (This item is displayed only for 10BASE-T/100BASE-TX/1000BASE-T ports and 100BASE-TX/1000BASE-T/2.5GBASE-T ports.)
Underrun	The number of underruns or CRC errors that occurred
Error frames	The total number of frames discarded due to errors (total value of Late collision, Excessive collisions, and Underrun values)
<In line error counter>	Receive error statistics
CRC errors	The number of times the frame length was valid but an error was detected by the FCS check
Alignment	The number of times the frame length was invalid and an error was detected by the FCS check
Fragments	The number of times a short frame (whose length was shorter than 64 octets) was received and an FCS error occurred
Jabber	The number of times a long frame (whose length exceeded the max frame length) was received and an FCS error occurred
Symbol errors	The number of symbol errors that occurred
Short frames	The number of received packets that are shorter than the frame length
Long frames	The number of received packets that exceed the frame length
Overrun	The number of overruns that occurred

Item	Displayed information
Error frames	The total number of frames discarded due to errors (total value of Short frames, Fragments, Jabber, CRC errors, Long frames, Overrun, and Symbol errors values)
<Line fault counter>	Failure statistics (This item is displayed only for 10BASE-T/100BASE-TX/1000BASE-T ports and 100BASE-TX/1000BASE-T/2.5GBASE-T ports.)
Polarity changed	The number of times the polarity of the send or receive pin of a twisted pair cable was changed
Link down	The number of times a link was not established
Link down in operational state	The number of link failures that occurred during communication (a link was not established)
<Line fault counter>	Failure statistics (For SFP ports or SFP+/SFP shared ports)
Link down	The number of times a link was not established
TX fault	The number of times a send line failure occurred
Signal detect errors	The number of times a signal line could not be detected
Transceiver notconnect	The number of times a transceiver was removed
Link down in operational state	The number of link failures that occurred during communication (a link was not established)
Signal detect errors in operational state	The number of failures that occurred during communication (signal line was not detected)
Transceiver notconnect in operational state	The number of failures that occurred during communication (transceiver was removed)

#1: It does not include the number of pause packets.

#2: The maximum frame length is equivalent to the MTU.

Impact on communication

None

Notes

1. All display items are cleared when:
   - The device starts up.
   - A device hardware failure occurs.
   - A failure occurs in the network interface management program (nimd).
2. If the model supports 10G uplink with an optional license but the license for 10G uplink is not registered, inserting an SFP+ transceiver changes the transceiver status to not support.

clear counters

Clears the Ethernet statistics counters to zero. The following information is cleared:

- Send and receive statistics
- Send error statistics
- Receive error statistics
- Failure statistics

Syntax

```
clear counters
clear counters <interface type> <interface number>
```

Input mode

User mode and administrator mode

Parameters

<interface type> <interface number>

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below.

For details, see "■How to specify an interface" in "Specifiable values for parameters".

- Ethernet interface

Behavior when all parameters are omitted:

The statistics counters of all Ethernet interfaces are cleared to zero.

Example and display items

None

Impact on communication

None

Notes

- Even if the statistics counters are cleared to zero, the values of the MIB information obtained by using SNMP are not cleared to zero.
- All display items are cleared when:
  - A failure occurs in the network interface management program (nimd).

show port

Lists information about the Ethernet ports implemented on the device.

Syntax

```
show port [<port list>]
show port protocol [<port list>]
show port statistics [<port list>] [{ up | down }] [discard]
show port transceiver [<port list>] [detail]
show port vlan [<port list>] [{ access | trunk | protocol | mac | tunnel }]
show port eee [<port list>]
```

Input mode

User mode and administrator mode

Parameters

<port list>

Lists information about the port numbers specified for Ethernet ports in list format. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

Information is listed without any qualifications regarding ports.

protocol

Displays the protocol information of the port.

statistics

Displays the number of sent, received, and discarded packets for ports implemented on the device.

{ up | down }

up

Displays information for ports whose status is up.

down

Displays information for ports whose status is not up. The statuses other than up are as follows:

- down: A line failure has occurred.
- init: Initialization or auto-negotiation is in progress.
- test: A line test is in progress.
- fault: Failure occurred
- inact: Operation has been stopped by the "inactivate" command.
- dis: Operation was stopped by using the "shutdown" configuration command.

Behavior when this parameter is omitted:

Information is listed without any qualifications regarding ports.

discard

Displays only the information for ports on which the number of discarded packets is 1 or more.

Behavior when this parameter is omitted:

Information is listed with no conditions applied.

transceiver

Lists information about whether transceivers are installed on ports that can use removable transceivers and provides type and identification information.

This parameter allows you to check the identification information of each transceiver.

detail

Displays detailed information about transceivers.

Behavior when this parameter is omitted:

Normal information about transceivers is displayed.

vlan

Displays VLAN information for ports.

{ access | trunk | protocol | mac | tunnel }

Specifies one of the above keywords as the type of port for which information is to be displayed.

access

Displays VLAN information for access ports.

trunk

Displays VLAN information for trunk ports.

protocol

Displays VLAN information for protocol ports.

mac

Displays VLAN information for MAC ports.

tunnel

Displays VLAN information for tunneling ports.

Behavior when this parameter is omitted:

The information for all types of ports is displayed.

eee

Displays EEE information for ports.

Behavior when all parameters are omitted:

The information for all implemented Ethernet ports is listed.

Example 1

Figure 20-4: Example of listing the link information for ports

```
> show port
Date 20XX/01/14 10:56:37 UTC
Port Counts: 54
Port    Name           Status   Speed               Duplex     FCtl FrLen ChGr/Status
 1/0/ 1 geth1/0/1      up       1000BASE-T          full(auto) off   1522   1/up
 1/0/ 2 geth1/0/2      inact    1000BASE-T          full       off   1522   -/-
 1/0/ 3 geth1/0/3      down     -                   -          -     -      -/-
       :
       :
       :
 1/0/49 geth1/0/49     down     -                   -          -     -      -/-
 1/0/50 geth1/0/50     up       1000BASE-T          full(auto) off   1522   1/up
 1/0/51 tengeth1/0/51  up       1000BASE-T          full       off   1522   -/-
 1/0/52 tengeth1/0/52  up       10GBASE-SR          full       off   1522  32/up
 1/0/53 tengeth1/0/53  down     -                   -          -     -      -/-
 1/0/54 tengeth1/0/54  up       10GBASE-SR          full       off   1522  32/up
>
```

Display items in Example 1

Table 20-5: Description of displayed items in the link information list for ports

Item	Meaning	Displayed detailed information
Port Counts	Number of target ports	—
Port	Port	Switch number/NIF number/port number
Name	Port name	The name assigned to the port is displayed.
Status	Port status	up: Active (up and running normally) down: Active (A line failure occurred.) init: Currently initializing or waiting for establishment of negotiation (auto-negotiation function is active). test: A line test is in progress. fault: Failure occurred inact: Operation has been stopped by the "inactivate" command. • The standby link function of link aggregation • The BPDU guard function of the Spanning Tree Protocol • The port has been deactivated by the unidirectional link failure detection function. • The port has been deactivated by the L2 loop detection function. • The port has been deactivated by storm control. • The port has been deactivated by port resetting of uplink redundancy. dis: Operation was stopped by using the "shutdown" configuration command.
Speed	Line speed	Displays the connection interface. 10BASE-T: 10BASE-T 100BASE-TX: 100BASE-TX 1000BASE-T: 1000BASE-T 1000BASE-LX: 1000BASE-LX 1000BASE-SX: 1000BASE-SX 1000BASE-LH: 1000BASE-LH 1000BASE-BX10-D: 1000BASE-BX10-D 1000BASE-BX10-U: 1000BASE-BX10-U 1000BASE-BX40-D: 1000BASE-BX40-D 1000BASE-BX40-U: 1000BASE-BX40-U 2.5GBASE-T: 2.5GBASE-T 10GBASE-SR: 10GBASE-SR 10GBASE-LR: 10GBASE-LR 10GBASE-ER: 10GBASE-ER 10GBASE-CU30CM: 10GBASE-CU (30cm) 10GBASE-CU1M: 10GBASE-CU (1m) 10GBASE-CU3M: 10GBASE-CU (3m) 10GBASE-CU5M: 10GBASE-CU (5m)

Item	Meaning	Displayed detailed information
		10GBASE-BR10-D: 10GBASE-BR10-D 10GBASE-BR10-U: 10GBASE-BR10-U 10GBASE-BR40-D: 10GBASE-BR40-D 10GBASE-BR40-U: 10GBASE-BR40-U -: The line speed is unknown (If auto-negotiation is enabled for a 10BASE-T/100BASE-TX/1000BASE-T or 100BASE-TX/1000BASE-T/2.5GBASE-T port and Status is neither up nor test, if Status is init or fault, or if the transceiver status is not connect, a hyphen (-) is displayed.)
Duplex	Duplex mode	full: Full duplex full(auto): Full duplex (resulting from auto-negotiation) half: Half duplex half(auto): Half duplex (resulting from auto-negotiation) -: The Duplex is unknown (If auto-negotiation is enabled for a 10BASE-T/100BASE-TX/1000BASE-T or 100BASE-TX/1000BASE-T/2.5GBASE-T port and Status is neither up nor test, if Status is init or fault, or if the transceiver status is not connect, a hyphen (-) is displayed.)
FCtl	Flow control	on: Flow control is enabled. off: Flow control is disabled. -: Status is neither up nor test.
FrLen	Maximum frame length	Displays the maximum frame length of the port in octets. -: Status is neither up nor test.
ChGr /Status	Channel group and status	The channel group to which the port belongs and the status. Channel group number: 1 to 120 up: Data packets can be sent and received. down: Data packets cannot be sent or received. dis: Link aggregation is disabled. For a port that does not belong to link aggregation, "-/-" is displayed.

Example 2

Figure 20-5: Example of listing the protocol information for ports

```
> show port protocol
Date 20XX/01/14 10:56:37 UTC
Port Counts: 54
Port    Name           Type        VLAN  STP   QoS Filter MACTbl   Ext.
 1/0/ 1 geth1/0/1      Protocl      100    0     0      0      0   - - - - - -
 1/0/ 2 geth1/0/2      Mac         1024    0   100    100      7   - - - - - -
 1/0/ 3 geth1/0/3      Trunk        256    0     0      0      0   - - - - - -
 1/0/ 4 geth1/0/4      Protocol      16    0     1      1      0   - - - - - -
            :
            :
            :
 1/0/51 tengeth1/0/51  Access         1    0     0      0      0   - - - - - -
 1/0/52 tengeth1/0/52  Access         1    0     0      0      0   - - - - - -
 1/0/53 tengeth1/0/53  Access         1    0     0      0      0   - - - - - -
 1/0/54 tengeth1/0/54  Access         1    0     0      0      0   - - - - - -
>
```

Display items in Example 2

Table 20-6: Displayed items for the protocol information list for ports

Item	Meaning	Displayed detailed information
Port Counts	Number of target ports	—
Port	Port	Switch number/NIF number/port number
Name	Port name	The name assigned to the port is displayed.
Type	Port type	Protocol: Protocol VLAN port Trunk: Trunk port Access: Access port Mac: MAC VLAN port Tunnel: Tunneling port
VLAN	Number of VLANs that share the port	Number of VLANs that share the port (including the default VLAN and VLANs in suspend state)
STP	The number used in the Spanning Tree topology calculation	When single is used: 1 When pvst+ is used: The number of VLANs set by pvst+ When mstp is used: The number of instances (When single and pvst+ are mixed, the number of VLANs set by pvst+ + 1)
QoS	Number of QoS flow lists	Displays the number of QoS flow lists set for the port. This number includes the number of QoS flow lists set for the VLAN to which the port belongs.
Filter	Number of access lists	Displays the number of access lists set for the port. This number includes the number of access lists set for the VLAN to which the port belongs. Note that this value does not include the number of implicitly discarded access lists.
MACTbl	Number of dynamically learned entries in the MAC address table	Displays the number of dynamically learned MAC address table entries.
Ext.	Extended function information	I: Indicates that relay blocking information is set. S: Indicates that storm control information is set. T: Indicates that tag translation is set. L: Indicates that LLDP is running. A: Indicates that the Ring Protocol is running. "-" is displayed if the relevant extended function is not set or is not running.

Example 3

Figure 20-6: Example of displaying the number of sent, received, and discarded packets for ports

```
> show port statistics
Date 20XX/01/14 10:56:37 UTC
Port Counts: 54
Port    Name           Status T/R  All packets   Multicast   Broadcast     Discard
 1/0/ 1 geth1/0/1      up     Tx         36060       36012          48           0
                              Rx  267868905982 67868905982           0           0
 1/0/ 2 geth1/0/2      inact  Tx             0           0           0           0
                              Rx             0           0           0           0
 1/0/ 3 geth1/0/3      down   Tx             0           0           0           0
                              Rx             0           0           0           0
 1/0/ 4 geth1/0/4      down   Tx             0           0           0           0
                              Rx             0           0           0           0
```

```
 1/0/ 5 geth1/0/5      down   Tx             0           0           0           0
                              Rx             0           0           0           0
             :
             :
             :
 1/0/49 geth1/0/49     down   Tx             0           0           0           0
                              Rx             0           0           0           0
 1/0/50 geth1/0/50     up     Tx          5679           0          10           0
                              Rx          5158           0          11           0
 1/0/51 tengeth1/0/51  up     Tx   41601114258 32945109231           1           0
                              Rx    6352088724       15118           8           0
 1/0/52 tengeth1/0/52  up     Tx  230169902708 25895910148      557807           0
                              Rx   34671538289       66885     1487508           0
 1/0/53 tebgeth1/0/53  down   Tx             0           0           0           0
                              Rx             0           0           0           0
 1/0/54 tebgeth1/0/54  up     Tx   42422843302 41973185821         160           0
                              Rx    5839856540        5593       42399           0
>
```

Display items in Example 3

Table 20-7: Display items of the number of sent, received, and discarded packets for ports

Item	Meaning	Displayed detailed information
Port Counts	Number of target ports	—
Port	Port	Switch number/NIF number/port number
Name	Port name	The name assigned to the port is displayed.
Status	Port status	up: Active (up and running normally) down: Active (A line failure occurred.) init: Currently initializing or waiting for establishment of negotiation (auto-negotiation function is active). test: A line test is in progress. fault: Failure occurred inact: Operation has been stopped by the "inactivate" command. • The standby link function of link aggregation • The BPDU guard function of the Spanning Tree Protocol • The port has been deactivated by the unidirectional link failure detection function. • The port has been deactivated by the L2 loop detection function. • The port has been deactivated by storm control. • The port has been deactivated by port resetting of uplink redundancy. dis: Operation was stopped by using the "shutdown" configuration command.
T/R	Receiving/sending	Tx: Sending Rx: Receiving
All packets	Number of all packets (including error packets)	
Multicast	Number of multicast packets	
Broadcast	Number of broadcast packets	

Item	Meaning	Displayed detailed information
Discard	Number of discarded packets	

Example 4

Figure 20-7: Example of listing the detailed transceiver information (if the transceiver type is SFP or SFP+)

```
> show port transceiver 1/0/51-52 detail
Date 20XX/01/14 10:56:38 UTC
Port Counts: 2
Port: 1/0/51 Status:notconnect  Type:-  Speed:-
             Vendor name:-                    Vendor SN :-
             Vendor PN  :-                    Vendor rev:-
             Tx power   :-                    Rx power  :-
Port: 1/0/52 Status:connect  Type:SFP+  Speed:10GBASE-SR
             Vendor name:xxxxxxxxxxxxxxx      Vendor SN :xxxxxxxxxxxxxxx
             Vendor PN  :xxxxxxxxxxxxxxx      Vendor rev:xxxx
             Tx power   :-2.0dBm              Rx power  :-2.4dBm
>
```

Display items in Example 4

Table 20-8: Display items of the transceiver information list (if the transceiver type is SFP or SFP+)

Item	Meaning	Displayed detailed information
Port Counts	Number of target ports	—
Port	Port	Switch number/NIF number/port number
Status	Status of the transceiver	connect: Installed notconnect: Not installed not support: An unsupported transceiver is installed. -: The status of the transceiver is unknown (- is displayed if the port status is init or fault).
Type	Type of transceiver	SFP: SFP or SFP-T SFP+: SFP+ -: The type of the transceiver is unknown (- is displayed if the transceiver status is notconnect).
Speed	Line speed	Displays the connection interface. 10BASE-T/100BASE-TX/1000BASE-T: 10BASE-T/100BASE-TX/1000BASE-T 1000BASE-LX: 1000BASE-LX 1000BASE-SX: 1000BASE-SX 1000BASE-LH: 1000BASE-LH 1000BASE-BX10-D: 1000BASE-BX10-D 1000BASE-BX10-U: 1000BASE-BX10-U 1000BASE-BX40-D: 1000BASE-BX40-D 1000BASE-BX40-U: 1000BASE-BX40-U 10GBASE-SR: 10GBASE-SR 10GBASE-LR: 10GBASE-LR 10GBASE-ER: 10GBASE-ER 10GBASE-CU30CM: 10GBASE-CU (30cm) 10GBASE-CU1M: 10GBASE-CU (1m)

Item	Meaning	Displayed detailed information
		10GBASE-CU3M: 10GBASE-CU (3m) 10GBASE-CU5M: 10GBASE-CU (5m) 10GBASE-BR10-D: 10GBASE-BR10-D 10GBASE-BR10-U: 10GBASE-BR10-U 10GBASE-BR40-D: 10GBASE-BR40-D 10GBASE-BR40-U: 10GBASE-BR40-U -: Unknown line speed (- is displayed if the port status is init or fault, or if the transceiver status is not connect).
Vendor name	Vendor name	Displays the vendor's name.# 1, #2
Vendor SN	Vendor serial number	Displays the serial number added by the vendor.# 1, #2
Vendor PN	Vendor part number	Displays the part number added by the vendor.# 1, #2
Vendor rev	Vendor revision	Displays a part number revision added by the vendor.# 1, #2
Tx power	Sending optical power	Displays the sending optical power in dBm.# 1, #2, #3, #4
Rx power	Receiving optical power	Displays the receiving optical power in dBm.# 1, #2, #3, #4

#1: A hyphen (-) is displayed if the transceiver status is neither connect nor fault.

#2: **** is displayed while transceiver information is being loaded even if the transceiver status is neither connect nor fault. Information is displayed when you re-execute the command. If transceiver information could not be loaded, a hyphen (-) is displayed.

#3: If the optical power is outside the range from −40 to 8.2 dBm, a hyphen (-) is displayed.

#4: An error might arise depending on the ambient conditions. To check the correct value, use an optical power meter.

Example 5

Figure 20-8: Example of listing VLAN information for ports

```
> show port vlan
Date 20XX/01/15 14:15:00
Port Counts: 54
Port    Name           Status Type       VLAN
 1/0/ 1 geth1/0/1      up     Protocl    100 (Global IP Network VLAN)
 1/0/ 2 geth1/0/2      inact  Mac        1024
      :
      :
      :
 1/0/51 tengeth1/0/51  up     Trunk      32
 1/0/52 tengeth1/0/52  up     Trunk      32
 1/0/53 tengeth1/0/53  down   Access     1   (DefaultVLAN)
 1/0/54 tengeth1/0/54  up     Trunk      32
>
```

Figure 20-9: Example of listing VLAN information for trunk ports

```
> show port vlan trunk
Date 20XX/11/15 14:15:00
Port Counts: 2
Port    Name           Status Type       VLAN
 1/0/ 3 geth1/0/3      up     Trunk      1-4094
 1/0/ 4 geth1/0/4      up     Trunk      1,3,5,7,9,11,13,15,17,19,21,23,25,27,
                                         29,31,33,35,37,39,41,43,45,47,49,120,
                                         130,140
```

Display items in Example 5

Table 20-9: Display items of the VLAN information list for ports

Item	Meaning	Displayed detailed information
Port counts	Number of target ports	—
Port	Port number	Switch number/NIF number/port number of the port whose information is to be displayed
Name	Name	The name assigned to a port
Status	Port status	up: Active (up and running normally) down: Active (A line failure occurred.) init: Currently initializing or waiting for establishment of negotiation (auto-negotiation function is active). test: A line test is in progress. fault: Failure occurred inact: Operation has been stopped by the "inactivate" command. • The standby link function of link aggregation • The BPDU guard function of the Spanning Tree Protocol • The port has been deactivated by the unidirectional link failure detection function. • The port has been deactivated by the L2 loop detection function. • The port has been deactivated by storm control. • The port has been deactivated by port resetting of uplink redundancy. dis: Operation was stopped by using the "shutdown" configuration command.
Type	Port type	Access: Access port Trunk: Trunk port Protocol: Protocol VLAN port Mac: MAC VLAN port Tunnel: Tunneling port
VLAN	VLAN ID	The list of VLANs set for a port. If only one VLAN has been set, the VLAN name is also displayed. If no VLAN exists, a hyphen (-) is displayed.

Example 6

Figure 20-10: Example of listing EEE information

```
> show port eee
Data 20XX/03/09 13:48:30 UTC
Port Counts: 48
Port    Name           Status  Config    Current      Tx-LPI  Rx-LPI
 1/0/ 1 geth1/0/1      up      enabled   operational  on      on
 1/0/ 2 geth1/0/2      up      disabled  disagreed    off     off
     :
 1/0/48 geth1/0/48     up      enabled   disagreed    off     off
```

Display items in Example 6

Table 20-10: Display items of the EEE information list

Item	Meaning	Displayed detailed information
Port counts	Number of target ports	—
Port	Port number	Switch number/NIF number/port number of the port whose information is to be displayed
Name	Name	The name assigned to a port
Status	Port status	up: Active (up and running normally) down: Active (A line failure occurred.) init: Currently initializing or waiting for establishment of negotiation (auto-negotiation function is active). test: A line test is in progress. fault: Failure occurred inact: Operation has been stopped by the "inactivate" command. • The standby link function of link aggregation • The BPDU guard function of the Spanning Tree Protocol • The port has been deactivated by the unidirectional link failure detection function. • The port has been deactivated by the L2 loop detection function. • The port has been deactivated by storm control. • The port has been deactivated by port resetting of uplink redundancy. dis: Operation was stopped by using the "shutdown" configuration command.
Config	Setting status of the EEE function	enabled: The EEE function is enabled. disabled: The EEE function is disabled
Current	Current EEE running status	operational: The EEE function is running. disagreed: The EEE function is disabled due to a disagreement in EEE auto-negotiation. -: Status is neither up nor test.
Tx-LPI	Sending-side power saving status	on: Running in power saving mode off: Running in normal mode after the power saving mode is exited -: Status is neither up nor test.
Rx-LPI	Receiving-side power saving status	on: Running in power saving mode off: Running in normal mode after the power saving mode is exited -: Status is neither up nor test.

Impact on communication

None

Notes

1. The displayed number of discarded packets is the total of the values for the items listed in the following table.

Table 20-11: Statistical items used to calculate the number of discarded packets

Port	Statistical item	
	Sending	Receiving
Ethernet	Late collision Excessive collisions Underrun	CRC errors Fragments Symbol errors Short frames Long frames Overrun

2. The statistic counter is cleared when:
   - The device starts up.
   - The "clear counters" command is executed.
   - A device hardware failure occurs.
   - A failure occurs in the network interface management program (nimd).
3. If the model supports 10G uplink with an optional license but the license for 10G uplink is not registered, inserting an SFP+ transceiver changes the transceiver status to not support.

activate

Returns the status of the Ethernet port to active from inactive when the "inactivate" command has been used to set inactive.

Syntax

```
activate <interface type> <interface number>
```

Input mode

User mode and administrator mode

Parameters

<interface type> <interface number>

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below.

For details, see "■How to specify an interface" in "Specifiable values for parameters".

- Ethernet interface

Example

In the following example, the status of the port whose switch number is 1, NIF number is 0, and port number is 1 is reset to active.

```
activate gigabitethernet 1/0/1
```

Display items

None

Impact on communication

Communication using the relevant Ethernet port resumes.

Notes

Executing this command does not change the configuration.

inactivate

Changes the status of an Ethernet port from active to inactive without changing the configuration.

Syntax

```
inactivate <interface type> <interface number>
```

Input mode

User mode and administrator mode

Parameters

<interface type> <interface number>

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below.

For details, see "■How to specify an interface" in "Specifiable values for parameters".

- Ethernet interface

Example

In the following example, the status of the port whose switch number is 1, NIF number is 0, and port number is 1 is changed to inactive.

```
inactivate gigabitethernet 1/0/1
```

Display items

None

Impact on communication

Communication using the relevant Ethernet port becomes unavailable.

Notes

- Executing this command does not change the configuration.
- If the device is restarted after command execution, the inactive status is canceled.
- To re-activate an Ethernet port that has been inactivated by this command, use the "activate" command.
- This command cannot be executed for a port for which a line test is being conducted. Before executing the command, make sure you use the "no test interfaces" command to stop the line test.

test interfaces

If an error occurs in communication over an Ethernet network, this command can be used to identify the fault location. After the fault location (such as a transceiver) has been replaced, this command can also be used to verify whether communication takes places properly (conduct a line test) on a frame basis.

Before you conduct a line test, make sure you use the "inactivate" command to change the status of the port to inactive. For details about the line tests, see "Troubleshooting Guide".

Syntax

```
test interfaces <interface type> <interface number> {internal | connector}
     [auto_negotiation {10base-t | 100base-tx | 1000base-t | 2500base-t}]
     [interval <interval time>] [pattern <test pattern no.>]
     [length <data length>]
```

Input mode

User mode and administrator mode

Parameters

<interface type> <interface number>

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below.

For details, see "■How to specify an interface" in "Specifiable values for parameters". Note that you specify <interface number> without <switch no.>.

- Ethernet interface

internal

Specifies that an internal loopback test will be conducted.

connector

Specifies that a loop connector loopback test will be conducted.

Before you conduct a loop connector loopback test, make sure that the loop connector has been connected.

auto_negotiation {10base-t | 100base-tx | 1000base-t | 2500base-t}

Specifies the segment standard that will be used for a line test conducted when "auto" is specified in the "speed" configuration command.

Note that this parameter can be specified only when "auto" is specified in the "speed" command. Specify "gigabitethernet" for <interface type>.

The following table shows the combination of a port type and specifiable parameters.

Table 20-12: Specifiable parameters

Port type	Specifiable parameters
10BASE-T/100BASE-TX/1000BASE-T port	10base-t 100base-tx 1000base-t
100BASE-TX/1000BASE-T/2.5GBASE-T port	100base-tx 1000base-t 2500base-t

Behavior when this parameter is omitted:

The command assumes that 100base-tx is specified.

interval <interval time>

Specifies the number of seconds as the sending interval. You can specify a decimal number from 1 to 30.

Behavior when this parameter is omitted:

The sending interval defaults to 1 second.

pattern <test pattern no.>

Specifies the number of the test pattern. You can specify a value from 0 to 4.

0: Repeats test patterns 1 to 4 in turn.

1: all 0xff

2: all 0x00

3: ** THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG.0123456789 **

pattern repeated

4: Sends a data corruption detection pattern.

Behavior when this parameter is omitted:

Test pattern 3 is used.

length <data length>

Specifies in octets the data length of the frame (excluding the MAC header and the FCS field) to be used for the test. For the value that you can specify, see the following table.

Table 20-13: Specifiable range of values for each test

No	Test type	Data length (in octets)	Default (in octets)
1	Internal loopback test	46 to 1500	500
2	Loop connector loopback test	46 to 9216#	500

#: If 10base-t is set for the auto_negotiation parameter, the maximum that can be specified is 1500 octets.

Behavior when all parameters are omitted:

The command works as described in each "Behavior when this parameter is omitted" section.

Example

The following figure shows an example of the screen displayed at the start of an Ethernet line test. This example starts an internal loopback test that sends a 100-octet frame in the all-0xff test pattern at five-second intervals to the port number of 2.

Figure 20-11: Starting a line test

```
> test interfaces  gigabitethernet 0/2 internal interval 5 pattern 1 length 100
```

Display items

None

Impact on communication

None

Notes

- Before you insert or remove a loop connector, make sure that the port is in inactive status.
- After a line test has started, the test processing is repeated until a request to stop the test is issued.
- To conduct a loop connector loopback test by specifying 1000base-t for the auto_negotiation parameter, an eight-core, four-pair loop connector of category 5 or higher is required.
- Conduct a line test on a port-by-port basis.
- To conduct a loop connector loopback test on a 1000BASE-LH or 10GBASE-ER port, an optical attenuator is required. For details about optical attenuation, see the following table.

  Table 20-14: Optical attenuation

Line type	Attenuation value (dB)
1000BASE-LH	5 to 22
10GBASE-ER	5 to 11

- You cannot conduct a normal loop connector loopback test on a 1000BASE-BX port because the port uses different wavelengths for sending and receiving and uses a one-core optical fiber cable.
- You cannot conduct a normal loop connector loopback test on a 10GBASE-BR port because the port uses different wavelengths for sending and receiving and uses a one-core optical fiber cable.
- If you connect or disconnect a transceiver while a line test is being conducted, all count values displayed in the test results might be 0. In addition, when you connect or disconnect a transceiver, if you start a line test before an operation message indicating that a transceiver was connected or disconnected is displayed, the operation message might not be output. In both cases, you can continue operation because the normal operating status is restored after you execute the "no test interfaces" command.
- The loop connector loopback test cannot be conducted when SFP-T is in use.
- When a 100BASE-TX/1000BASE-T/2.5GBASE-T port is used, the module internal loopback test cannot be conducted on a 100BASE-TX or 1000BASE-T port, and the loop connector loopback test cannot be conducted on a 1000BASE-T or 2.5GBASE-T port.

no test interfaces

Stops an Ethernet line test, and displays the test results.

For details about the line tests, see "Troubleshooting Guide".

Syntax

```
no test interfaces <interface type> <interface number>
```

Input mode

User mode and administrator mode

Parameters

<interface type> <interface number>

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below.

For details, see "■How to specify an interface" in "Specifiable values for parameters". Note that you specify <interface number> without <switch no.>.

- Ethernet interface

Example

This example starts an internal loopback test that sends a 100-octet frame in the all-0xff test pattern at five-second intervals. The following figure shows the result of conducting a line test.

Figure 20-12: Result of conducting a line test

```
>test interfaces gigabitethernet 0/2 internal interval 5 pattern 1 length 100
>no test interfaces gigabitethernet 0/2
Date 20XX/10/23 12:00:00 UTC
Interface type             :1000BASE-LX
Test count                 :60
Send-OK                    :60             Send-NG               :0
Receive-OK                 :60             Receive-NG            :0
Data compare error         :0
Out buffer hunt error      :0              Out line error        :0
In CRC error               :0              In alignment          :0
In monitor time out        :0              In line error         :0
H/W error                  :none
>
```

Display items

Table 20-15: Items displayed as a line test result

Item	Meaning	Presumed cause	Measures
Interface type	Line type (which displays the connection interface) • 10BASE-T • 100BASE-TX • 1000BASE-T • 1000BASE-LX	—	—

Item	Meaning	Presumed cause	Measures
	• 1000BASE-SX • 1000BASE-LH • 1000BASE-BX10-D • 1000BASE-BX10-U • 1000BASE-BX40-D • 1000BASE-BX40-U • 2.5GBASE-T • 10GBASE-SR • 10GBASE-LR • 10GBASE-ER • 10GBASE-CU30CM • 10GBASE-CU1M • 10GBASE-CU3M • 10GBASE-CU5M • 10GBASE-BR10-D • 10GBASE-BR10-U • 10GBASE-BR40-D • 10GBASE-BR40-U • ----[#1]		
Test count	Number of times the test was conducted	—	—
Send-OK	Number of times data was sent normally	—	—
Send-NG	Number of times data was sent abnormally	Sum of frames discarded due to a line failure	For a loop connector loopback test, verify that a loopback connector is correctly connected to the port.
Receive-OK	Number of times data was received normally	—	—
Receive-NG	Number of times data was received abnormally	Sum of the number of times a data compare error occurred and the number of times reception monitoring timed out	See Data compare error and subsequent items in this table.
Data compare error	Number of data compare errors (number of received frames that did not match the sent frames)	Line failure	Replace the device.
Out buffer hunt error	Number of times a send buffer could not be secured	Congestion on another port	Resolve the congestion on the other port, and then try again.
Out line error	Number of send line failures that occurred	Line failure	Replace the device.
In CRC error	The number of times the frame length was valid but an error was detected by the FCS check[#2]	Line failure	Replace the device.

Item	Meaning	Presumed cause	Measures
In alignment	The number of times the frame length was invalid and an error was detected by the FCS check#2	Line failure	Replace the device.
In monitor time out	Timeout for the reception monitoring timer	Line failure	For a loop connector loop-back test, verify that a loop-back connector is correctly connected to the port.# 3
In line error	Number of receive line failures that occurred	Line failure	For a loop connector loop-back test, verify that a loop-back connector is correctly connected to the port.
H/W error	Whether a hardware failure has occurred. none: No hardware error occurred. occurred: A hardware error occurred.	Line failure	Replace the device.

#1: The line type is unknown. This is indicated when:

- The transceiver status is not connect.
- A line test was stopped immediately after it started.
- A line failure occurred.

#2: The frame length indicates the length from the MAC header to the FCS field. For details about frame formats, see "Configuration Guide Vol. 1, 20.2.2 Frame format".

#3: If the loop connector is connected correctly, and if test is the internal loopback test, the packets for the line test might have accumulated in the device. Make sure that the packet forwarding load on the device on which the line test is being conducted is low, and then try again. If the value of the item still increments even after the line test is conducted multiple times, replace the device.

Impact on communication

None

Notes

- Before you insert or remove a loop connector, make sure that the port is in inactive status.
- When a line test is stopped, depending on the timing, the test might stop while the command is waiting for the response to a test frame that was sent. Therefore, in the displayed test results, the total of Receive-OK and Receive-NG values could be one smaller than the Send-OK value.

show power inline

Displays the usage of the device and the PoE information for each port so that PoE power can be controlled.

Syntax

```
show power inline [<port list>] [{on | off | faulty | denied | inact | wait}]
[{critical | high | low | never}]
```

Input mode

User mode and administrator mode

Parameters

<port list>

Specifies a list of ports for which you want to display the PoE information. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

The PoE information for all ports that support PoE is listed.

{on | off | faulty | denied | inact | wait}

on

Displays information about a port that is supplying power (the power supply status is on).

off

Displays information about a port that is not supplying power (the power supply status is off).

faulty

Displays information about a port that is not supplying power because of a failure on the connected device (the power supply status is faulty).

denied

Displays information about a port that is not supplying power because of a power shortage (the power supply status is denied).

inact

Displays information about a port where supplying power is suspended by an operation command (the power supply status is inact).

wait

Displays information about a port that is waiting for supplying power to start by the PoE time-shifting power supply (the power supply status is wait).

{critical | high | low | never}

critical

Displays information about a port whose priority setting for supplying power is set to critical.

high

Displays information about a port whose priority setting for supplying power is set to high.

low

Displays information about a port whose priority setting for supplying power is set to low.

never

Displays information about a port for which the PoE function is set to never.

Specifying parameters

This command can display only the information relevant to the condition applied by a parameter that has been set. If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information conforming to all the conditions will be displayed.

Behavior when all parameters are omitted:

The PoE information for all ports that support PoE is listed.

Example

Figure 20-13: Example of listing PoE information

```
> show power inline
Date 20XX/02/24 16:24:01 UTC
System Wattage:
Threshold(W)              :   785.0
Total Allocate(W)         :   218.4
Total Power(W)            :   142.2
Priority Control          :  enable
System Delay Time(sec)    :    3600
Port Delay Time(sec)      :      60
Port Counts               :      48
 Port   Status Priority Type Class  Alloc(mW) Power(mW) Vol(V) Cur(mA) Description
 1/0/1  on     critical SP   manual     30000     26900   53.8      501 Port 1/0/1
 1/0/2  off    never    -    -              0         0    0.0        0
 1/0/3  off    never    -    -              0         0    0.0        0
 1/0/4  on     critical SP   4          30000      4400   54.0       82 Port 1/0/4
 1/0/5  on     low      SP   3          15400      1600   54.2       30 Port 1/0/5
 1/0/6  on     low      SP   1           4000       700   54.1       14
 1/0/7  on     low      SP   2           7000      1100   54.1       21
 1/0/8  faulty high     -    -              0         0    0.0        0 Port 1/0/8
  :
  :
 1/0/21  on     high    SS   6          60000     48000   53.8      892 Port 1/0/21
 1/0/22  on     low     SS   auto       12000     11500   54.1      212 Port 1/0/22
 1/0/23  inact  high    -    -              0         0    0.0        0 IPphone(1004)
 1/0/24  on     high    DS   4,4        60000     48000   53.8      892 Port 1/0/12
  :
  :
 1/0/47 wait   high     -    -              0         0    0.0        0
 1/0/48 wait   high     -    -              0         0    0.0        0 Port 1/0/48
>
```

Display items

Table 20-16: Items displayed for the power usage and setting information of the entire device

Item	Meaning	Displayed detailed information
System Wattage	Power used by the entire device	—
Threshold(W)	Threshold value for guaranteeing power to the entire device	Displays the threshold value of the range in which the supply of power is guaranteed (to the first decimal place). This is displayed in watts. If an attempt is made to supply power to a new port when the threshold value is exceeded, supplying power is stopped according to the priority control status.

Item	Meaning	Displayed detailed information
Total Allocate(W)	Amount of power allocated to PoE	Displays the amount of power allocated to PoE by the device (to the first decimal place). This is displayed in watts. The following values can be used to calculate the amount of power allocated to ports: Class0: 15.4 W Class1: 4.0 W Class2: 7.0 W Class3: 15.4 W Class4: 30.0 W Class5: 45.0 W Class6: 60.0 W manual: Amount of power allocated manually auto: Amount of power allocated with the Autoclass function
Total Power(W)	Total amount of power supplied to the entire device	Displays the total amount of power supplied to the entire device (to the first decimal place). This is displayed in watts.
Priority Control	Priority control status for supplying power on the device	enable: Enabled disable: Disabled
System Delay Time(sec)	Wait time before the device starts supplying power over PoE	Displays the wait time before the device starts supplying power from 0 to 3600. This is displayed in seconds.
Port Delay Time(sec)	Delay time to start supplying time on a PoE port	Displays the delay time, after the wait time before the device starts supplying power over PoE elapsed and prior to the start of power supply on the port over PoE, from 0 to 60. This is displayed in seconds.

Table 20-17: Items displayed for the PoE information of the port

Item	Meaning	Displayed detailed information
Port Counts	Number of ports	Displays the total number of the ports that meet the conditions.
Port	Port	Displays the port number of the interface.
Status	Power supply status	Displays the PoE status of a port. on: Power is being supplied. off: Power is not being supplied. faulty: Power cannot be supplied to the connected device. denied: Power is not being supplied due to a shortage of power. inact: Supply of power was suspended by an operation command. wait: The port is waiting for supplying power to start by the PoE time-shifting power supply.
Priority	Priority for supplying power	critical: Power is supplied as a port of the greatest importance. high: Power is supplied with the "high" priority. low: Power is supplied with the "low" priority. never: The PoE function is disabled. -: The port priority setting is disabled.
Type	Type of power supply to powered device	SP: Supplies power with one pair of wiring (Single Pairset) SS: Supplies power with two pairs of wiring and a single power feed (Single Signature) DS: Supplies power with two pairs of wiring and two power feeds (Dual Signature)

Item	Meaning	Displayed detailed information
Class#1	Power supply class	0: Power class Class 0 (15.4 W), which conforms to IEEE 802.3af 1: Power class Class 1 (4.0 W), which conforms to IEEE 802.3af 2: Power class Class 2 (7.0 W), which conforms to IEEE 802.3af 3: Power class Class 3 (15.4 W), which conforms to IEEE 802.3af 4: Power class Class 4 (30.0 W), which conforms to IEEE 802.3af 5: Power class Class 5 (45.0 W), which conforms to IEEE 802.3bt 6: Power class Class 6 (60.0 W), which conforms to IEEE 802.3bt manual: Allocate the amount of power supply manually auto: Allocate the amount of power supply with the Autoclass function -: Class not acquired or invalid
Alloc(mW)#2	Amount of power allocated	Displays the amount of power allocated to each port. This is displayed in milliwatts.
Power(mW)#2	Power consumption	Displays the amount of power consumed by each port. This is displayed in milliwatts.
Vol(V)	Voltage	Displays the voltage each port is using. This is displayed in volts.
Cur(mA)#2	Current	Displays the current each port is using. This is displayed in milliampere.
Description	Port name	Displays the setting configured by the "description" configuration command.

#1: When the type of power supply to powered device is "DS", two classes are displayed.

#2: When the type of power supply to powered device is "DS", the total current of the two pairs of wiring is displayed.

Impact on communication

None

Notes

- Total Allocate display item and the Power display item for each port
  The command collects the information for the Power display item on a port basis, which results in a time delay between collecting it from port 1 and the last port. Therefore, if the power supplied to a port fluctuates, the total value displayed in the Power display item (Threshold(W) value) can be exceeded. Note that it will not occur in the Total Allocate display item. There is also no problem in priority control setting because it works with the Total Allocate value.
- It will take some time to display the results of command execution.
- These amounts of allocated power have a little more margin than the displayed values. Therefore, the actual power consumption displayed may exceed the allocated amount of power.

activate power inline

Manually resumes supplying power.

Syntax

```
activate power inline gigabitethernet <port list>
```

Input mode

User mode and administrator mode

Parameters

gigabitethernet

Specifies that Ethernet interface.

<port list>

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

Example

Figure 20-14: Manually resuming the supply of power

```
> activate power inline gigabitethernet 1/0/1
```

Display items

None

Impact on communication

None

Notes

- After this command is used to manually resume supplying power (the status is on), executing the "shutdown" configuration command sets the status to the one with no power supply (off).

inactivate power inline

Manually stops supplying power.

Syntax

```
inactivate power inline gigabitethernet <port list>
```

Input mode

User mode and administrator mode

Parameters

gigabitethernet

Specifies that Ethernet interface.

<port list>

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

Example

Figure 20-15: Manually stopping the supply of power

```
> inactivate power inline gigabitethernet 1/0/1
```

Display items

None

Impact on communication

None

Notes

- After this command is used to manually stop supplying power (the status is inact), executing the "shutdown" configuration command sets the status to the one with no power supply (off).

21 Link Aggregation

show channel-group

Shows link aggregation information.

Syntax

```
show channel-group [{[<channel group list>] [detail] | summary}]
```

Input mode

User mode and administrator mode

Parameters

{[<channel group list>] [detail] | summary}

<channel group list>

Displays link aggregation information for the channel group numbers specified in list format. For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

All link aggregation information is displayed.

detail

Displays detailed link aggregation information.

Behavior when this parameter is omitted:

The link aggregation information is displayed.

summary

Displays summary information about link aggregation.

Behavior when this parameter is omitted:

Complete link aggregation information is displayed.

Example 1

The following shows an example of displaying information about link aggregation.

Figure 21-1: Displaying the link aggregation information

```
>show channel-group
Date 20XX/12/10 12:00:00 UTC
channel-group Counts:4
ChGr:1    Mode:LACP
  CH Status    :Up        Elapsed Time:10:10:39
  Load Balance:default
  Max Active Port:8
  Max Detach Port:7
  Description : 6 ports aggregated.
  MAC address: 0012.e2ac.8301     VLAN ID:
  Periodic Timer:Short
  Actor   information: System Priority:1     MAC: 0012.e212.ff02
                       KEY:1
  Partner information: System Priority:10000 MAC: 0012.e2f0.69be
                       KEY:10
  Port(6)        :1/0/1-3,10,12-13
  Up Port(2)     :1/0/1-2
  Down Port(4)   :1/0/3,10,12-13
ChGr:2    Mode:LACP
  CH Status    :Down      Elapsed Time:-
```

```
  Load Balance:default
  Max Active Port:8
  Max Detach Port:7
  MAC address: 0012.e2ac.8302     VLAN ID:30-35,40
  Periodic Timer:Long
  Actor   information: System Priority:1     MAC: 0012.e212.ff02
                       KEY:11
  Partner information: System Priority:10000 MAC: 0012.e2f0.69bd
                       KEY:20
  Port(3)        :1/0/4-6
  Up Port(0)     :
  Down Port(3)   :1/0/4-6
ChGr:3    Mode:Static
  CH Status    :Disabled  Elapsed Time:-
  Load Balance:default
  Max Active Port:8
  Max Detach Port:7
  MAC address: 0012.e2ac.8304     VLAN ID:200
  Port(2)        :1/0/7-8
  Up Port(0)     :
  Down Port(2)   :1/0/7-8
ChGr:4    Mode:Static
  CH Status    :Up        Elapsed Time:160.11:45:10
  Load Balance:default
  Max Active Port:2  (no-link-down mode)
  Max Detach Port:7
  MAC address: 0012.e2ac.8305     VLAN ID:250
  Port(3)        :1/0/9,14-15
  Up Port(2)     :1/0/9,14
  Down Port(1)   :1/0/15
  Standby Port(1):1/0/15
>
```

Display items in Example 1

Table 21-1: Display items for the link aggregation information

Item	Meaning	Displayed detailed information
channel-group Counts	Number of channel groups to be displayed	Number of channel groups
ChGr	Channel group number	Channel group number
Mode	Link aggregation mode	LACP: LACP link aggregation mode
		Static: Static link aggregation mode
		-: Link aggregation mode is not set.
CH Status	Channel group status	Up: Data packets can be sent and received.
		Down: Data packets cannot be sent or received.
		Disabled: Link aggregation is disabled.
Elapsed Time	Time the channel group has been Up	hh:mm:ss (when the elapsed time is less than 24 hours) ddd.hh:mm:ss (when the elapsed time exceeds 24 hours) Over 1000 days (when the elapsed time is more than 1000 days) "-" is displayed when the channel group status is not Up.

Item	Meaning	Displayed detailed information
Max Active Port	Maximum number of ports used by link aggregation	1 to 8 (8 is displayed as the initial value.) "-" is displayed when link aggregation mode is not set.
	Standby link mode	Standby link link-down mode
		(link-down mode): Link-down mode
		(no-link-down mode): Link-not-down mode
Max Detach Port	Restriction on the number of detached ports	0 or 7 (7 is displayed as the initial value.) "-" is displayed when link aggregation mode is not set.
Load Balance	Distribution method	default: The load is distributed according to the default distribution method of the Switch. For details, see "Configuration Guide Vol.1, 21.1.5 Port allocation for sending frames".
Description	Supplementary explanation regarding the channel group	This item is not displayed if a supplementary explanation has not been set in the configuration.
MAC Address	Channel group's MAC address	The MAC address of the group. One of the MAC addresses of the ports that belong to the group is used.
VLAN ID	VLAN ID of the VLAN to which the channel group belongs	VLAN ID
Periodic Time	Sending interval for LACPDU	This item is displayed only when LACP mode is enabled.
		Short: The sending interval is 1 second.
		Long: The sending interval is 30 seconds.
Actor information	Information about the actor system	Information about the actor system. This item is displayed only when LACP mode is enabled.
System Priority	System priority	Priority of the LACP system ID 1 to 65535 can be specified as the priority value (1 indicates the highest priority).
MAC	MAC address	The MAC address of the LACP system ID
KEY	Group key	Group key This value is the same as the channel group number.
Partner information	Information about the partner system	Information about the partner system. This item is displayed only when LACP mode is enabled. "-" is displayed if the partner system is not defined for LACP.
System Priority	System priority	Priority of the LACP system ID 0 to 65535 can be specified as the priority value (0 indicates the highest priority).
MAC	MAC address	MAC address
KEY	Group key	0 to 65535
Port(n)	Port information of a channel group	n: Number of ports Switch number/NIF number/port number of a channel group

Item	Meaning	Displayed detailed information
Up Port(n)	Information about ports that can be used for sending or receiving in a channel group	n: Number of ports that can be used for sending and receiving Switch number/NIF number/port number of a port that can be used for sending or receiving
Down Port(n)	Information about ports that cannot be used for sending or receiving in a channel group	n: Number of ports that cannot be used for sending and receiving Switch number/NIF number/port number of a port that cannot be used for sending or receiving (For a standby link in link-not-down mode, sending is impossible but receiving is possible.)
Standby Port(n)	Information about standby ports in a channel group	n: Number of standby ports Switch number/NIF number/port number of a port in a standby state

Example 2

The following shows an example of displaying summary information about link aggregation.

Figure 21-2: Displaying the summary information about link aggregation

```
>show channel-group summary
Date 20XX/07/14 12:00:00 UTC
CH Status            :ChGr ID
Up(2)                :1,3
Down(1)              :1
Disabled(1)          :3
>
```

Display items in Example 2

Table 21-2: Display items for the summary information about link aggregation

Item	Meaning	Displayed detailed information
Up(n)	Information about link aggregations in Up status	n: Number of link aggregations IDs of link aggregations in Up status
Down(n)	Information about link aggregations in Down status	n: Number of link aggregations IDs of link aggregations in Down status
Disabled(n)	Information about link aggregations in Disabled status	n: Number of link aggregations IDs of link aggregations in Disabled status

Example 3

The following shows an example of displaying detailed information about link aggregation.

Figure 21-3: Displaying the detailed information about link aggregation

```
>show channel-group detail
Date 20XX/12/10 12:00:00 UTC
channel-group Counts:4
ChGr:1    Mode:LACP
  CH Status    :Up        Elapsed Time:10:10:39
  Load Balance:default
  Max Active Port:8
  Max Detach Port:7
  Description : All 100M Full-Duplex
  MAC address: 0012.e2ac.8301     VLAN ID:
  Periodic Timer:Short
  Actor   information: System Priority:1     MAC: 0012.e212.ff02
```

```
                      KEY:1
  Partner information: System Priority:10000 MAC: 0012.e2f0.69be
                      KEY:10
  Port Counts:6       Up Port Counts:2
  Port:1/0/1   Status:Up    Reason: Partner-
               Speed :100M  Duplex:Full  LACP Activity:Active
               Actor   Priority:128     Partner Priority:100
  Port:1/0/2   Status:Up    Reason:-
               Speed :100M  Duplex:Full  LACP Activity:Active
               Actor   Priority:128     Partner Priority:100
  Port:1/0/3   Status:Down  Reason:LACPDU Expired
               Speed :100M  Duplex:Full  LACP Activity:Active
               Actor   Priority:128     Partner Priority:100
  Port:1/0/10  Status:Down  Reason:LACPDU Expired
               Speed: 100M  Duplex:Full  LACP Activity:Active
               Actor   Priority:128     Partner Priority:100
  Port:1/0/12  Status:Down  Reason:Partner Aggregation Individual
               Speed: 100M  Duplex:Full  LACP Activity:Active
               Actor   Priority:128     Partner Priority:100
  Port:1/0/13  Status:Down  Reason:Synchronization OUT_OF_SYNC
               Speed: 100M  Duplex:Full  LACP Activity:Active
               Actor   Priority:128     Partner Priority:100
ChGr:2    Mode:LACP
  CH Status    :Down      Elapsed Time:-
  Load Balance:default
  Max Active Port:8
  Max Detach Port:7
  MAC address: 0012.e2ac.8302     VLAN ID:30-35,40
  Periodic Timer:Long
  Actor   information: System Priority:1     MAC: 0012.e212.ff02
                      KEY:11
  Partner information: System Priority:10000 MAC: 0012.e2f0.69bd
                      KEY:20
  Port Counts:3       Up Port Counts:0
  Port:1/0/4   Status:Down    Reason:Port Down
               Speed :100M  Duplex:Full  LACP Activity:Active
               Actor   Priority:128     Partner Priority:100
  Port:1/0/5   Status:Down  Reason:Partner Key Unmatch
               Speed :100M  Duplex:Full  LACP Activity:Active
               Actor   Priority:128     Partner Priority:100
               Unmatched Partner Key:201
  Port:1/0/6   Status:Down  Reason:Partner System ID Unmatch
               Speed :100M  Duplex:Full  LACP Activity:Active
               Actor   Priority:128     Partner Priority:1
               Unmatched System ID:  Priority:5000   MAC:0012.e2f0.69ba
ChGr:3    Mode:Static
  CH Status    :Disabled  Elapsed Time:-
  Load Balance:default
  Max Active Port:8
  Max Detach Port:7
  MAC address: 0012.e2ac.8304     VLAN ID:200
  Port Counts:2       Up Port Counts:0
  Port:1/0/7   Status:Down  Reason:CH Disabled
               Speed :100M  Duplex:Full      Priority:128
  Port:1/0/8   Status:Down  Reason:CH Disabled
               Speed :100M  Duplex:Full      Priority:128
ChGr:4    Mode:Static
  CH Status    :Up        Elapsed Time:160.11:45:10
  Load Balance:default
  Max Active Port:2  (no-link-down mode)
  Max Detach Port:7
  MAC address: 0012.e2ac.8305     VLAN ID:250
  Port Counts:3       Up Port Counts:2
  Port:1/0/9   Status:Up    Reason:-
               Speed :100M  Duplex:Full      Priority:0
  Port:1/0/14  Status:Up    Reason:-
               Speed :100M  Duplex:Full      Priority:0
  Port:1/0/15  Status:Down  Reason:Standby
               Speed :100M  Duplex:Full      Priority:0
>
```

Display items in Example 3

Table 21-3: Display items for the detailed link aggregation information

Item	Meaning	Displayed detailed information
channel-group Counts	Number of channel groups to be displayed	Number of channel groups
ChGr	Channel group number	Channel group number
Mode	Link aggregation mode	LACP: LACP link aggregation mode
		Static: Static link aggregation mode
		-: Link aggregation mode is not set.
CH Status	Channel group status	Up: Data packets can be sent and received.
		Down: Data packets cannot be sent or received. (For a standby link in no-link-down mode, sending is impossible but receiving is possible.)
		Disabled: Link aggregation is disabled.
Elapsed Time	Time the channel group has been Up	hh:mm:ss (when the elapsed time is less than 24 hours) ddd.hh:mm:ss (when the elapsed time exceeds 24 hours) Over 1000 days (when the elapsed time is more than 1000 days) "-" is displayed when the channel group status is not Up.
Max Active Port	Maximum number of ports used by link aggregation	1 to 8 (8 is displayed as the initial value.) "-" is displayed when link aggregation mode is not set.
	Standby link mode	Standby link link-down mode
		(link-down mode): Link-down mode
		(no-link-down mode): Link-not-down mode
Max Detach Port	Restriction on the number of detached ports	0 or 7 (7 is displayed as the initial value.) "-" is displayed when link aggregation mode is not set.
Load Balance	Distribution method	default: The load is distributed according to the default distribution method of the Switch. For details, see "Configuration Guide Vol.1, 21.1.5 Port allocation for sending frames".
Description	Supplementary explanation regarding the channel group	This item is not displayed if a supplementary explanation has not been set in the configuration.
MAC Address	Channel group's MAC address	The MAC address of the group. One of the MAC addresses of the ports that belong to the group is used.
VLAN ID	VLAN ID of the VLAN to which the channel group belongs	VLAN ID
Periodic Time	Sending interval for LACPDU	This item is displayed only when LACP mode is enabled.
		Short: The sending interval is 1 second.
		Long: The sending interval is 30 seconds.

Item	Meaning	Displayed detailed information
Actor information	Information about the actor system	Information about the actor system. This item is displayed only when LACP mode is enabled.
System Priority	System priority	Priority of the LACP system ID 1 to 65535 can be specified as the priority value (1 indicates the highest priority).
MAC	MAC address	The MAC address of the LACP system ID
KEY	Group key	Group key This value is the same as the channel group number.
Partner information	Information about the partner system	Information about the partner system. This item is displayed only when LACP mode is enabled. "-" is displayed if the partner system is not defined for LACP.
System Priority	System priority	Priority of the LACP system ID 0 to 65535 can be specified as the priority value (0 indicates the highest priority).
MAC	MAC address	MAC address
KEY	Group key	0 to 65535
Port Counts	Number of ports that have been set up	Number of ports that have been set up by configuration
Up Port Counts	Number of ports that can be used for sending and receiving data packets	Number of ports that can be used for sending and receiving data
Port	Port information	Switch number/NIF number/port number
Status	Status of the port aggregation	Up: Data packets can be sent and received.
		Down: Data packets cannot be sent or received.
Reason	Cause of the failure	-: Status is "Up".
		Standby: The ports in the local channel group are in Standby state.
		CH Disabled: The status of the local channel group is Disable.
		Port Down: The ports in the local channel group are in DOWN state.
		Port Speed Unmatch: Ports in the local channel group do not use the same line speed.
		Port Selecting: A port aggregation condition check is being conducted on the local channel group.
		Waiting Partner Synchronization: The port aggregation condition check on the local channel group has finished, and the channel group is waiting for the connected port to synchronize.
		LACPDU Expired: The valid time period of the LACPDU received from the connected port expired.

Item	Meaning	Displayed detailed information
		Partner System ID Unmatch: The partner system ID received from the connected port is different from the partner system ID of the group. The Unmatched Partner System ID is also displayed.
		Partner Key Unmatch: The key received from the connected port is different from the Partner Key of the group. The Unmatched Partner Key is also displayed.
		Partner Aggregation Individual: The connected port cannot be a member of link aggregation.
		Partner Synchronization OUT_OF_SYNC: The port connected to the local port cannot synchronize with the local port.
		Port Moved: A port moved in the channel group.
		Operation of Detach Port Limit: The maximum number of ports that can be detached is limited.
Speed	Line speed	10M: 10 Mbit/s
		100M: 100 Mbit/s
		1G: 1 Gbit/s
		2.5G: 2.5G bit/s
		10G: 10 Gbit/s
		-: The line speed is unknown.
Duplex	Duplex mode	Full: Full duplex
		Half: Half duplex
		-: The duplex mode is unknown.
LACP Activity	LACP activation method	This item is displayed only when LACP mode is enabled.
		Active: LACPDUs are always sent.
		Passive: An LACPDU is sent after an LACPDU is received.
Actor Priority	Priority of the actor system port	0 to 65535 can be specified as the priority value (0 indicates the highest priority). This item is displayed only when LACP mode is enabled.
Partner Priority	Priority of the partner system port	0 to 65535 can be specified as the priority value (0 indicates the highest priority). This item is displayed only when LACP mode is enabled.
Priority	Priority of the actor system port	0 to 65535 can be specified as the priority value (0 indicates the highest priority). This item is displayed only in static mode.
Unmatched Partner Key	Partner key that is unmatched	1 to 65535 This item is displayed only when Status is Down and Reason:Unmatched Partner Key.

Item	Meaning	Displayed detailed information
Unmatched Partner System ID	Partner system ID that is unmatched	This item is displayed only when Status is Down and Reason:Unmatched Partner System ID.
Priority	System priority	0 to 65535 can be specified as the priority value (0 indicates the highest priority).
MAC Address	MAC address	The MAC address for the system ID

Impact on communication

None

Notes

If the standby link function is used in link-down mode, as many ports as the maximum number of available ports are used for operation and the rest of the ports become standby ports. For Reason (cause of failure), Standby is displayed regardless of the status of the standby ports. If the status of a port changes to Standby due to a failure, a message to that effect is not logged, but the port will work as a standby port after the failure is corrected.

show channel-group statistics

Displays link aggregation statistics.

Syntax

```
show channel-group statistics [lacp] [<channel group list>]
```

Input mode

User mode and administrator mode

Parameters

lacp

Displays for each port the statistics for sent and received LACPDUs in link aggregation. Information is not displayed if static link aggregation mode is enabled or link aggregation mode has not been set.

<channel group list>

Displays link aggregation statistics for the channel group numbers specified in list format. For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

Statistics for all link aggregations are displayed.

Behavior when all parameters are omitted:

Statistics for sent and received data packets (for each port) in all link aggregations are displayed.

Example 1

The following shows an example of displaying statistics on sent and received data packets for link aggregation (by port).

Figure 21-4: Displaying statistics on sent and received data packets for link aggregation

```
>show channel-group statistics
Date 20XX/07/14 12:00:00 UTC
channel-group counts:4
ChGr:1(Up)
 Total:      Octets    Tx:            12760301  Rx:             9046110
             Frames    Tx:               71483  Rx:               64377
             Discards  Tx:                  96  Rx:                   9
 Port:0/1    Octets    Tx:            12745991  Rx:             9033008
             Frames    Tx:               71432  Rx:               64332
             Discards  Tx:                  95  Rx:                   5
 Port:0/2    Octets    Tx:               14310  Rx:               13102
             Frames    Tx:                  51  Rx:                  45
             Discards  Tx:                   1  Rx:                   4
 Port:0/3    Octets    Tx:                   0  Rx:                   0
             Frames    Tx:                   0  Rx:                   0
             Discards  Tx:                   0  Rx:                   0
 Port:0/10   Octets    Tx:                   0  Rx:                   0
             Frames    Tx:                   0  Rx:                   0
             Discards  Tx:                   0  Rx:                   0
 Port:0/12   Octets    Tx:                   0  Rx:                   0
             Frames    Tx:                   0  Rx:                   0
             Discards  Tx:                   0  Rx:                   0
 Port:0/13   Octets    Tx:                   0  Rx:                   0
             Frames    Tx:                   0  Rx:                   0
             Discards  Tx:                   0  Rx:                   0
ChGr:2(Up)
```

```
 Total:      Octets    Tx:            2031141  Rx:            1643359
             Frames    Tx:               3344  Rx:               2353
             Discards  Tx:                 14  Rx:                 25
 Port:0/4    Octets    Tx:            2008831  Rx:            1623147
             Frames    Tx:               3312  Rx:               2332
             Discards  Tx:                 10  Rx:                 22
 Port:0/5    Octets    Tx:              22310  Rx:              20212
             Frames    Tx:                 32  Rx:                 21
             Discards  Tx:                  4  Rx:                  3
 Port:0/6    Octets    Tx:                  0  Rx:                  0
             Frames    Tx:                  0  Rx:                  0
             Discards  Tx:                  0  Rx:                  0
ChGr:3(Down)
 Total:      Octets    Tx:                  0  Rx:                  0
             Frames    Tx:                  0  Rx:                  0
             Discards  Tx:                  0  Rx:                  0
 Port:0/7    Octets    Tx:                  0  Rx:                  0
             Frames    Tx:                  0  Rx:                  0
             Discards  Tx:                  0  Rx:                  0
 Port:0/8    Octets    Tx:                  0  Rx:                  0
             Frames    Tx:                  0  Rx:                  0
             Discards  Tx:                  0  Rx:                  0
ChGr:4(Up)
 Total:      Octets    Tx:            5971370  Rx:            5205702
             Frames    Tx:              11133  Rx:              10286
             Discards  Tx:                 12  Rx:                 32
 Port:0/9    Octets    Tx:            4023121  Rx:            3403392
             Frames    Tx:               7211  Rx:               6884
             Discards  Tx:                  0  Rx:                  0
 Port:0/14   Octets    Tx:            1948249  Rx:            1802310
             Frames    Tx:               3922  Rx:               3402
             Discards  Tx:                 12  Rx:                 32
 Port:0/15   Octets    Tx:                  0  Rx:                  0
             Frames    Tx:                  0  Rx:                  0
             Discards  Tx:                  0  Rx:                  0
>
```

Display items in Example 1

Table 21-4: Display items for the statistics for sent and received data packets related to link aggregation

Item	Meaning	Displayed detailed information
channel-group counts	Number of channel groups to be displayed	Number of channel groups per switch
ChGr	Channel group number. The status of the channel group is displayed enclosed in parentheses.	Channel group number Up: Data packets can be sent and received. Down: Data packets cannot be sent or received. Disabled: Link aggregation is disabled.
Total	Total statistics	Statistics are displayed for each channel group.
Port	Port information	Statistics are displayed for each port. NIF number/port number
Octets	Data size of the sent and received data packets	Tx: Total number of sent bytes Rx: Total number of received bytes This item is displayed in octets starting with the MAC header and ending with the FCS.
Frames	Number of sent and received data frames	Tx: Total number of sent data frames Rx: Total number of received data frames

Item	Meaning	Displayed detailed information
Discards	Number of discarded sent and received data frames	Tx: Total number of discarded sent data frames Rx: Total number of discarded received data frames For details about the items used for counting the number of discarded frames, see "Table 20-11: Statistical items used to calculate the number of discarded packets".

Example 2

The following shows an example of displaying statistics for sent and received LACPDUs in link aggregation.

Figure 21-5: Displaying the statistics for sent and received LACPDUs in link aggregation

```
>show channel-group statistics lacp
Date 20XX/07/14 12:00:00 UTC
channel-group counts:2
ChGr:1     Port Counts:6
  Port:1/0/1
    TxLACPDUs           : 50454011  RxLACPDUs   : 16507650
    TxMarkerResponsePDUs:       10  RxMarkerPDUs:       10
    RxDiscards          :        8
  Port:1/0/2
    TxLACPDUs           : 50454011  RxLACPDUs   : 16507650
    TxMarkerResponsePDUs:       10  RxMarkerPDUs:       10
    RxDiscards          :        8
  Port:1/0/3
    TxLACPDUs           :      100  RxLACPDUs   :      100
    TxMarkerResponsePDUs:       10  RxMarkerPDUs:       10
    RxDiscards          :        8
  Port:1/0/10
    TxLACPDUs           :      100  RxLACPDUs   :      100
    TxMarkerResponsePDUs:       10  RxMarkerPDUs:       10
    RxDiscards          :        8
  Port:1/0/12
    TxLACPDUs           :      100  RxLACPDUs   :      100
    TxMarkerResponsePDUs:       10  RxMarkerPDUs:       10
    RxDiscards          :        8
  Port:1/0/13
    TxLACPDUs           :      100  RxLACPDUs   :      100
    TxMarkerResponsePDUs:       10  RxMarkerPDUs:       10
    RxDiscards          :        8
ChGr:11    Port counts:3
  Port:1/0/4
    TxLACPDUs           :      100  RxLACPDUs   :      100
    TxMarkerResponsePDUs:       10  RxMarkerPDUs:       10
    RxDiscards          :        8
  Port:1/0/5
    TxLACPDUs           :      100  RxLACPDUs   :      100
    TxMarkerResponsePDUs:       10  RxMarkerPDUs:       10
    RxDiscards          :        8
  Port:1/0/6
    TxLACPDUs           :      100  RxLACPDUs   :      100
    TxMarkerResponsePDUs:       10  RxMarkerPDUs:       10
    RxDiscards          :        8
>
```

Display items in Example 2

Table 21-5: Display items for the statistics for sent and received LACPDUs in link aggregation

Item	Meaning	Displayed detailed information
channel-group counts	Number of channel groups to be displayed	Number of channel groups

Item	Meaning	Displayed detailed information
ChGr	Channel group number	Channel group number
Port Counts	Number of ports to be displayed	Number of ports
Port	Port information	Switch number/NIF number/port number
TxLACPDUs	Number of sent LACPDUs	—
RxLACPDUs	Number of received LACPDUs	—
Tx MarkerResponsePDUs	Number of sent marker response PDUs	—
RxMarkerPDUs	Number of received marker PDUs	—
RxDiscards	Number of discarded received PDUs	Number of LACPDUs discarded due to parameter errors

Impact on communication

None

Notes

- Statistics are cleared when the device starts up or when the following commands are executed:

  Statistics for sent and received data packets: clear counters

  Information about sent and received LACPs: clear channel-group statistics lacp

- The statistics for the sent and received data packets displayed by this command are the sum of the statistics on the Ethernet lines for each channel group. To clear the statistics for sent and received data packets, use a command that clears Ethernet lines. The following are related commands:

  Related commands: show interfaces

  clear counters

clear channel-group statistics lacp

Clears the statistics for sent and received LACPDUs in link aggregation.

Syntax

```
clear channel-group statistics lacp [<channel group list>]
```

Input mode

User mode and administrator mode

Parameters

<channel group list>

Specifies a list of the channel group numbers for which you want to clear LACPDU statistics. For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

The statistics on the sent and received LACPDUs for all channel groups are cleared.

Example

Figure 21-6: Clearing the statistics on sent and received LACPDUs for link aggregation

```
>clear channel-group statistics lacp
>
```

Figure 21-7: Clearing the statistics on sent and received LACPDUs for a specific channel group number in a link aggregation

```
>clear channel-group statistics lacp 1
>
```

Display items

None

Impact on communication

None

Notes

- This command clears only LACPDU statistics. It cannot clear the statistics for the data packets for each channel group. See Notes for the "show channel-group statistics" command.
- Even if statistics are cleared to zero, the value for the MIB information obtained by using SNMP is not cleared to zero.
- If deletion or addition is performed in the configuration, the relevant LACPDU statistics are cleared to zero.

restart link-aggregation

Restarts the link aggregation program.

Syntax

```
restart link-aggregation [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the link aggregation program without outputting any restart confirmation messages.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the link aggregation program's core file (LAd.core) when the link aggregation program is re-started.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

After the restart confirmation message is output, the link aggregation program is restarted.

Example

Figure 21-8: Restarting the link aggregation program

```
> restart link-aggregation
Link Aggregation restart OK? (y/n):y
>
```

Figure 21-9: Restarting the link aggregation program (-f parameter specified)

```
> restart link-aggregation -f
>
```

Impact on communication

Ports for which link aggregation is enabled temporarily become unable to send or receive data.

Notes

The storage directory and the name of the core file are as follows:

Storage directory: /usr/var/core/

Core file: LAd.core

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

dump protocols link-aggregation

Outputs to a file detailed event trace information and control table information collected for the link aggregation program.

Syntax

```
dump protocols link-aggregation
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 21-10: Taking a link aggregation dump

```
> dump protocols link-aggregation
>
```

Impact on communication

None

Notes

The storage directory and the name of the output dump file are as follows.

Storage directory: /usr/var/LA/

File name: LAd_dump.gz

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

22 MAC Address Table

show mac-address-table

Shows information about the MAC address table.

Syntax

```
show mac-address-table [ <mac> ] [ vlan <vlan id list> ] [ port <port list> ]
     [channel-group-number <channel group list>]
     [{ static | dynamic | snoop | dot1x | wa | macauth }]
show mac-address-table learning-counter [ port <port list> ]
     [channel-group-number <channel group list>]
show mac-address-table learning-counter vlan [<vlan id list>]
```

Input mode

User mode and administrator mode

Parameters

<mac>

Displays the information in the MAC address table for the specified MAC address.

vlan <vlan id list>

Displays the information in the MAC address table for the VLAN IDs specified in list format.

For details about how to specify <vlan id list>, see "Specifiable values for parameters".

[port <port list>] [channel-group-number <channel group list>]

Displays the information in the MAC address table for the specified ports or the specified channel groups. If you specify both a list of ports and a list of channel groups, the information in the MAC address table for either the specified ports or channel groups is displayed.

port <port list>

Displays the information in the MAC address table for the ports specified in list format. The MAC address table entries that include at least one of the ports specified in the list are displayed. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters".

channel-group-number <channel group list>

Displays the information in the MAC address table for the channel groups specified in list format for the specified link aggregation. For details about how to specify <channel group list>, see "Specifiable values for parameters".

Even if the command is executed with this parameter set, information about the MAC address table is displayed in port-list format.

Behavior when this parameter is omitted:

The information in the MAC address table for all ports and channel groups is displayed.

{ static | dynamic | snoop | dot1x | wa | macauth }

Displays the information in the MAC address table that was registered under the specified condition.

static

Displays the information in the MAC address table registered by the "mac-address-table static" configuration command.

dynamic

Displays the information in the MAC address table registered dynamically through MAC address learning.

snoop

Displays the information in the MAC address table registered by using the IGMP snooping or MLD snooping function.

dot1x

Displays the information in the MAC address table registered by using IEEE 802.1X.

wa

Displays the information in the MAC address table registered by using the Web authentication function.

macauth

Displays the information in the MAC address table registered by using the MAC-based authentication function.

learning-counter

Displays the number of learned addresses in the MAC address table.

learning-counter vlan [<vlan id list>]

Displays the number of learned addresses in the MAC address table for each VLAN. For details about how to specify <vlan id list>, see "Specifiable values for parameters". If <vlan id list> is omitted, the number of learned addresses for all VLANs is displayed.

Behavior when each parameter is omitted:

This command can display only information relevant to the condition applied by a parameter that has been set. If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information conforming to the conditions will be displayed.

Behavior when all parameters are omitted:

All the information in the MAC address table is displayed.

Example 1

Figure 22-1: Displaying all the information in the MAC address table

```
> show mac-address-table
Date 20XX/10/29 11:33:50 UTC
MAC address        VLAN    Type     Port-list
0012.e280.5cbf        3    Static   1/0/5
0012.e205.0558        1    Dynamic  1/0/23
0012.e28e.0602        1    Dynamic  1/0/23
0012.e2a8.250c        1    Dynamic  1/0/23
0012.e205.0642      100    Dynamic  1/0/2-3,10
0012.e205.0643      103    Dynamic  1/0/4,7
0012.e205.0643      104    Dynamic  1/0/4,7
>
```

Display items in Example 1

Table 22-1: Display items for the information in the MAC address table

Item	Meaning	Displayed detailed information
MAC address	MAC address	—
VLAN	VLAN ID	—

Item	Meaning	Displayed detailed information
Type	Type of MAC address table entry	Dynamic: Entry registered dynamically Snoop: Entry registered by using the IGMP snooping or MLD snooping function Static: Entry registered statically Dot1x: Entry registered via IEEE 802.1X Wa: Entry registered via the Web authentication function Macauth: Entry registered via the MAC-based authentication function
Port-list	Port (Switch number/NIF number/port number)	Note that items other than ports are displayed in the following cases: Drop: Drop (discarded MAC address) specified -: Entry whose type is Snoop and that is being deleted from the MAC address table, or Dot1x/Wa/Macauth entry registered in a channel group whose channels have been all deleted

Example 2

Figure 22-2: Displaying the status of learning in the MAC address table (for each port)

```
>show mac-address-table learning-counter port 1/0/1-10
Date 20XX/12/21 20:00:57 UTC
Port counts:10
Port       Count
1/0/1          3
1/0/2       1000
1/0/3          0
1/0/4         50
1/0/5         45
1/0/6          0
1/0/7         22
1/0/8          0
1/0/9          0
1/0/10         0
>
```

Figure 22-3: Displaying the status of learning in the MAC address table (for each VLAN)

```
>show mac-address-table learning-counter vlan
Date 20XX/12/10 20:00:57 UTC
VLAN counts:4
ID         Count  Maximum
   1           3        -
 100        1000        -
 200           0        -
4094          90        -
>
```

Display items in Example 2

Table 22-2: Display items for the status of learning in the MAC address table

Item	Meaning	Displayed detailed information
Port counts	Number of target ports	—
VLAN counts	Number of applicable VLANs	—
Port	Port (Switch number/NIF number/port number)	—
ID	VLAN ID	VLAN ID

Item	Meaning	Displayed detailed information
Count	Number of learned entries in the current MAC address table	—
Maximum	Maximum number of addresses that can be learned in the MAC address table	"-" is displayed at all times.

Impact on communication

None

Notes

1. When a Layer 2 authentication port receives a packet from an unauthenticated terminal, the packet is registered as a dynamic entry when the authentication process is in progress or when authentication fails. However, only limited packets are relayed from the unauthenticated terminal to other ports.

clear mac-address-table

Clears the information in the MAC address table registered dynamically through MAC address learning.

Syntax

```
clear mac-address-table [ vlan <vlan id list> ]
     [ port <port list> ][channel-group-number <channel group list>][-f]
clear mac-address-table vlan <vlan id list> mac-address <mac> [-f]
```

Input mode

User mode and administrator mode

Parameters

vlan <vlan id list>

Specifies a list of VLAN IDs for which you want to clear the MAC address table entries.

For details about how to specify <vlan id list>, see "Specifiable values for parameters".

[port <port list>] [channel-group-number <channel group list>]

Specifies a list of ports or channel groups for which you want to clear the information in the MAC address table. If you specify both a list of ports and a list of channel groups, the information in the MAC address table for either the specified ports or channel groups will be cleared.

port <port list>

Specifies a list of ports for which you want to clear the information in the MAC address table that have been learned. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters".

channel-group-number <channel group list>

Specifies a list of channel groups in the link aggregation for which you want to clear the information in the MAC address table that have been learned. For details about how to specify <channel group list>, see "Specifiable values for parameters".

mac-address <mac>

Clears the information in the MAC address table for the specified MAC address. For the specifiable range of MAC address values, see "Specifiable values for parameters".

-f

Clears information in the MAC address table without displaying a clear confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Behavior when each parameter is omitted:

This command can clear only the information in the MAC address table that meets the conditions specified by the parameter. If no parameter is specified, information in the MAC address table is cleared without being limited by any conditions. If multiple parameters are specified, the information in the MAC address table conforming to the conditions will be cleared.

Behavior when all parameters are omitted:

All dynamically learned MAC address table information is cleared.

Example

Figure 22-4: Clearing the MAC address table information when a VLAN ID and port are specified

```
>clear mac-address-table vlan 90 port 1/0/9
mac-address-table clear OK? (y/n): y
>
```

Figure 22-5: Clearing the MAC address table without displaying the clear confirmation message

```
>clear mac-address-table vlan 100-200 -f
>
```

Display items

None

Impact on communication

Frames are flooded until learning is completed again. Execute this command at a time when flooding will have a minimal impact.

Notes

None

23 VLAN

show vlan

Displays various VLAN statuses and the status of accommodated lines.

Syntax

```
show vlan [{ summary | detail | list | configuration }]
show vlan <vlan id list> [{ summary | detail | list | configuration }]
show vlan [port <port list>] [ channel-group-number <channel group list>]
          [{ summary | detail | list | configuration }]
```

Input mode

User mode and administrator mode

Parameters

{ summary | detail | list | configuration }

summary

Displays VLAN summary information.

detail

Displays detailed information about VLANs.

list

Displays VLAN information with the information for one VLAN being displayed on one line.

configuration

Displays information about the ports assigned in a VLAN.

Behavior when this parameter is omitted:

VLAN information is displayed.

<vlan id list>

Displays the VLAN information for the VLAN IDs specified in list format.

For details about how to specify <vlan id list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

Information about all VLANs is displayed.

[port <port list>] [channel-group-number <channel group list>]

Specifies a list of ports or channel groups for which you want to display VLAN information. If you specify both a list of ports and a list of channel groups, the VLAN information for either the specified ports or channel groups is displayed.

port <port list>

Specifies a list of ports for which you want to display the VLAN information. The information about all VLANs that contain one or more specified ports is displayed. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters".

channel-group-number <channel group list>

Specifies a list of channel groups for which you want to display the information of the VLAN in the specified link aggregation. For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

All VLAN information, not limited by port or channel group, is displayed.

Behavior when all parameters are omitted:

All the VLAN information is displayed.

Example 1

The following figure shows an example of displaying the summary information about all configured VLANs.

Figure 23-1: Example of displaying the VLAN summary information

```
> show vlan summary
Date 20XX/09/21 14:15:00 UTC
Total(18)           :1,3-5,8,10-20,100,2000
Port based(10)      :1,3-5,8,10,12,14,16,18
Protocol based(8)   :11,13,15,17,19-20,100,2000
MAC based(0)        :
>
```

Display items in Example 1

Table 23-1: Display items of the VLAN summary

Item	Meaning	Displayed detailed information
Total(n)	Applicable VLAN information	n: Number of applicable VLANs VLAN ID list
Port based(n)	Port VLAN information	n: Number of applicable VLANs VLAN ID list
Protocol based(n)	Protocol VLAN information	n: Number of applicable VLANs VLAN ID list
MAC based(n)	MAC VLAN information	n: Number of applicable VLANs VLAN ID list

Example 2

The following figures show examples of displaying the statuses of all configured VLANs and the statuses of accommodated ports.

Figure 23-2: Result of displaying the VLAN information

```
> show vlan
Date 20XX/01/26 17:01:40 UTC
VLAN counts:4
VLAN ID:1     Type:Port based      Status:Up
  Learning:On            Tag-Translation:On
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN0001
  IP Address:10.215.201.1/24
             3ffe:501:811:ff08::5/64
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0001
  Spanning Tree:PVST+(802.1D)
  AXRP RING ID:      AXRP VLAN group:
  IGMP snooping:     MLD snooping:
  Untagged(8)   :1/0/5-12
  Tagged(2)     :1/0/19-20
  Tag-Trans(2)  :1/0/19-20
VLAN ID:120   Type:Protocol based  Status:Up
  Protocol VLAN Information  Name:ipv6
  EtherType:08dd  LLC:  Snap-EtherType:
   :
   :
```

Figure 23-3: Result of displaying the VLAN information in list format (when the Ring Protocol is used)

```
> show vlan 3,5
Date 20XX/11/15 17:01:40 UTC
VLAN counts:2
VLAN ID:3     Type:Port based      Status:Up
  Learning:On            Tag-Translation:
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN0003
  IP Address:
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0003
  Spanning Tree:
  AXRP RING ID:1      AXRP VLAN group:2
  AXRP RING ID:100    AXRP VLAN group:1
  AXRP RING ID:500    AXRP VLAN group:2
  AXRP RING ID:1000   AXRP VLAN group:2
  IGMP snooping:     MLD snooping:
  Untagged(8)   :1/0/5-12
  Tagged(8)     :1/0/25-32
VLAN ID:5     Type:Port based      Status:Up
  Learning:On            Tag-Translation:
  :
  :
```

Figure 23-4: Result of displaying the VLAN information with the detail parameter specified

```
> show vlan 3,1000-1500 detail
Date 20XX/12/10 12:00:00 UTC
VLAN counts:2
VLAN ID:3     Type:Port based      Status:Up
  Learning:On            Tag-Translation:On
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN0003
  IP Address:10.215.196.1/23
             ee80::220:afff:fed7:8f0a/64
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0003
  Spanning Tree:Single(802.1D)
  AXRP RING ID:      AXRP VLAN group:
  IGMP snooping:     MLD snooping:
  Port Information
   1/0/5          Up   Forwarding      Untagged
   1/0/6          Up   Blocking(STP)   Untagged
     :
     :
   1/0/25(CH:9)   Up   Forwarding      Tagged   Tag-Translation:103
   1/0/26(CH:9)   Up   Blocking(CH)    Tagged   Tag-Translation:103
VLAN ID:1340  Type:Mac based       Status:Up
  Learning:On            Tag-Translation:On
   :
   :
```

Display items in Example 2

Table 23-2: Display items for the VLAN information

Item	Meaning	Displayed detailed information
VLAN counts	Number of applicable VLANs	—
VLAN tunneling enabled	VLAN tunneling information	VLAN tunneling function is enabled. (This item is displayed only when VLAN tunneling function is used.)
VLAN ID	VLAN information	VLAN ID

Item	Meaning	Displayed detailed information
Type	VLAN type	Port based: Port VLAN Protocol based: Protocol VLAN Mac based: MAC VLAN
Status	VLAN status	Up: Indicates that the VLAN is in Up status. Down: Indicates that the VLAN is in Down status. Disabled: The VLAN is in Disable status.
Protocol VLAN Information	Protocol VLAN information	This item is displayed only for a protocol VLAN.
Name	Name	—
EtherType	EtherType value of Ethernet V2 frames	Displayed as a four-digit hexadecimal number
LLC	LLC value of 802.3 frames	Displayed as a four-digit hexadecimal number
Snap-EtherType	EtherType value of 802.3 SNAP frames	Displayed as a four-digit hexadecimal number
Learning	Status of MAC address learning	On: MAC address learning is enabled. Off: MAC address learning is disabled.
Tag-Translation	Tag translation	Blank: No IP address has been set. On: Tag translation is being used.
BPDU Forwarding	BPDU forwarding	Blank: No IP address has been set. On: The BPDU forwarding function is being used.
EAPOL Forwarding	EAPOL forwarding	Blank: No IP address has been set. On: The EAPOL forwarding function is being used.
Router Interface Name	Interface name	Displays the name of the interface assigned to the VLAN.
IP Address	IP address (/mask)	Blank: No IP address has been set.
Source MAC address	Source MAC address used during Layer 3 communication	System: The MAC address for the device is used.
Description	Description	The character string set for the VLAN name is displayed. VLANxxxx is displayed if this item is not set. (xxxx: VLAN ID)
Spanning Tree	STP being used	Blank: Stopped Single (802.1D): IEEE 802.1D is used for the entire device. Single (802.1w): IEEE 802.1w is used for the entire device. PVST+ (802.1D): IEEE 802.1D is used for the VLAN. PVST+ (802.1w): IEEE 802.1w is used for the VLAN. MSTP (802.1s): Multiple Spanning Tree is used.
AXRP RING ID	Ring ID for the Ring Protocol function	Blank: No IP address has been set. (Information about a maximum of 24 IDs is displayed.)

Item	Meaning	Displayed detailed information
AXRP VLAN group	ID of the VLAN group using the Ring Protocol function or the control VLAN	Blank: No IP address has been set. 1 or 2: ID of the assigned VLAN group Control-VLAN: The control VLAN is assigned.
IGMP snooping	Setting status of IGMP snooping	Blank: No IP address has been set. On: IGMP snooping is being used.
MLD snooping	Setting status of MLD snooping	Blank: No IP address has been set. On: MLD snooping is being used.

Table 23-3: Display items related to the number of ports in VLAN information

Item	Meaning	Displayed detailed information
Untagged(n)	Untagged port	n: Number of applicable ports Port list
Tagged(n)	Tagged port	n: Number of applicable ports Port list
Tag-Trans(n)	Port for which tag translation is set	n: Number of applicable ports Port list

Table 23-4: Display items for the VLAN information with the detail parameter specified

Item	Meaning	Displayed detailed information
Port Information	Port information (Switch number/NIF number/port number)	If there is no port information for the VLAN, No Port Information is displayed.
CH	Channel group number	1 to 120 This item is not displayed for the ports that do not belong to the channel group.
<port status>	Port status	Up: Indicates that the port status is Up. Down: Indicates that the port status is Down.
<data-forwarding-status>	Data forwarding status	Forwarding: Data is being forwarded. Blocking: Data forwarding is blocked. (VLAN) VLAN disabled (CH): Data forwarding has been stopped by link aggregation. (STP): Data forwarding has been stopped by STP. (dot1x): Data forwarding has been stopped by IEEE 802.1X. (CNF): Data forwarding has been stopped because a duplicated protocol value was encountered in the protocol VLAN configuration (data is being forwarded for the protocol values that have successfully been set). (AXRP): Forwarding has been suspended by the Ring Protocol. (ULR): Data transfers have been stopped by uplink redundancy. -: The port is in Down state.
Tag	Tag setting status	Untagged: Untagged port Tagged: Tagged port

Item	Meaning	Displayed detailed information
Tag-Translation	ID subject to tag translation	1 to 4094

Example 3

The following figures show examples of displaying the VLAN information in list format.

Figure 23-5: Example of displaying the VLAN information in list format

```
> show vlan list
Date 20XX/11/15 17:01:40 UTC
VLAN counts:4
Number of VLAN ports:41
ID   Status  Fwd/Up /Cfg Name            Type  Protocol       Ext.  IP
   1 Up       16/ 18/ 18 VLAN0001        Port  STP PVST+:1D   - - - 4
   3 Up        9/ 10/ 10 VLAN0003        Port  STP Single:1D  - - T 4/6
 120 Up        4/  5/  5 VLAN0120        Proto -              - - - -
1340 Disable   0/  8/  8 VLAN1340        Mac   -              - - - 4
     AXRP (C:Control-VLAN)
     S:IGMP/MLD snooping  T:Tag Translation
     4:IPv4 address configured  6:IPv6 address configured
>
```

Figure 23-6: Example of displaying the VLAN information in list format (when the Ring Protocol is used)

```
> show vlan list
Date 20XX/11/15 17:01:40 UTC
VLAN counts:4
Number of VLAN ports:10
ID   Status  Fwd/Up /Cfg Name            Type  Protocol       Ext.  IP
   1 Up        1/  2/  2 VLAN0001        Port  AXRP (-)       - - - -
   5 Up        2/  2/  2 VLAN0005        Port  AXRP (C)       - - - -
  10 Up        1/  2/  2 VLAN0010        Port  AXRP (-)       - - - -
  20 Up        3/  4/  4 VLAN0020        Port  AXRP (-)       - - - -
     AXRP (C:Control-VLAN)
     S:IGMP/MLD snooping  T:Tag Translation
     4:IPv4 address configured  6:IPv6 address configured
>
```

Figure 23-7: Example of displaying the VLAN information in list format (when both the Ring Protocol and STP are used)

```
> show vlan list
Date 20XX/11/15 17:01:40 UTC
VLAN counts:4
Number of VLAN ports:11
ID   Status  Fwd/Up /Cfg Name            Type  Protocol       Ext.  IP
   1 Up        3/  3/  3 VLAN0001        Port  STP Single:1D  - - - -
   5 Up        2/  2/  2 VLAN0005        Port  AXRP (C)       - - - -
  10 Up        3/  3/  3 VLAN0010        Port  STP PVST+:1D   - - - -
  20 Up        3/  3/  3 VLAN0020        Port  STP Single:1D  - - - -
     AXRP (C:Control-VLAN)
     S:IGMP/MLD snooping  T:Tag Translation
     4:IPv4 address configured  6:IPv6 address configured
>
```

Display items in Example 3

Table 23-5: Display items for the VLAN information in list format

Item	Meaning	Displayed detailed information
VLAN counts	Number of applicable VLANs	—

Item	Meaning	Displayed detailed information
VLAN tunneling enabled	VLAN tunneling information	VLAN tunneling function is enabled. (This item is displayed only when VLAN tunneling function is used.)
Number of VLAN ports	Total number of VLAN ports	Displays the total number of ports belonging to the specified VLAN.
ID	VLAN ID	VLAN ID
Status	VLAN status	Up: Indicates that the VLAN is in Up status. Down: Indicates that the VLAN is in Down status. Disabled: The VLAN is in Disable status.
Fwd	Number of ports in Forward state	The number of ports belonging to the VLAN that are in Forward state
Up	Number of ports in Up status	The number of ports belonging to the VLAN that are in Up status
Cfg	Number of VLAN ports	The number of ports belonging to the VLAN
Name	VLAN name	The character string set for the VLAN name is displayed. VLANxxxx is displayed if this item is not set. (xxxx: VLAN ID)
Type	VLAN type	Port: Port VLAN Proto: Protocol VLAN Mac: MAC VLAN
Protocol	STP information or Ring Protocol information	For STP: STP <type>:<protocol> <type>: Single, PVST+, or MSTP <protocol>: 802.1D, 802.1w, or 802.1s For the Ring Protocol: AXRP (C): Indicates that the control VLAN is assigned, (-) is displayed if the control VLAN is not assigned. Note, however, that (-) is not displayed for a VLAN that co-exists with other protocols. If nothing is specified, a hyphen (-) is displayed.
Ext.	Extended function information	S: Indicates that IGMP snooping or MLD snooping is set. T: Indicates that tag translation is set. -: Indicates that the relevant function is not set.
IP	IP address setting information	4: Indicates that an IPv4 address is set. 6: Indicates that an IPv6 address is set. 4/6: Indicates that both an IPv4 address and an IPv6 address are set. -: Indicates that an IP address is not set for the VLAN.

Example 4

The following figure shows an example of displaying the information about all the ports configured for VLANs.

Figure 23-8: Example of displaying the information about all the ports set for the VLANs

```
> show vlan configuration
```

```
Date 20XX/11/15 14:15:00
VLAN counts: 3
ID   Name             Status  Ports
   1 DefaultVLAN      Up      1/0/1-10,1/0/12,1/0/14,1/0/16,1/0/20-23,1/0/30,
                              1/0/32,1/0/34,1/0/36,1/0/49-50
 200 Global IP Netw.. Down    1/0/11,1/0/15,1/0/31
4000 VLAN4000         Disable 1/0/2-10,1/0/12,1/0/31
>
```

Display items in Example 4

Table 23-6: Display items for the information about all the ports set for the VLANs

Item	Meaning	Displayed detailed information
VLAN counts	Number of applicable VLANs	—
ID	VLAN ID	VLAN ID
Name	VLAN name	VLAN name (a maximum of 14 characters from the beginning)
Status	VLAN status	Up: Indicates that the VLAN is in Up status. Down: Indicates that the VLAN is in Down status. Disabled: The VLAN is in Disable status.
Ports	Port information	Switch number/NIF number/port number If no port exists, a hyphen (-) is displayed.

Impact on communication

None

Notes

1. If the "switchport mac" configuration command with no vlan parameter specified has been executed for MAC ports that are placed in dynamic VLAN mode for Web authentication or MAC-based authentication, this command displays all the VLANs for which the "vlan mac-based" configuration command has been executed.

show vlan mac-vlan

Shows the MAC addresses registered for MAC VLANs.

Syntax

```
show vlan mac-vlan [<vlan id list>] [{ static | dynamic }]
show vlan mac-vlan <mac>
```

Input mode

User mode and administrator mode

Parameters

<vlan id list>

Displays MAC VLAN information for the VLAN IDs specified in list format.

For details about how to specify <vlan id list>, see "Specifiable values for parameters". Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

{ static | dynamic }

static

Displays the MAC address information registered in the configuration.

The MAC address information disabled by hardware conditions is also displayed.

dynamic

Displays the MAC address information registered by the Layer 2 authentication function. The MAC address information disabled because it is also registered by configuration is also displayed.

<mac>

Displays VLANs for which the specified MAC address is registered.

The MAC address information disabled because it is registered by both configuration and the Layer 2 authentication function is also displayed.

The MAC address information in the configuration disabled by hardware conditions is also displayed.

Example

The following figures show examples of displaying the information related to MAC VLANs from the information for all configured VLANs.

Figure 23-9: Example of displaying the MAC VLAN information

```
> show vlan mac-vlan
Date 20XX/09/21 14:15:00 UTC
VLAN counts:2    Total MAC Counts:5
VLAN ID:100     MAC Counts:4
   0012.e200.0001 (static)    0012.e200.0002 (static)
   0012.e200.0003 (static)    0012.e200.0004 (macauth)
VLAN ID:200     MAC Counts:1
   0012.e200.1111 (macauth)
>
```

Figure 23-10: Example of displaying the MAC VLAN information with the dynamic parameter specified

```
> show vlan mac-vlan dynamic
Date 20XX/09/21 14:15:00 UTC
VLAN counts:2    Total MAC Counts:3
```

```
VLAN ID:100     MAC Counts:2
 * 0012.e200.0003 (macauth)    0012.e200.0004 (macauth)
VLAN ID:200     MAC Counts:1
 0012.e200.1111 (macauth)
>
```

Figure 23-11: Example of displaying the MAC VLAN information with a MAC address specified

```
> show vlan mac-vlan 0012.e200.0003
Date 20XX/09/21 14:15:00 UTC
VLAN counts:1    Total MAC Counts:2
VLAN ID:100     MAC Counts:2
  0012.e200.0003 (static)   * 0012.e200.0003 (macauth)
>
```

Display items

Table 23-7: Display items for the MAC VLAN information

Item	Meaning	Displayed detailed information
VLAN Counts	Number of MAC VLANs to be displayed	—
Total MAC Counts	Number of displayed MAC addresses	Number of displayed MAC addresses. The total number of MAC addresses that include valid entries already assigned to the hardware (an asterisk (*) does not appear next to the displayed MAC address) and invalid entries that have not been assigned to the hardware (an asterisk (*) appears next to the displayed MAC address).
VLAN ID	VLAN information	VLAN ID
MAC Counts	Number of displayed MAC addresses for each VLAN	Number of MAC addresses displayed for the applicable VLAN
<MAC-address> (type)	Registered MAC address	type: Indicates which function registered the address. static: Indicates that the address was registered by configuration. dot1x: Indicates that the address was registered by IEEE 802.1X authentication. wa: Indicates that the address was registered by Web authentication. macauth: Indicates that the address was registered by MAC-based authentication. *: An asterisk (*) is added in either of the following cases: • - Dynamically registered entry that specifies a MAC address that is also specified in an entry registered by configuration • - Entry that has not been registered on hardware due to capacity limits

Impact on communication

None

Notes

None

restart vlan mac-manager

Restarts the L2MAC manager program.

Syntax

```
restart vlan mac-manager [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the L2MAC manager program without displaying a restart confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

When the L2MAC manager program is restarted, the core file of the program is output.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

After the restart confirmation message is output, the L2MAC manager program is restarted.

Example

Figure 23-12: Restarting the L2MAC manager program

```
> restart vlan mac-manager
L2 Mac Manager restart OK? (y/n): y
>
```

Figure 23-13: Restarting the L2MAC manager program (with the –f parameter specified)

```
> restart vlan mac-manager -f
>
```

Display items

None

Impact on communication

Ethernet interfaces with MAC VLAN or Layer 2 authentication configured may become unable to send or receive data temporarily.

Notes

- The storage directory and the name of the core file are as follows:

  Storage directory: /usr/var/core/

  Core file: L2MacManager.core

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

dump protocols vlan

Dumps detailed event trace information and control table information collected by the L2MAC manager program to a file.

Syntax

```
dump protocols vlan
```

Input mode

User mode and administrator mode

Parameters

None

Dumps detailed event trace information and control table information to a file.

Example

Figure 23-14: Taking a VLAN dump

```
> dump protocols vlan
>
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of an output file are as follows:

Storage directory: /usr/var/l2/

File: L2MacManager_dump.gz

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

24 Spanning Tree Protocols

show spanning-tree

Shows Spanning Tree information.

Syntax

```
show spanning-tree [ { vlan [ <vlan id list> ] | single | mst [ instance <mst instance id list>
 ] } [ port <port list> ] [channel-group-number <channel group list>] ] [ detail ] [active]
```

Input mode

User mode and administrator mode

Parameters

{ vlan [<vlan id list>] | single | mst [instance <mst instance id list>] }

vlan

Displays PVST+ Spanning Tree information.

<vlan id list>

Displays PVST+ Spanning Tree information for the VLAN IDs specified in list format.

For details about how to specify <vlan id list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

Statistics for all VLANs for which PVST+ is running are displayed.

single

Displays Single Spanning Tree information.

mst

Displays Multiple Spanning Tree information.

instance <mst instance id list>

Displays Multiple Spanning Tree information for the MST instance IDs specified in list format. Specifiable values for the MST instance ID are in the range from 0 to 4095.

If 0 is specified as the MST instance ID, CIST is subject to display.

Behavior when this parameter is omitted:

All MST instances are subject to display.

port <port list>

Displays Spanning Tree information for the specified port number. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters".

channel-group-number <channel group list>

Displays Spanning Tree information for the channel groups specified in list format in the specified link aggregation. For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when each parameter is omitted:

This command can display only the information relevant to the condition applied by a parameter that has been set. If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information conforming to the conditions will be displayed.

detail

Displays detailed information about Spanning Tree Protocols.

Behavior when this parameter is omitted:

All MST instances are subject to display.

active

Displays port information for only those ports in Up status.

Behavior when this parameter is omitted:

Information for all ports is displayed.

Behavior when all parameters are omitted:

Spanning Tree information for Single Spanning Tree, PVST+, and Multiple Spanning Tree is displayed.

Example 1

Figure 24-1: Displaying the PVST+ Spanning Tree information

```
> show spanning-tree vlan 10-13
Date 20XX/04/01 12:00:00 UTC
VLAN 10             PVST+ Spanning Tree:Enabled  Mode:Rapid PVST+
  Bridge ID        Priority:32778       MAC Address:0012.e200.0004
    Bridge Status:Designated
  Root Bridge ID   Priority:32778       MAC Address:0012.e200.0001
    Root Cost:2000000
    Root Port:1/0/1
  Port Information
    1/0/1      Up    Status:Forwarding  Role:Root       LoopGuard
    1/0/3      Up    Status:Discarding  Role:Backup
    1/0/4      Up    Status:Forwarding  Role:Designated PortFast(BPDU Guard)
    1/0/5      Up    Status:Discarding  Role:Alternate  LoopGuard
    1/0/8      Up    Status:Forwarding  Role:Designated RootGuard
    1/0/9      Down  Status:Disabled    Role:-
    1/0/10     Up    Status:Forwarding  Role:Designated PortFast  BPDU Filter
VLAN 11             PVST+ Spanning Tree:Disabled Mode:Rapid PVST+
VLAN 12             PVST+ Spanning Tree:Enabled  Mode:Rapid PVST+
  Bridge ID        Priority:32780       MAC Address:0012.e200.0004
    Bridge Status:Designated
  Root Bridge ID   Priority:32780       MAC Address:0012.e200.0002
    Root Cost:2000000
    Root Port:1/0/5
  Port Information
    1/0/5      Up    Status:Forwarding  Role:Root       Compatible
    1/0/6      Up    Status:Forwarding  Role:Designated Compatible
    1/0/7      Up    Status:Forwarding  Role:Designated
    1/0/9      Down  Status:Disabled    Role:-
VLAN 13(Disabled)   PVST+ Spanning Tree:Enabled  Mode:Rapid PVST+
>
```

Display items in Example 1

Table 24-1: Display items for the PVST+ Spanning Tree information

Item	Meaning	Displayed detailed information
VLAN	VLAN ID	ID of the VLAN on which PVST+ Spanning Tree Protocol is running. (Disabled) is displayed if the VLAN is not running.
PVST+ Spanning Tree:	Behavior status of the PVST+ Spanning Tree Protocol	Enabled: The Spanning Tree Protocol is running. Disabled: The Spanning Tree Protocol is not running.
Mode	Configured protocol type	PVST+: The protocol type is set to PVST+ mode. Rapid PVST+: The protocol type is set to Rapid PVST+ mode.
Bridge ID	Bridge ID of the Switch	—

Item	Meaning	Displayed detailed information
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address of the Switch
Bridge Status	Status of the Switch	Root: Root bridge Designated: Designated bridge
Root Bridge ID	Bridge ID for the root bridge	—
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address for the root bridge
Root Cost	Root path cost	Path cost value from the Switch to the root bridge "0" is displayed if the Switch is the root bridge.
Root Port	Root port	Displays the port number of the root port. If the root port is a link aggregation port, the port list for the channel group and the channel group number (ChGr) are displayed. A hyphen (-) is displayed if the Switch is the root bridge.
Port Information	Displays information about the ports managed by the PVST+ Spanning Tree Protocol.	
<switch no.>/<nif no.>/<port no.>	Port number or channel group number	The port number or channel group number of the port for which information is displayed
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
Status	Port status	If Mode is PVST+: Blocking: Blocking status Listening: Listening status Learning: Learning status Forwarding: Forwarding status Disabled: Disabled status If Mode is Rapid PVST+: Discarding: Discarding status Learning: Learning status Forwarding: Forwarding status Disabled: Disabled status This item shows Disabled if the port is in Down status.
Role	The role of the port	Root: Root port Designated: Designated port Alternate: Alternate port Backup: Backup port If the port is in Down status, a hyphen (-) is displayed because ports in this status are not included in the topology calculations. This item shows a value common to PVST+ and Rapid PVST+ in Mode.

Item	Meaning	Displayed detailed information
PortFast	PortFast	Indicates that the applicable port is a PortFast port.
PortFast(BPDU Guard)	PortFast (The BPDU guard function is applied)	Indicates that the applicable port is a PortFast port, and that the BPDU guard function is applied.
BPDU Filter	BPDU filter	Indicates that the BPDU filter function is applied.
LoopGuard	Loop guard	Indicates that the applicable port applies the loop guard function.
RootGuard	Root guard	Indicates that the applicable port applies the root guard function.
Compatible	Compatible mode	Indicates that the applicable port is running in compatible mode when Mode for the Spanning Tree Protocol is Rapid PVST+. Ports that are running in compatible mode do not perform rapid status transitions.

Example 2

Figure 24-2: Displaying the Single Spanning Tree information

```
> show spanning-tree single
Date 20XX/04/01 12:00:00 UTC
Single Spanning Tree:Enabled  Mode:STP
  Bridge ID        Priority:32768       MAC Address:0012.e200.0004
    Bridge Status:Designated
  Root Bridge ID   Priority:32768       MAC Address:0012.e200.0001
    Root Cost:2000000
    Root Port:1/0/1-2(ChGr:8)
  Port Information
    1/0/3      Up   Status:Blocking     Role:Alternate
    1/0/4      Up   Status:Forwarding   Role:Designated PortFast(BPDU Guard)
    1/0/5      Up   Status:Blocking     Role:Alternate  LoopGuard
    1/0/6      Up   Status:Forwarding   Role:Designated
    1/0/7      Up   Status:Forwarding   Role:Designated PortFast
    1/0/8      Up   Status:Forwarding   Role:Designated RootGuard
    1/0/9      Down Status:Disabled     Role:-
    1/0/10     Up   Status:Forwarding   Role:Designated PortFast  BPDU Filter
    ChGr:8     Up   Status:Forwarding   Role:Root       LoopGuard
>
```

Display items in Example 2

Table 24-2: Display items for the Single Spanning Tree information

Item	Meaning	Displayed detailed information
Single Spanning Tree:	Behavior status of the Single Spanning Tree Protocol	Enabled: The Spanning Tree Protocol is running. Disabled: The Spanning Tree Protocol is not running.
Mode	Configured protocol type	STP: The protocol type is set to STP mode. Rapid STP: The protocol type is set to Rapid STP mode.
Bridge ID	Bridge ID of the Switch	—
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address of the Switch

Item	Meaning	Displayed detailed information
Bridge Status	Status of the Switch	Root: Root bridge Designated: Designated bridge
Root Bridge ID	Bridge ID for the root bridge	—
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address for the root bridge
Root Cost	Root path cost	Path cost value from the Switch to the root bridge "0" is displayed if the Switch is the root bridge.
Root Port	Root port	Displays the port number of the root port. If the root port is a link aggregation port, the port list for the channel group and the channel group number (ChGr) are displayed. A hyphen (-) is displayed if the Switch is the root bridge.
Port Information	Displays information about the ports managed by Single Spanning Tree.	
<switch no.>/<nif no.>/<port no.>	Port number or channel group number	The port number or channel group number of the port for which information is displayed
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
Status	Port status	If Mode is STP: Blocking: Blocking status Listening: Listening status Learning: Learning status Forwarding: Forwarding status Disabled: Disabled status If Mode is Rapid STP: Discarding: Discarding status Learning: Learning status Forwarding: Forwarding status Disabled: Disabled status This item shows Disabled if the port is in Down status.
Role	The role of the port	Root: Root port Designated: Designated port Alternate: Alternate port Backup: Backup port If the port is in Down status, a hyphen (-) is displayed because ports in this status are not included in the topology calculations. This item shows a value common to STP and Rapid STP in Mode.

Item	Meaning	Displayed detailed information
PortFast	PortFast	Indicates that the applicable port is a PortFast port.
PortFast(BPDU Guard)	PortFast (The BPDU guard function is applied)	Indicates that the applicable port is a PortFast port, and that the BPDU guard function is applied.
BPDU Filter	BPDU filter	Indicates that the BPDU filter function is applied.
LoopGuard	Loop guard	Indicates that the applicable port applies the loop guard function.
RootGuard	Root guard	Indicates that the applicable port applies the root guard function.
Compatible	Compatible mode	Indicates that the applicable port is running in compatible mode when Mode for the Spanning Tree Protocol is Rapid STP+. Ports that are running in compatible mode do not perform rapid status transitions.

Example 3

Figure 24-3: Displaying the Multiple Spanning Tree information

```
> show spanning-tree mst instance 0-4095
Date 20XX/04/01 12:00:00 UTC
Multiple Spanning Tree: Enabled
Revision Level: 65535  Configuration Name: MSTP Region Tokyo
CIST Information
  VLAN Mapped: 1,3-4093,4095
  Unmatch VLAN Mapped: -
  CIST Root      Priority: 4096        MAC      : 0012.e200.0001
  External Root Cost     : 2000000     Root Port: 1/0/1-2(ChGr:8)
  Regional Root  Priority: 32768       MAC      : 0012.e200.0003
  Internal Root Cost     : 0
  Bridge ID      Priority: 32768       MAC      : 0012.e200.0003
  Regional Bridge Status : Root
  Port Information
    1/0/4      Up   Status:Blocking    Role:Alternate   Boundary  Compatible
    1/0/7      Up   Status:Forwarding  Role:Designated
    1/0/8      Up   Status:Forwarding  Role:Designated  RootGuard
    1/0/10     Up   Status:Forwarding  Role:Designated
    1/0/11     Up   Status:Forwarding  Role:Designated  BPDUGuard
    1/0/12     Up   Status:Forwarding  Role:Designated  BPDUFilter
    ChGr:8     Up   Status:Forwarding  Role:Root        Boundary
MST Instance 1
  VLAN Mapped: 2,4094
  Unmatch VLAN Mapped: -
  Regional Root  Priority: 4097        MAC      : 0012.e200.0004
  Internal Root Cost     : 2000000     Root Port: 1/0/7
  Bridge ID      Priority: 32769       MAC      : 0012.e200.0003
  Regional Bridge Status : Designated
  Port Information
    1/0/4      Up   Status:Blocking    Role:Alternate   Boundary  Compatible
    1/0/7      Up   Status:Forwarding  Role:Root
    1/0/10     Up   Status:Blocking    Role:Alternate
    1/0/11     Up   Status:Forwarding  Role:Designated  BPDUGuard
    ChGr:8     Up   Status:Forwarding  Role:Master      Boundary
>
```

Display items in Example 3

Table 24-3: Display items for the Multiple Spanning Tree information

Item	Meaning	Displayed detailed information
Multiple Spanning Tree	Behavior status of Multiple Spanning Tree	Enabled: Running Disabled: Disabled

Item	Meaning	Displayed detailed information
Revision Level	Revision level	Displays the revision level that is set in the configuration. 0 to 65535
Configuration Name	Region name	Displays the region name that is set in the configuration. 0 to 32 characters
CIST Information	CIST Spanning Tree information	CIST Spanning Tree information
VLAN Mapped	Instance mapping VLAN	Lists the VLANs allocated to MST instance 0 (IST). A hyphen (-) is displayed if no VLANs are allocated. The Switch supports 1 to 4094 VLAN IDs, although according to the standard, 1 to 4095 VLAN IDs are used for region configuration. VLAN IDs from 1 to 4095 are clearly displayed so that you can determine which instance each VLAN ID supported by the standard belongs to.
Unmatch VLAN Mapped	Instance mapping VLAN in Blocking status	If Ring Protocol is also used, this item displays instance mapping VLANs whose Spanning Tree Protocols are blocked because of mismatches with the VLAN mapping of Ring Protocol. A hyphen (-) is displayed if there is no mismatch.
CIST Root	Bridge ID for the CIST root bridge	—
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address for the CIST root bridge
External Root Cost	External root path cost	Path cost value from the Switch's CIST internal bridge to the CIST root bridge. "0" is displayed if the Switch is the CIST root bridge.
Root Port	Root port	Displays the port number of the CIST root port. If the CIST root port is a link aggregation port, the link aggregation port list and the channel group number are displayed. A hyphen (-) is displayed if the Switch is the CIST root bridge.
Regional Root	Bridge ID for the regional root bridge of MST instance 0 (IST)	Displays information about the regional root bridge of MST instance 0 (IST).
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address for the regional root bridge of MST instance 0 (IST)
Internal Root Cost	Internal root path cost for MST instance 0 (IST)	Path cost value from the Switch to the regional root bridge of MST instance 0 (IST). "0" is displayed if the Switch is the regional root bridge of MST instance 0 (IST). A hyphen (-) is displayed if Multiple Spanning Tree is disabled.
Bridge ID	Bridge ID for MST instance 0 (IST) of the Switch	Displays information about the bridge of MST instance 0 (IST) of the Switch.

Item	Meaning	Displayed detailed information
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	The MAC address of the Switch.
Regional Bridge Status	Status of the bridge for MST instance 0 (IST) of the Switch	Root: Root bridge Designated: Designated bridge
MST Instance	MST instance ID	Displays the MST instance ID and information about the instance.
VLAN Mapped	Instance mapping VLAN	Lists the VLANs allocated to the MST instance. A hyphen (-) is displayed if no VLANs are allocated.
Unmatch VLAN Mapped	Instance mapping VLAN in Blocking status	If Ring Protocol is also used, this item displays instance mapping VLANs whose Spanning Tree Protocols are blocked because of mismatches with the VLAN mapping of Ring Protocol. A hyphen (-) is displayed if there is no mismatch.
Regional Root	Bridge ID of the regional root bridge of the MST instance	Displays information about the regional root bridge of the MST instance.
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address for the regional root bridge of the MST instance
Internal Root Cost	Internal root path cost for the MST instance	Path cost value from the Switch to the regional root bridge of MST instance. "0" is displayed if the Switch is the regional root bridge of the MST instance.
Root Port	Root port of the MST instance	Displays the port number of the root port of the MST instance. If the root port of the MST instance is a link aggregation port, the link aggregation port list and the channel group number are displayed. A hyphen (-) is displayed if the Switch is the regional root bridge of the MST instance.
Bridge ID	Bridge ID for the MST instance of the Switch	Displays information about the bridge of the MST instance of the Switch.
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	The MAC address of the Switch.
Regional Bridge Status	Status of the bridge of the MST instance of the Switch	Root: Root bridge Designated: Designated bridge
Port Information	Information about the ports of the MST instance	Displays information about the ports managed by Multiple Spanning Tree. If no VLANs are allocated to the MST instance, a response message is displayed because there are no ports.

Item	Meaning	Displayed detailed information
<switch no.>/<nif no.>/ <port no.>	Port number or channel group number	The port number or channel group number of the port for which information is displayed
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
Status	Port status	Discarding: Discarding status Learning: Learning status Forwarding: Forwarding status Disabled: Disabled status This item shows Disabled if the port is in Down status.
Role	The role of the port	Root: Root port Designated: Designated port Alternate: Alternate port Backup: Backup port Master: Master port If the port is in Down status, a hyphen (-) is displayed because ports in this status are not included in the topology calculations.
Boundary	Boundary port	Indicates that the port is the boundary port for the region. If the role of the port of the partner device is an alternate port or backup port, the boundary port might never receive BPDUs. In such cases, the port is not displayed as the boundary port.
PortFast	PortFast	Indicates that the applicable port is a PortFast port. (Received): Indicates that the port is subject to the Spanning Tree topology calculations because BPDUs are received while PortFast is being applied.
BPDUGuard	Application of the BPDU guard function for PortFast	Indicates that the applicable port is a PortFast port, and that the BPDU guard function is applied. (Received): Indicates that the port is down because BPDUs are received while PortFast is being applied.
BPDUFilter	BPDU filter	Indicates that the BPDU filter function is applied.
RootGuard	Root guard	Indicates that the applicable port applies the root guard function.
Compatible	Compatible mode	Indicates that the port is running in compatible mode for an MSTP Spanning Tree Protocol. Ports that are running in compatible mode do not perform rapid status transitions.

Example 4

Figure 24-4: Displaying the detailed PVST+ Spanning Tree information

```
> show spanning-tree vlan 10 detail
Date 20XX/04/01 12:00:00 UTC
VLAN 10             PVST+ Spanning Tree:Enabled  Mode:Rapid PVST+
  Bridge ID
    Priority:32778                  MAC Address:0012.e200.0004
    Bridge Status:Designated        Path Cost Method:Long
    Max Age:20                      Hello Time:2
    Forward Delay:15
  Root Bridge ID
    Priority:32778                  MAC Address: 0012.e200.0001
    Root Cost:2000000
    Root Port:1/0/1
    Max Age:20                      Hello Time:2
    Forward Delay:15
  Port Information
  Port:1/0/1 Up
    Status:Forwarding               Role:Root
    Priority:128                    Cost:2000000
    LinkType:point-to-point         Compatible Mode:-
    LoopGuard:ON                    PortFast:OFF
    BpduFilter:OFF                  RootGuard:OFF
    BPDU Parameters(20XX/04/01 12:00:00):
      Designated Root
        Priority:32778              MAC Address: 0012.e200.0001
      Designated Bridge
        Priority:32778              MAC Address: 0012.e200.0001
        Root Cost:0
      Port ID
        Priority:128                Number:16
      Message Age Time:1(2)/20
  Port:1/0/3 Up
    Status:Discarding               Role:Backup
    Priority:128                    Cost:2000000
    LinkType:point-to-point         Compatible Mode:-
    LoopGuard:OFF                   PortFast:OFF
    BpduFilter:OFF                  RootGuard:OFF
    BPDU Parameters(20XX/04/01 12:00:00):
      Designated Root
        Priority:32778              MAC Address: 0012.e200.0001
      Designated Bridge
        Priority:32778              MAC Address: 0012.e200.0001
        Root Cost:0
      Port ID Priority:128          Number:8
      Message Age Time:5(2)/20
  Port:1/0/4 Up
    Status:Disabled(unmatched)      Role:-
    Priority:-                      Cost:-
    LinkType:-                      Compatible Mode:-
    LoopGuard:OFF                   PortFast:BPDU Guard(BPDU not received)
    BpduFilter:OFF                  RootGuard:OFF
  Port:1/0/5 Up
    Status:Discarding               Role:Alternate
    Priority:128                    Cost:2000000
    LinkType:point-to-point         Compatible Mode:-
    LoopGuard:ON(Blocking)          PortFast:OFF
    BpduFilter:OFF                  RootGuard:OFF
    BPDU Parameters(20XX/04/01 12:00:00):
      Designated Root
        Priority:32778              MAC Address:0012.e200.0001
      Designated Bridge
        Priority:32778              MAC Address:0012.e200.0002
        Root Cost:200000
      Port ID Priority:128          Number:16
      Message Age Time:2(2)/20
  Port:1/0/10 Up
    Status:Forwarding               Role:Designated
    Priority:128                    Cost:2000000
    LinkType:point-to-point         Compatible Mode:-
    LoopGuard:OFF                   PortFast:ON
    BpduFilter:ON                   RootGuard:OFF
  Port:1/0/11 Up
    Status:Discarding               Role:Designated
    Priority:128                    Cost:2000000
    LinkType:point-to-point         Compatible Mode:-
```

```
    LoopGuard:OFF                   PortFast:OFF
    BpduFilter:OFF                  RootGuard:ON(Blocking)
    BPDU Parameters(20XX/04/01 12:00:00):
      Designated Root
        Priority:4096               MAC Address:0012.e200.0011
      Designated Bridge
        Priority:32778              MAC Address:0012.e200.0022
        Root Cost:200000
      Port ID Priority:128          Number:16
      Message Age Time:2(2)/20
>
```

Display items in Example 4

Table 24-4: Display items for the detailed PVST+ Spanning Tree information

Item	Meaning	Displayed detailed information
VLAN	VLAN ID	ID of the VLAN on which PVST+ Spanning Tree Protocol is running. (Disabled) is displayed if the VLAN is not running.
PVST+ Spanning Tree:	Behavior status of the PVST+ Spanning Tree Protocol	Enabled: The Spanning Tree Protocol is running. Disabled: The Spanning Tree Protocol is not running.
Mode	Configured protocol type	PVST+: The protocol type is set to PVST+ mode. Rapid PVST+: The protocol type is set to Rapid PVST+ mode.
Bridge ID	Bridge ID of the Switch	—
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address of the Switch
Bridge Status	Status of the Switch	Root: Root bridge Designated: Designated bridge
Path Cost Method	Path cost length mode	Long: 32-bit values are used for the path cost value. Short: 16-bit values are used for the path cost value.
Max Age	Maximum valid time of BPDUs	Maximum valid time of BPDUs sent from the Switch
Hello Time	BPDU sending interval	Sending interval of BPDUs that are regularly sent from the Switch
Forward Delay	Time required for a status transition of the port	Time required for a status transition when the status transition is triggered by the timer
Root Bridge ID	Bridge ID for the root bridge	—
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address for the root bridge
Root Cost	Root path cost	Path cost value from the Switch to the root bridge "0" is displayed if the Switch is the root bridge.

Item	Meaning	Displayed detailed information
Root Port	Root port	Displays the port number of the root port. If the root port is a link aggregation port, the port list for the channel group and the channel group number (ChGr) are displayed. A hyphen (-) is displayed if the Switch is the root bridge.
Max Age	Maximum valid time of BPDUs sent from the root bridge	Maximum valid time of BPDUs sent from the root bridge
Hello Time	Sending interval of BPDUs sent from the root bridge	Sending interval of BPDUs that are regularly sent from the root bridge
Forward Delay	Time required for a status transition of the root bridge port	Time required for a status transition when the status transition in the root bridge is triggered by the timer
Port	Port number or channel group number	The port number or channel group number of the port for which information is displayed
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
Status	Port status	If Mode is PVST+: Blocking: Blocking status Listening: Listening status Learning: Learning status Forwarding: Forwarding status Disabled: Disabled status. This status is displayed when the port is in Down status. Disabled(unmatched): Disabled status. A configuration mismatch was detected because a BPDU with an IEEE 802.1Q VLAN tag was received when the port was disabled. If Mode is Rapid PVST+: Discarding: Discarding status Learning: Learning status Forwarding: Forwarding status Disabled: Disabled status. This status is displayed when the port is in Down status. Disabled(unmatched): Disabled status. A configuration mismatch was detected because a BPDU with an IEEE 802.1Q VLAN tag was received when the port was disabled.
Role	The role of the port	Root: Root port Designated: Designated port Alternate: Alternate port Backup: Backup port If the port is in Down status, a hyphen (-) is displayed because ports in this status are not included in the topology calculations. This item shows a value common to STP and Rapid STP.
Priority	Port priority	Value set for the port priority of the port on the Switch If the port is in Down status, a hyphen (-) is displayed.

Item	Meaning	Displayed detailed information
Cost	Port cost	Value set for the port cost of the Switch. If the port is in Down status, a hyphen (-) is displayed.
Link Type	Link type of the line	point-to-point: The line is a 1-to-1 connection. shared: The line is a shared connection. A hyphen (-) is displayed when Mode is PVST+ or when the port is in Down status.
Compatible Mode	Compatible mode	ON: Running in compatible mode. A hyphen (-) is displayed when the port is running in normal mode (non-compatible mode) or when the port is in Down status. Ports that are running in compatible mode do not perform rapid status transitions.
Loop Guard	Loop guard function	ON: The loop guard function is being applied. ON(Blocking): The loop guard function is running and the port is blocked. OFF: The loop guard function is not being used.
PortFast	Status of PortFast. The receive status of BPDUs is displayed enclosed in parentheses.	OFF: PortFast is not operating. ON: PortFast is operating. BPDU Guard: The BPDU guard function is being applied in PortFast. The receive status of BPDUs is displayed when this item is ON or BPDU Guard. • BPDU received (when PortFast is ON: The port is included in the calculations of the Spanning Tree topology, when PortFast is BPDU Guard: The port is down) • BPDU not received (the port is not included in the calculations of the Spanning Tree topology)
BpduFilter	BPDU filter	ON: The BPDU filter function is being applied. OFF: The BPDU filter function is not being used.
Root Guard	Root guard function	ON: The root guard function is being applied. ON(Blocking): The root guard function is running and the port is blocked. OFF: The root guard function is not being used.
BPDU Parameters	Information about received BPDUs on the applicable port. The last time a BPDU was received is displayed enclosed in parentheses.	Displays information about the BPDUs received on the port. This item is not displayed if BPDUs are not received. If the port is blocked by the root guard function, this item displays information about the BPDUs that caused the port to be blocked.
Designated Root	Root bridge information stored in the BPDU	—
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address for the root bridge
Designated Bridge	Bridge information stored in the BPDU	—
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.

Item	Meaning	Displayed detailed information
MAC Address	MAC address	MAC address
Root Cost	Root path cost	Root path cost stored in the BPDU
Port ID	Port information stored in the BPDU	—
Priority	Port priority	0 to 255 The lower the value, the higher the priority.
Number	Port number	0 to 897
Message Age Time	Valid time of received BPDUs	Indicates how long received BPDUs are valid. A hyphen (-) is displayed if this period has expired. <current-time>(<time-BPDU-received>)/<maximum-time> <current-time>: The time at which the BPDU is received plus the time that has elapsed <time-BPDU-received>: The time that has elapsed when the BPDU is received (Message Age of the received BPDU) <maximum-time>: Valid time (Max Age of the received BPDU)

Example 5

Figure 24-5: Displaying the detailed Single Spanning Tree information

```
> show spanning-tree single detail
Date 20XX/04/01 12:00:00 UTC
Single Spanning Tree:Enabled  Mode:STP
  Bridge ID
    Priority:32768                  MAC Address:0012.e200.0004
    Bridge Status:Designated        Path Cost Method:Long
    Max Age:20                      Hello Time:2
    Forward Delay:15
  Root Bridge ID
    Priority:32768                  MAC Address: 0012.e200.0001
    Root Cost:2000000
    Root Port:1/0/1-2(ChGr:8)
    Max Age:20                      Hello Time:2
    Forward Delay:15
  Port Information
  Port:1/0/3 Up
    Status:Blocking                 Role:Alternate
    Priority:128                    Cost:2000000
    LinkType:-                      Compatible Mode:-
    LoopGuard:OFF                   PortFast:OFF
    BpduFilter:OFF                  RootGuard:OFF
    BPDU Parameters(20XX/04/01 12:00:00):
      Designated Root
        Priority:32768              MAC Address:0012.e200.0001
      Designated Bridge
        Priority:32768              MAC Address:0012.e200.0001
        Root Cost:0
      Port ID
        Priority:128                Number:8
      Message Age Time:5(2)/20
  Port:1/0/4 Up
    Status:Forwarding               Role:Designated
    Priority:128                    Cost:2000000
    LinkType:-                      Compatible Mode:-
    LoopGuard:OFF                   PortFast:BPDU Guard(BPDU not received)
    BpduFilter:OFF                  RootGuard:OFF
  Port:1/0/5 Up
    Status:Blocking                 Role:Alternate
    Priority:128                    Cost:2000000
```

```
    LinkType:-                      Compatible Mode:-
    LoopGuard:ON(Blocking)          PortFast:OFF
    BpduFilter:OFF                  RootGuard:OFF
  Port:1/0/9 Up
    Status:Disabled(unavailable)    Role:-
    Priority:-                      Cost:-
    LinkType:-                      Compatible Mode:-
    LoopGuard:OFF                   PortFast:OFF
    BpduFilter:OFF                  RootGuard:OFF
  Port:1/0/10 Up
    Status:Forwarding               Role:Designated
    Priority:128                    Cost:2000000
    LinkType:point-to-point         Compatible Mode:-
    LoopGuard:OFF                   PortFast:ON
    Bpdu Filter:ON                  RootGuard:OFF
  Port:1/0/11 Up
    Status:Blocking                 Role:Designated
    Priority:128                    Cost:2000000
    LinkType:-                      Compatible Mode:-
    LoopGuard:OFF                   PortFast:OFF
    BpduFilter:OFF                  RootGuard:ON(Blocking)
  BPDU Parameters(20XX/04/01 12:00:00):
      Designated Root
        Priority:4096               MAC Address:0012.e200.0011
      Designated Bridge
        Priority:32768              MAC Address:0012.e200.0022
        Root Cost:0
      Port ID
        Priority:128                Number:16
      Message Age Time:1(2)/20
  Port:ChGr:8 Up
    Status:Forwarding               Role:Root
    Priority:128                    Cost:2000000
    LinkType:-                      Compatible Mode:-
    LoopGuard:ON                    PortFast:OFF
    BpduFilter:OFF                  RootGuard:OFF
    BPDU Parameters(20XX/04/01 12:00:00):
      Designated Root
        Priority:32768              MAC Address:0012.e200.0001
      Designated Bridge
        Priority:32768              MAC Address:0012.e200.0001
        Root Cost:0
      Port ID
        Priority:128                Number:16
      Message Age Time:1(2)/20
>
```

Display items in Example 5

Table 24-5: Display items for the detailed Single Spanning Tree information

Item	Meaning	Displayed detailed information
Single Spanning Tree:	Behavior status of the Single Spanning Tree Protocol	Enabled: The Spanning Tree Protocol is running. Disabled: The Spanning Tree Protocol is not running.
Mode	Configured protocol type	STP: The protocol type is set to STP mode. Rapid STP: The protocol type is set to Rapid STP mode.
Bridge ID	Bridge ID of the Switch	—
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address of the Switch
Bridge Status	Status of the Switch	Root: Root bridge Designated: Designated bridge

Item	Meaning	Displayed detailed information
Path Cost Method	Path cost length mode	Long: 32-bit values are used for the path cost value. Short: 16-bit values are used for the path cost value.
Max Age	Maximum valid time of BPDUs	Maximum valid time of BPDUs sent from the Switch
Hello Time	BPDU sending interval	Sending interval of BPDUs that are regularly sent from the Switch
Forward Delay	Time required for a status transition of the port	Time required for a status transition when the status transition is triggered by the timer
Root Bridge ID	Bridge ID for the root bridge	—
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address for the root bridge
Root Cost	Root path cost	Path cost value from the Switch to the root bridge "0" is displayed if the Switch is the root bridge.
Root Port	Root port	Displays the port number of the root port. If the root port is a link aggregation port, the port list and the channel group number (ChGr) for the link aggregation are displayed. A hyphen (-) is displayed if the Switch is the root bridge.
Max Age	Maximum valid time of BPDUs sent from the root bridge	Maximum valid time of BPDUs sent from the root bridge
Hello Time	Sending interval of BPDUs sent from the root bridge	Sending interval of BPDUs that are regularly sent from the root bridge
Forward Delay	Time required for a status transition of the root bridge port	Time required for a status transition when the status transition in the root bridge is triggered by the timer
Port	Port number or channel group number	The port number or channel group number of the port for which information is displayed
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
Status	Port status	If Mode is STP: Blocking: Blocking status Listening: Listening status Learning: Learning status Forwarding: Forwarding status Disabled: Disabled status. This status is displayed when the port is in Down status. Disabled(unavailable): Disabled status. Single Spanning Tree cannot be used because PVST+ is enabled for the port. If Mode is Rapid STP:

Item	Meaning	Displayed detailed information
		Discarding: Discarding status Learning: Learning status Forwarding: Forwarding status Disabled: Disabled status. This status is displayed when the port is in Down status. Disabled(unavailable): Disabled status. Single Spanning Tree cannot be used because PVST+ is enabled for the port.
Role	The role of the port	Root: Root port Designated: Designated port Alternate: Alternate port Backup: Backup port If the port is in Down status, a hyphen (-) is displayed because ports in this status are not included in the topology calculations. This item shows a value common to STP and Rapid STP.
Priority	Port priority	Value set for the port priority of the port on the Switch If the port is in Down status, a hyphen (-) is displayed.
Cost	Port cost	Value set for the port cost of the Switch. If the port is in Down status, a hyphen (-) is displayed.
Link Type	Link type of the line	point-to-point: The line is a 1-to-1 connection. shared: The line is a shared connection. A hyphen (-) is displayed when Mode is PVST+ or when the port is in Down status.
Compatible Mode	Compatible mode	ON: Running in compatible mode. A hyphen (-) is displayed when the port is running in normal mode (non-compatible mode) or when the port is in Down status. Ports that are running in compatible mode do not perform rapid status transitions.
Loop Guard	Loop guard function	ON: The loop guard function is being applied. ON(Blocking): The loop guard function is running and the port is blocked. OFF: The loop guard function is not being used.
PortFast	Status of PortFast. The receive status of BPDUs is displayed enclosed in parentheses.	OFF: PortFast is not operating. ON: PortFast is operating. BPDU Guard: The BPDU guard function is being applied in PortFast. The receive status of BPDUs is displayed when this item is ON or BPDU Guard. • BPDU received (when PortFast is ON: The port is included in the calculations of the Spanning Tree topology, when PortFast is BPDU Guard: The port is down) • BPDU not received (the port is not included in the calculations of the Spanning Tree topology)
BpduFilter	BPDU filter	ON: The BPDU filter function is being applied. OFF: The BPDU filter function is not being used.
Root Guard	Root guard function	ON: The root guard function is being applied. ON(Blocking): The root guard function is running and the port is blocked. OFF: The root guard function is not being used.

Item	Meaning	Displayed detailed information
BPDU Parameters	Information about received BPDUs on the applicable port. The last time a BPDU was received is displayed enclosed in parentheses.	Displays information about the BPDUs received on the port. This item is not displayed if BPDUs are not received. If the port is blocked by the root guard function, this item displays information about the BPDUs that caused the port to be blocked.
Designated Root	Root bridge information stored in the BPDU	—
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address for the root bridge
Designated Bridge	Bridge information stored in the BPDU	—
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address
Root Cost	Root path cost	Root path cost stored in the BPDU
Port ID	Port information stored in the BPDU	—
Priority	Port priority	0 to 255 The lower the value, the higher the priority.
Number	Port number	0 to 897
Message Age Time	Valid time of received BPDUs	Indicates how long received BPDUs are valid. A hyphen (-) is displayed if this period has expired. <current-time>(<time-BPDU-received>)/<maximum-time> <current-time>: The time at which the BPDU is received plus the time that has elapsed <time-BPDU-received>: The time that has elapsed when the BPDU is received (Message Age of the received BPDU) <maximum-time>: Valid time (Max Age of the received BPDU)

Example 6

Figure 24-6: Displaying the detailed Multiple Spanning Tree information

```
> show spanning-tree mst detail
Date 20XX/04/01 12:00:00 UTC
Multiple Spanning Tree: Enabled
Revision Level: 65535  Configuration Name: MSTP Region Tokyo
CIST Information           Time Since Topology Change: 2.4:25:50
  VLAN Mapped: 1,3-4093,4095
  Unmatch VLAN Mapped: -
  CIST Root      Priority: 4096        MAC           : 0012.e200.0001
  External Root Cost     : 2000000     Root Port     : 1/0/1-2(ChGr:8)
  Max Age                : 20
  Forward Delay          : 15
  Regional Root  Priority: 32768       MAC           : 0012.e200.0003
  Internal Root Cost     : 0
  Remaining Hops         : 20
```

```
  Bridge ID      Priority: 32768       MAC             : 0012.e200.0003
  Regional Bridge Status : Root        Path Cost Method: Long
  Max Age                : 20          Hello Time      : 2
  Forward Delay          : 15          Max Hops        : 20
  Port Information
  Port:1/0/4  Up    Boundary  Compatible
    Status    : Blocking         Role      : Alternate
    Priority  : 128              Cost      : 2000000
    Link Type : shared           PortFast  : OFF
    BpduFilter: OFF              Hello Time: 4
    RootGuard : OFF
    BPDU Parameters(20XX/04/01 12:00:00):
      Protocol Version  : STP(IEEE802.1D)
      Root              Priority: 4096    MAC    : 0012.e200.0001
      External Root Cost          : 2000000
      Designated Bridge Priority: 32768   MAC    : 0012.e200.0002
      Designated Port ID  Priority: 128     Number : 1
      Message Age Timer : 1(2)/20    Remaining Hops: -
  Port:1/0/7  Up
    Status    : Forwarding       Role      : Designated
    Priority  : 128              Cost      : 2000000
    Link Type : point-to-point   PortFast  : OFF
    BpduFilter: OFF              Hello Time: 2
    RootGuard : OFF
    BPDU Parameters(20XX/04/01 12:00:00):
      Protocol Version  : MSTP(IEEE802.1s)
      Root              Priority: 4096    MAC    : 0012.e200.0001
      External Root Cost          : 2000000
      Regional Root       Priority: 4096    MAC    : 0012.e200.0003
      Internal Root Cost          : 2000000
      Designated Bridge   Priority: 32768   MAC    : 0012.e200.0004
      Designated Port ID  Priority: 128     Number : 2
      Message Age Timer : 1(2)/20    Remaining Hops: 19
  Port:1/0/10  Up
    Status    : Forwarding       Role      : Designated
    Priority  : 128              Cost      : 2000000
    LinkType  : point-to-point   PortFast  : OFF
    BpduFilter: OFF              Hello Time: 2
    RootGuard : OFF
    BPDU Parameters(20XX/04/01 12:00:00):
      Protocol Version  : MSTP(IEEE802.1s)
      Root              Priority: 4096    MAC    : 0012.e200.0001
      External Root Cost          : 2000000
      Regional Root       Priority: 4096    MAC    : 0012.e200.0003
      Internal Root Cost          : 2000000
      Designated Bridge   Priority: 32768   MAC    : 0012.e200.0005
      Designated Port ID  Priority: 128     Number : 3
      Message Age Timer : 1(2)/20    Remaining Hops: 19
  Port:1/0/11  Up
    Status    : Forwarding       Role      : Designated
    Priority  : 128              Cost      : 2000000
    Link Type : point-to-point   PortFast  : BPDU Guard(BPDU not received)
    BpduFilter: OFF              Hello Time: 2
    RootGuard : OFF
  Port:1/0/12  Up
    Status    : Forwarding       Role      : Designated
    Priority  : 128              Cost      : 2000000
    Link Type : point-to-point   PortFast  : BPDU Filter
    BpduFilter: ON               Hello Time: 2
    RootGuard : OFF
  Port:ChGr:8   Up    Boundary
    Status    : Forwarding       Role      : Root
    Priority  : 128              Cost      : 2000000
    Link Type : point-to-point   PortFast  : OFF
    BpduFilter: OFF              Hello Time: 4
    RootGuard : OFF
    BPDU Parameters(20XX/04/01 12:00:00):
      Protocol Version  : MSTP(IEEE802.1s)
      Root              Priority: 4096    MAC    : 0012.e200.0001
      External Root Cost          : 2000000
      Regional Root       Priority: 4096    MAC    : 0012.e200.0001
      Internal Root Cost          : 2000000
      Designated Bridge   Priority: 32768   MAC    : 0012.e200.0001
      Designated Port ID  Priority: 128     Number : 800
      Message Age Timer : 1(2)/20    Remaining Hops: 19
MST Instance 1             Time Since Topology Change: 2.4:25:30
  VLAN Mapped: 2,4094
  Unmatch VLAN Mapped: -
  Regional Root  Priority: 4097        MAC           : 0012.e200.0004
```

```
  Internal Root Cost     : 2000000     Root Port     : 1/0/7
  Remaining Hops         : 20
  Bridge ID      Priority: 32768       MAC           : 0012.e200.0003
  Regional Bridge Status : Designated
  Max Age                : 20          Hello Time    : 2
  Forward Delay          : 15          Max Hops      : 20
  Port Information
  Port:1/0/4  Up    Boundary  Compatible
    Status    : Blocking         Role      : Alternate
    Priority  : 128              Cost      : 2000000
    Link Type : shared           PortFast  : OFF
    BpduFilter: OFF              Hello Time: 2
    RootGuard : OFF
  Port:1/0/7  Up
    Status    : Forwarding       Role      : Root
    Priority  : 128              Cost      : 2000000
    Link Type : point-to-point   PortFast  : OFF
    BpduFilter: OFF              Hello Time: 4
    RootGuard : OFF
    BPDU Parameters(20XX/04/01 12:00:00):
      Protocol Version  : MSTP(IEEE802.1s)
      Regional Root       Priority: 4096    MAC    : 0012.e200.0004
      Internal Root Cost          : 2000000
      Designated Bridge   Priority: 32768   MAC    : 0012.e200.0004
      Designated Port ID  Priority: 128     Number : 2
      Message Age Timer : 1(2)/20    Remaining Hops: 19
  Port:1/0/10  Up
    Status    : Blocking         Role      : Alternate
    Priority  : 128              Cost      : 2000000
    Link Type : point-to-point   PortFast  : OFF
    BpduFilter: OFF              Hello Time: 4
    RootGuard : OFF
    BPDU Parameters(20XX/04/01 12:00:00):
      Protocol Version  : MSTP(IEEE802.1s)
      Regional Root       Priority: 4096    MAC    : 0012.e200.0004
      Internal Root Cost          : 2000000
      Designated Bridge   Priority: 32768   MAC    : 0012.e200.0002
      Designated Port ID  Priority: 128     Number : 3
      Message Age Timer : 1(2)/20    Remaining Hops: 19
  Port:1/0/11  Up
    Status    : Forwarding       Role      : Designated
    Priority  : 128              Cost      : 2000000
    Link Type : point-to-point   PortFast  : BPDU Guard(BPDU not received)
    BpduFilter: OFF              Hello Time: 2
    RootGuard : OFF
  Port:ChGr:8   Up    Boundary
    Status    : Forwarding       Role      : Master
    Priority  : 128              Cost      : 2000000
    Link Type : point-to-point   PortFast  : OFF
    BpduFilter: OFF              Hello Time: 4
    RootGuard : OFF
    BPDU Parameters(20XX/04/01 12:00:00):
      Protocol Version  : MSTP(IEEE802.1s)
      Regional Root       Priority: 4096    MAC    : 0012.e200.0004
      Internal Root Cost          : 2000000
      Designated Bridge   Priority: 32768   MAC    : 0012.e200.0001
      Designated Port ID  Priority: 128     Number : 800
      Message Age Timer : 1(2)/20    Remaining Hops: 19
>
```

Display items in Example 6

Table 24-6: Display items for the detailed Multiple Spanning Tree information

Item	Meaning	Displayed detailed information
Multiple Spanning Tree	Behavior status of Multiple Spanning Tree	Enabled: Running Disabled: Disabled
Revision Level	Revision level	Displays the revision level that is set in the configuration. 0 to 65535

Item	Meaning	Displayed detailed information
Configuration Name	Region name	Displays the region name that is set in the configuration. 0 to 32 characters
CIST Information	CIST Spanning Tree information	CIST Spanning Tree information
Time Since Topology Change	Time since a topology change was detected	hh:mm:ss (when the elapsed time is less than 24 hours) ddd.hh:mm:ss (when the elapsed time exceeds 24 hours) Over 1000 days (when the elapsed time is more than 1000 days)
VLAN Mapped	Instance mapping VLAN	Lists the VLANs allocated to MST instance 0 (IST). A hyphen (-) is displayed if no VLANs are allocated. The Switch supports 1 to 4094 VLAN IDs, although according to the standard, 1 to 4095 VLAN IDs are used for region configuration. VLAN IDs from 1 to 4095 are clearly displayed so that you can determine which instance each VLAN ID supported by the standard belongs to.
Unmatch VLAN Mapped	Instance mapping VLAN in Blocking status	If Ring Protocol is also used, this item displays instance mapping VLANs whose Spanning Tree Protocols are blocked because of mismatches with the VLAN mapping of Ring Protocol. A hyphen (-) is displayed if there is no mismatch.
CIST Root	Bridge ID for the CIST root bridge	—
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address for the CIST root bridge
External Root Cost	External root path cost	Path cost value from the Switch's CIST internal bridge to the CIST root bridge. "0" is displayed if the Switch is the CIST root bridge.
Root Port	Root port	Displays the port number of the CIST root port. If the CIST root port is a link aggregation port, the link aggregation port list and the channel group number are displayed. A hyphen (-) is displayed if the Switch is the CIST root bridge.
Max Age	Maximum valid time of BPDUs sent from the CIST root bridge	Displays the maximum valid time of BPDUs sent from the CIST root bridge.
Forward Delay	Time required for a status transition of the CIST root bridge port	Displays the time required for a status transition when the status transition in the CIST root bridge is triggered by the timer.
Regional Root	Bridge ID for the regional root bridge of MST instance 0 (IST)	Displays information about the regional root bridge of MST instance 0 (IST).

Item	Meaning	Displayed detailed information
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address for the regional root bridge of MST instance 0 (IST)
Internal Root Cost	Internal root path cost for MST instance 0 (IST)	Path cost value from the Switch to the regional root bridge of MST instance 0 (IST). "0" is displayed if the Switch is the regional root bridge of MST instance 0 (IST).
Remaining Hops	Number of remaining hops	0 to 40 Displays the remaining number of hops for BPDUs that the regional root bridge of MST instance 0 (IST) sends.
Bridge ID	Bridge ID for MST instance 0 (IST) of the Switch	Displays information about the bridge of MST instance 0 (IST) of the Switch.
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	The MAC address of the Switch.
Regional Bridge Status	Status of the bridge for MST instance 0 (IST) of the Switch	Root: Root bridge Designated: Designated bridge
Path Cost Method	Path cost length mode	Long: 32-bit values are used for the path cost value.
Max Age	Maximum valid time for BPDUs sent from the MST instance 0 (IST) of the Switch	Displays the maximum valid time for BPDUs sent from the MST instance 0 (IST) bridge of the Switch.
Hello Time	Sending interval of BPDUs for MST instance 0 (IST) of the Switch	Displays the sending interval of BPDUs that are regularly sent from the MST instance 0 (IST) bridge of the Switch.
Forward Delay	Time required for a status transition of the MST instance 0 (IST) port on the Switch	Displays the time required for a status transition when the status transition in the bridge of MST instance 0 (IST) on the Switch is triggered by the timer.
Max Hops	Maximum number of hops in MST instance 0 (IST) of the Switch	2 to 40 This item displays the maximum number of hops for BPDUs sent from the MST instance 0 (IST) bridge of the Switch.
MST Instance	MST instance ID	Displays the MST instance ID and information about the instance.
Time Since Topology Change	Time since a topology change was detected	hh:mm:ss (when the elapsed time is less than 24 hours) ddd.hh:mm:ss (when the elapsed time exceeds 24 hours) Over 1000 days (when the elapsed time is more than 1000 days)
VLAN Mapped	Instance mapping VLAN	Lists the VLANs allocated to the MST instance. A hyphen (-) is displayed if no VLANs are allocated.

Item	Meaning	Displayed detailed information
Unmatch VLAN Mapped	Instance mapping VLAN in Blocking status	If Ring Protocol is also used, this item displays instance mapping VLANs whose Spanning Tree Protocols are blocked because of mismatches with the VLAN mapping of Ring Protocol. A hyphen (-) is displayed if there is no mismatch.
Regional Root	Bridge ID for the regional root bridge of the MST instance	Displays information about the regional root bridge of the MST instance.
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address for the regional root bridge of the MST instance
Internal Root Cost	Internal root path cost for the MST instance	Path cost value from the Switch to the regional root bridge of MST instance. "0" is displayed if the Switch is the regional root bridge of the MST instance.
Root Port	Root port of the MST instance	Displays the port number of the root port of the MST instance. If the root port of the MST instance is a link aggregation port, the link aggregation port list and the channel group number are displayed. A hyphen (-) is displayed if the Switch is the regional root bridge of the MST instance.
Remaining Hops	Number of remaining hops	0 to 40 Displays the remaining number of hops for BPDUs that the regional root bridge of the MST instance sends.
Bridge ID	Bridge ID for the MST instance of the Switch	Displays information about the bridge of the MST instance of the Switch.
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	The MAC address of the Switch.
Regional Bridge Status	Status of the bridge of the MST instance of the Switch	Root: Root bridge Designated: Designated bridge
Max Age	Maximum valid time of BPDUs sent from the MST instance of the Switch	Displays the maximum valid time of BPDUs sent from the MST instance bridge of the Switch.
Hello Time	Sending interval of BPDUs for MST instance of the Switch	Displays the sending interval of BPDUs that are regularly sent from the MST instance bridge of the Switch.
Forward Delay	Time required for a status transition of the MST instance port on the Switch	Displays the time required for a status transition when the status transition in the bridge of the MST instance on the Switch is triggered by the timer.
Max Hops	Maximum number of hops in the MST instance of the Switch	2 to 40 Displays the maximum number of hops for BPDUs sent from the MST instance bridge of the Switch.

Item	Meaning	Displayed detailed information
Port Information	Information about the ports of the MST instance	Displays information about the ports managed by Multiple Spanning Tree. If no VLANs are allocated to the MST instance, a response message is displayed because there are no ports.
<switch no.>/<nif no.>/<port no.>	Port number or channel group number	The port number or channel group number of the port for which information is displayed
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
Boundary	Boundary port	Indicates that the port is the boundary port for the region. If the role of the port of the partner device is an alternate port or backup port, the boundary port might never receive BPDUs. In such cases, the port is not displayed as the boundary port.
Compatible	Compatible mode	Indicates that the port is running in compatible mode for an MSTP Spanning Tree Protocol. Ports that are running in compatible mode do not perform rapid status transitions.
Status	Port status	Discarding: Discarding status Learning: Learning status Forwarding: Forwarding status Disabled: Disabled status This item shows Disabled if the port is in Down status.
Role	The role of the port	Root: Root port Designated: Designated port Alternate: Alternate port Backup: Backup port Master: Master port If the port is in Down status, a hyphen (-) is displayed because ports in this status are not included in the topology calculations.
Priority	Port priority	Displays the value of the port priority setting for the MST instance of the Switch. If the port is in Down status, a hyphen (-) is displayed.
Cost	Port cost	Displays the value of the port cost setting for the MST instance of the Switch. If the port is in Down status, a hyphen (-) is displayed.
Link Type	Link type of the line	point-to-point: The line is a 1-to-1 connection. shared: The line is a shared connection. -: A hyphen (-) is displayed when Mode is STP or when the port is in Down status.

Item	Meaning	Displayed detailed information
PortFast	Status of PortFast. The status of receive BPDUs is displayed enclosed in parentheses.	OFF: PortFast is not operating. ON: PortFast is operating. BPDU Guard: The BPDU guard function is being applied in PortFast. The receive status of BPDUs is displayed when this item is On or BPDU Guard. • BPDU received (when PortFast is On: The port is included in the calculations of the Spanning Tree topology, when PortFast is BPDU Guard: The port is down) • BPDU not received (the port is not included in the calculations of the Spanning Tree topology)
BpduFilter	BPDU filter	ON: The BPDU filter function is being applied. OFF: The BPDU filter function is not being used.
Hello Time	Interval for sending and receiving BPDUs on the port	For the root port, alternate port, and backup port, the value on the partner device is displayed. For the designated port, the value on the Switch is displayed.
Root Guard	Root guard function	ON: The root guard function is being applied. ON(Blocking): The root guard function is running and the port is blocked (all MSTIs for the port are blocked). OFF: The root guard function is not being used.
BPDU Parameters	Information about received BPDUs on the applicable port. The last time a BPDU was received is displayed enclosed with parentheses.	Displays information about the BPDUs received at the CIST or MST instance port. This item is not displayed if BPDUs are not received. The BPDU information whose Mode Version is STP or Rapid STP is displayed only by CIST.
Protocol Version	Protocol versions	Displays the protocol version of the received BPDUs. STP(IEEE 802.1D): Indicates that BPDUs in which the protocol version is set to STP (IEEE 802.1D) were received from neighboring devices. Rapid STP(IEEE 802.1w): Indicates that BPDUs in which the protocol version is set to RSTP (IEEE 802.1w) were received from neighboring devices. MSTP(IEEE 802.1s): Indicates that BPDUs in which the protocol version is set to MSTP (IEEE 802.1s) were received from neighboring devices.
Root	Root bridge information stored in the BPDU	If Protocol Version is MSTP, information about the CIST root bridge is displayed. This item is not displayed for MST instance 1 or later instances. If Mode Version is STP or Rapid STP, information about the root bridge is displayed.
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address for the root bridge

Item	Meaning	Displayed detailed information
External Root Cost	External root path cost	If Protocol Version is MSTP, information about the CIST root path cost is displayed. This item is not displayed for MST instance 1 or later instances. If Mode Version is STP or Rapid STP, information about the root path cost is displayed.
Regional Root	Regional root bridge information stored in the BPDU	If Protocol Version is MSTP, information about the CIST and MSTI regional root bridge is displayed. If Mode Version is STP or Rapid STP, this information is not displayed.
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address for the regional root bridge
Internal Root Cost	Internal root path cost	If Protocol Version is MSTP, the internal root path cost is displayed. If Mode Version is STP or Rapid STP, this information is not displayed.
Designated Bridge	Bridge information stored in the BPDU	—
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address
Port ID	Port information stored in the BPDU	—
Priority	Port priority	0 to 255 The lower the value, the higher the priority.
Number	Port number	0 to 892
Message Age Timer	Valid time of received BPDUs	Indicates how long received BPDUs are valid. A hyphen (-) is displayed if this period has expired. <current-time>(<time-BPDU-received>)/<maximum-time> <current-time>: The time at which the BPDU is received plus the time that has elapsed <time-BPDU-received>: The time that has already elapsed when the BPDU is received (Message Age of the received BPDU) <maximum-time>: Valid time (Max Age of the received BPDU)
Remaining Hops	Number of remaining hops	0 to 40 This item displays the number of remaining hops for the MST bridge stored in the received BPDU. A hyphen (-) is displayed if Mode Version is STP or Rapid STP.

Impact on communication

None

Notes

None

show spanning-tree statistics

Shows Spanning Tree statistics.

Syntax

```
show spanning-tree statistics [ {vlan [ <vlan id list> ] | single | mst [ instance <mst instanc
e id list> ] } [ port <port list> ] [channel-group-number <channel group list>]]
```

Input mode

User mode and administrator mode

Parameters

{vlan [<vlan id list>] | single | mst [instance <mst instance id list>]}

vlan

Displays PVST+ statistics.

<vlan id list>

Displays PVST+ Spanning Tree statistics for the VLAN IDs specified in list format.

For details about how to specify <vlan id list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

Statistics for all VLANs for which PVST+ is running are displayed.

single

Displays statistics about Single Spanning Tree.

mst

Displays statistics about Multiple Spanning Tree.

instance <mst instance id list>

Displays statistics about the Multiple Spanning Tree for the MST instance IDs specified in list format. Specifiable values for the MST instance ID are in the range from 0 to 4095.

If 0 is specified as the MST instance ID, CIST is subject to display.

Behavior when this parameter is omitted:

All MST instances are subject to display.

port <port list>

Displays Spanning Tree statistics for the specified port number. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters".

channel-group-number <channel group list>

Displays Spanning Tree statistics for the channel groups specified in list format in the specified link aggregation. For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when all parameters are omitted:

Displays statistics about Single Spanning Tree, PVST+, and Multiple Spanning Tree.

Example 1

Figure 24-7: Displaying the PVST+ Spanning Tree statistics

```
> show spanning-tree statistics vlan 10,12
Date 20XX/04/01 12:00:00 UTC
```

```
VLAN 10
Time Since Topology Change:1 day 10 hour 50 minute 20 second
Topology Change Times:130
  Port:1/0/1   Up
    TxBPDUs              :    904567  RxBPDUs        :       130
    Forward Transit Times:       120  RxDiscard BPDUs:         3
    Discard BPDUs by reason
          Timeout        :         3  Invalid        :         0
          Not Support    :         0  Other          :         0
  Port:1/0/2   Up
    TxBPDUs              :       100  RxBPDUs        :     80572
    Forward Transit Times:        10  RxDiscard BPDUs:         0
    Discard BPDUs by reason
          Timeout        :         0  Invalid        :         0
          Not Support    :         0  Other          :         0
  Port:1/0/3   Up
    TxBPDUs              :       129  RxBPDUs        :     79823
    Forward Transit Times:        10  RxDiscard BPDUs:         4
    Discard BPDUs by reason
          Timeout        :         2  Invalid        :         0
          Not Support    :         2  Other          :         0
  Port:1/0/10  Up
    TxBPDUs              :       129  RxBPDUs        :     79823
    Forward Transit Times:        10  RxDiscard BPDUs:       123
    Discard BPDUs by reason
          Timeout        :         0  Invalid        :         0
          Not Support    :         0  Other          :       123
VLAN 12
Time Since Topology Change:1 day 10 hour 50 minute 20 second
Topology Change Times:130
  Port:1/0/1   Up
    TxBPDUs              :       154  RxBPDUs        :     86231
    Forward Transit Times:        24  RxDiscard BPDUs:         2
    Discard BPDUs by reason
          Timeout        :         2  Invalid        :         0
          Not Support    :         0  Other          :         0
  Port:1/0/2   Up
    TxBPDUs              :       100  RxBPDUs        :     80572
    Forward Transit Times:        10  RxDiscard BPDUs:         0
    Discard BPDUs by reason
          Timeout        :         0  Invalid        :         0
          Not Support    :         0  Other          :         0
  Port:1/0/3   Up
    TxBPDUs              :       421  RxBPDUs        :     84956
    Forward Transit Times:        19  RxDiscard BPDUs:        10
    Discard BPDUs by reason
          Timeout        :        10  Invalid        :         0
          Not Support    :         0  Other          :         0
>
```

Figure 24-8: Displaying the Single Spanning Tree statistics

```
> show spanning-tree statistics single
Date 20XX/04/01 12:00:00 UTC
Time Since Topology Change:2 day 4 hour 25 minute 50 second
Topology Change Times:280
  Port:1/0/1   Up
    TxBPDUs              :   1865421  RxBPDUs        :       260
    Forward Transit Times:       250  RxDiscard BPDUs:        10
    Discard BPDUs by reason
          Timeout        :        10  Invalid        :         0
          Not Support    :         0  Other          :         0
  Port:1/0/2   Up
    TxBPDUs              :      1970  RxBPDUs        :    183450
    Forward Transit Times:       120  RxDiscard BPDUs:         5
    Discard BPDUs by reason
          Timeout        :         1  Invalid        :         1
          Not Support    :         3  Other          :         0
  Port:1/0/3   Up
    TxBPDUs              :   1771092  RxBPDUs        :   1745312
    Forward Transit Times:         2  RxDiscard BPDUs:         1
    Discard BPDUs by reason
          Timeout        :         1  Invalid        :         0
          Not Support    :         0  Other          :         0
  Port:1/0/10  Up
    TxBPDUs              :       129  RxBPDUs        :     79823
    Forward Transit Times:        10  RxDiscard BPDUs:       123
    Discard BPDUs by reason
```

```
          Timeout        :         0  Invalid        :         0
          Not Support    :         0  Other          :       123
>
```

Display items in Example 1

Table 24-7: Display Items for the PVST+ and Single Spanning Tree statistics

Item	Meaning	Displayed detailed information
Time Since Topology Change	Time since a topology change was detected	n day: Days n hour: Hours n minute: Minutes n second: Seconds For Rapid STP or Rapid PVST+, this item shows the time that has elapsed since the Spanning Tree Protocol started working.
Topology ChangeTimes	Number of topology changes detected	—
Port	Port number	—
ChGr	Channel group number	—
VLAN ID	VLAN ID subject to PVST+	Displayed only when vlan is specified.
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
Forward Transit Times	Number of transitions to the forwarding status	—
TxBPDUs	Number of sent BPDUs	—
RxBPDUs	Number of received BPDUs	—
RxDiscardsBPDUs	Number of BPDUs received but discarded	—
Timeout	Number of BPDUs whose valid time expired	Number of received BPDUs whose maximum valid time (which is set in the BPDUs) expired
Invalid	Number of invalid BPDUs	Number of received BPDUs whose format was invalid
Not Support	Number of unsupported BPDUs	Number of received BPDUs that had unsupported parameters
Other	Number of BPDUs discarded for another reason	Displays the number of BPDUs received but discarded if BPDU discard has been configured, when: • A BPDU filter has been set. • The root guard function is activated. • The port receives BPDUs that were sent from the applicable port.

Example 2

Figure 24-9: Displaying the Multiple Spanning Tree statistics

```
> show spanning-tree statistics mst
Date 20XX/04/01 12:00:00 UTC
MST Instance ID: 0     Topology Change Times: 280
  Port:1/0/1   Up
    TxBPDUs              :   1865421  RxBPDUs        :       260
    Forward Transit Times:       250  RxDiscard BPDUs:        10
    Discard BPDUs by reason
          Timeout        :        10  Invalid        :         0
          Not Support    :         0  Other          :         0
    Ver3Length Invalid   :         0  Exceeded Hop   :         0
  Port:1/0/2   Up
    TxBPDUs              :      1970  RxBPDUs        :    183450
    Forward Transit Times:       120  RxDiscard BPDUs:         5
    Discard BPDUs by reason
          Timeout        :         1  Invalid        :         1
          Not Support    :         3  Other          :         0
    Ver3Length Invalid   :        22  Exceeded Hop   :        21
  Port:1/0/3   Up
    TxBPDUs              :    177092  RxBPDUs        :      1742
    Forward Transit Times:         2  RxDiscard BPDUs:         0
    Discard BPDUs by reason
          Timeout        :         0  Invalid        :         0
          Not Support    :         0  Other          :         0
    Ver3Length Invalid   :        10  Exceeded Hop   :         5
  Port:1/0/4   Up
    TxBPDUs              :      1092  RxBPDUs        :      1312
    Forward Transit Times:         3  RxDiscard BPDUs:        41
    Discard BPDUs by reason
          Timeout        :         0  Invalid        :         2
          Not Support    :         0  Other          :        39
    Ver3Length Invalid   :         0  Exceeded Hop   :         0
  ChGr:8       Up
    TxBPDUs              :         2  RxBPDUs        :        15
    Forward Transit Times:         2  RxDiscard BPDUs:         5
    Discard BPDUs by reason
          Timeout        :         0  Invalid        :         0
          Not Support    :         3  Other          :         2
    Ver3Length Invalid   :         0  Exceeded Hop   :         0
MST Instance ID: 1     Topology Change Times: 290
  Port:1/0/1   Up
    TxBPDUs              :   1865421  RxBPDUs        :       260
    Forward Transit Times:       250  Discard Message:         0
    Exceeded Hop         :         0
  Port:1/0/2   Up
    TxBPDUs              :      1970  RxBPDUs        :    183450
    Forward Transit Times:       120  Discard Message:         7
    Exceeded Hop         :         1
  Port:1/0/3   Up
    TxBPDUs              :    177092  RxBPDUs        :      1742
    Forward Transit Times:         2  Discard Message:         0
    Exceeded Hop         :         5
  Port:1/0/4   Up
    TxBPDUs              :      1092  RxBPDUs        :      1312
    Forward Transit Times:         3  Discard Message:         0
    Exceeded Hop         :         0
  ChGr:8       Up
    TxBPDUs              :         2  RxBPDUs        :        15
    Forward Transit Times:         2  Discard Message:         0
    Exceeded Hop         :         0
>
```

Display items in Example 2

Table 24-8: Display Items of the Multiple Spanning Tree statistics

Item	Meaning	Displayed detailed information
MST Instance ID	Instance ID of the applicable MST instance	—

Item	Meaning	Displayed detailed information
Topology ChangeTimes	Number of topology changes detected	—
Port	Port number	—
ChGr	Channel group number	—
Up	The port is in Up status.	Indicates that the port is in Up status. This indicates that the channel group in link aggregation is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. This indicates that the channel group in link aggregation is in Down status.
TxBPDUs	Number of sent BPDUs	—
RxBPDUs	Number of received BPDUs	—
Forward Transit Times	Number of transitions to the forwarding status	—
RxDiscardsFrames	Number of BPDUs received but discarded	— (Displayed only for MST Instance ID: 0)
Discard BPDUs by reason	Number of BPDUs received but discarded	— (Displayed only for MST Instance ID: 0)
Timeout	Number of BPDUs whose valid time expired	Displays the number of received BPDUs whose maximum valid time (which is set in the BPDUs) expired. (Displayed only for MST Instance ID: 0)
Invalid	Number of invalid BPDUs	Displays the number of received BPDUs whose format is invalid (Displayed only for MST Instance ID: 0). When the length of the configured BPDU is less than 35 octets When the length of the TCN BPDU is less than 4 octets When the length of the RST BPDU is less than 36 octets When the length of the MST BPDU is less than 35 octets When the Version 3 Length value of the MST BPDU is less than 64
Not Support	Number of unsupported BPDUs	Displays the number of received BPDUs that have unsupported parameters (Displayed only for MST Instance ID: 0). When the BPDU type value is other than 0x00, 0x02, or 0x80
Other	Number of BPDUs discarded for another reason	Displays the number of BPDUs received but discarded if PVST+ BPDUs are received or if BPDU discard has been configured, when: • BPDU filtering has been configured. • The root guard function is activated. (Displayed only for MST Instance ID: 0) • The port receives BPDUs that were sent from the applicable port.

Item	Meaning	Displayed detailed information
Discard Message	MSTI configuration message when the received BPDUs are discarded	Displays the number of MSTI configuration messages when BPDU discard has set by the following function: • When the root guard function is set (Displayed only for MST instance IDs 1 to 4095.)
Ver3Length Invalid	Number of received BPDUs whose Version 3 Length value is invalid	Displays the number of received BPDUs whose Version 3 Length value is invalid. • When the value is less than 64 • When the value is 1089 or more • When the value is not a multiple of 16 (Displayed only for MST Instance ID: 0)
Exceeded Hop	Number of discarded MST configuration messages whose remaining hop value is 0	—

Impact on communication

None

Notes

None

clear spanning-tree statistics

Clears Spanning Tree statistics.

Syntax

```
clear spanning-tree statistics [ {vlan [ <vlan id list> ] | single | mst [ instance <mst instan
ce id list> ] } [ port <port list> ] [channel-group-number <channel group list>]]
```

Input mode

User mode and administrator mode

Parameters

{vlan [<vlan id list>] | single | mst [instance <mst instance id list>]}

vlan

Clears PVST+ statistics.

<vlan id list>

Specifies a list of VLAN IDs for which you want to clear PVST+ Spanning Tree statistics.

For details about how to specify <vlan id list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

Statistics for all VLANs for which PVST+ is running are cleared.

single

Clears statistics about Single Spanning Tree.

mst

Clears statistics about Multiple Spanning Tree.

instance <mst instance id list>

Clears statistics about the Multiple Spanning Tree for the MST instance IDs specified in list format. Specifiable values for the MST instance ID are in the range from 0 to 4095.

If an MST instance ID of 0 is specified, the CIST statistics are also cleared.

Behavior when this parameter is omitted:

All MST instances are subject to clearance.

port <port list>

Clears Spanning Tree statistics for the port numbers specified in list format. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters".

channel-group-number <channel group list>

Clears Spanning Tree statistics for the channel groups specified in list format in the specified link aggregation. For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when all parameters are omitted:

Statistics about all Spanning Tree Protocols are cleared.

Example

Figure 24-10: Clearing all the Spanning Tree statistics

```
> clear spanning-tree statistics
>
```

Figure 24-11: Clearing the Single Spanning Tree statistics

```
> clear spanning-tree statistics single
>
```

Figure 24-12: Clearing the Multiple Spanning Tree statistics

```
>clear spanning-tree statistics mst
>
```

Display items

None

Impact on communication

None

Notes

- Even if statistics are cleared, the value for the MIB information obtained by using SNMP is not cleared.
  To clear MIB information, use the "restart spanning-tree" command.
- If the configuration is deleted or added, the target statistics are cleared to zero.

clear spanning-tree detected-protocol

Forces recovery of STP compatible mode for Spanning Tree Protocols.

Syntax

```
clear spanning-tree detected-protocol [ { vlan [ <vlan id list> ] | single | mst } ] [ port <po
rt list> ] [ channel-group-number <channel group list> ]
```

Input mode

User mode and administrator mode

Parameters

{ vlan [<vlan id list>] | single | mst }

vlan

Forces recovery of STP-compatible mode for PVST+.

<vlan id list>

Forces recovery of STP-compatible mode for PVST+ for the VLAN IDs specified in list format.

For details about how to specify <vlan id list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

All VLANs for which PVST+ is running are subject to a forced recovery of STP-compatible mode.

single

Forces recovery of STP-compatible mode for Single Spanning Tree.

mst

Forces recovery of STP-compatible mode for Multiple Spanning Tree.

port <port list>

Forces recovery of STP-compatible mode for the specified port number.

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

channel-group-number <channel group list>

Forces recovery of STP-compatible mode for the channel groups specified in list format in the specified link aggregation.

For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when all parameters are omitted:

STP-compatible mode is forcibly recovered for the ports of all Spanning Tree Protocols.

Example

The following figure shows an example of forcing recovery of STP-compatible mode for Spanning Tree Protocols.

Figure 24-13: Forcibly recovering the STP-compatible mode for Spanning Tree Protocols

```
> clear spanning-tree detected-protocol
>
```

Display items

None

Impact on communication

None

Notes

This command is valid only for Rapid PVST+, rapid Spanning Tree Protocols, and Multiple Spanning Tree.

show spanning-tree port-count

Displays the numbers handled by Spanning Tree Protocols.

Syntax

```
show spanning-tree port-count [ {vlan | single | mst} ]
```

Input mode

User mode and administrator mode

Parameters

{vlan | single | mst}

vlan

Displays the number of VLANs handled by PVST+.

single

Displays the number of VLANs handled by Single Spanning Tree.

mst

Displays the number of VLANs handled by Multiple Spanning Tree.

Behavior when this parameter is omitted:

The numbers of VLANs and ports handled by PVST+, Single Spanning Tree, and Multiple Spanning Tree are displayed.

Example 1

The following shows an example of displaying the number of VLANs handled by PVST+.

Figure 24-14: Displaying the number of VLANs handled by PVST+

```
> show spanning-tree port-count vlan
Date 20XX/04/14 12:00:00 UTC
PVST+    VLAN Counts:    5     VLAN Port Counts:      20     Tree Counts:    7
>
```

Display items in Example 1

Table 24-9: Display items for the number of VLANs handled by PVST+

Item	Meaning	Displayed detailed information
PVST+ VLAN Counts	Number of VLANs	Number of VLANs for which PVST+ is running
VLAN Port Counts	Number of VLAN ports	Total number of ports configured for all VLANs for which PVST+ is running
Tree Counts	Number of PVST+ Spanning Tree Protocols	Number of PVST+ target VLANs

Example 2

The following figure shows an example of displaying the number of VLANs handled by Single Spanning Tree.

Figure 24-15: Displaying the number of VLANs handled by Single Spanning Tree

```
> show spanning-tree port-count single
Date 20XX/01/26 12:00:00 UTC
Single   VLAN Counts:   16     VLAN Port Counts:      64
>
```

Display items in Example 2

Table 24-10: Display items for the number of VLANs handled by Single Spanning Tree

Item	Meaning	Displayed detailed information
Single VLAN Counts	Number of VLANs	Number of VLANs for which Single Spanning Tree is running
VLAN Port Counts	Number of VLAN ports	Total number of ports configured for all VLANs for which Single Spanning Tree is running

Example 3

The following figure shows an example of displaying the number of VLANs handled by Multiple Spanning Tree.

Figure 24-16: Displaying the number of VLANs handled by Multiple Spanning Tree

```
> show spanning-tree port-count mst
Date 20XX/01/26 12:00:00 UTC
CIST     VLAN Counts: 4073     VLAN Port Counts:      48
MST    1 VLAN Counts:    4     VLAN Port Counts:      12
MST  128 VLAN Counts:   10     VLAN Port Counts:      80
MST 1024 VLAN Counts:    8     VLAN Port Counts:      32
>
```

Display items in Example 3

Table 24-11: Display items for the number of VLANs handled by Multiple Spanning Tree

Item	Meaning	Displayed detailed information
CIST VLAN Counts	Number of VLANs	Number of CIST instance VLANs
MST VLAN Counts	Number of VLANs	Number of MSTI instance VLANs
VLAN Port Counts	Number of VLAN ports	Total number of ports configured for the applicable instance VLANs among existing VLANs

Impact on communication

None

Notes

- The number of VLANs handled by PVST+ and Single Spanning Tree does not include the number of VLANs in suspend state. The total number of VLANs, including those in suspend state, handled by PVST+ Spanning Tree Protocol, is displayed under Tree Counts.
- The number of VLAN ports for the PVST+, Single Spanning Tree, and Multiple Spanning Tree does not include the following VLANs or ports:
  - VLANs for which the suspend parameter is set by the "state" configuration command
  - Ports for which VLAN tunneling is set
  - Ports for which the BPDU filter function is not set when the BPDU guard function is used.

- Access ports for which the PortFast function and BPDU filter function are set

restart spanning-tree

Restarts the Spanning Tree program.

Syntax

```
restart spanning-tree [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the Spanning Tree program without outputting any restart confirmation messages.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file when the program is restarted.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

After a restart confirmation message is output, the Spanning Tree program is restarted.

Example

Figure 24-17: Example of restarting the Spanning Tree Protocols

```
> restart spanning-tree
Spanning Tree restart OK? (y/n): y
>
```

Display items

None

Impact on communication

All VLANs become unable to send or receive data temporarily.

Notes

- The storage directory and the name of the core file are as follows:

  Storage directory: /usr/var/core/

  Core file: stpd.core

  If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.
- When this command is executed, the uplink redundancy program is also restarted.

dump protocols spanning-tree

Outputs to a file detailed event trace information and control table information collected for Spanning Tree programs.

Syntax

```
dump protocols spanning-tree
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 24-18: Example of taking a Spanning Tree dump

```
> dump protocols spanning-tree
>
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of the output dump file are as follows.

Storage directory: /usr/var/stp/

Event trace information file: stpd_trace.gz

Control table information file: stpd_dump.gz

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

25 Ring Protocol

show axrp

Shows Ring Protocol information.

Syntax

```
show axrp [<ring id list>] [detail]
```

Input mode

User mode and administrator mode

Parameters

<ring id list>

Specify a list of ring IDs for which you want to display information. If you specify multiple ring IDs, you can specify a range.

[Specifying a range by using "-" or ","]

All rings defined by the range are specified. The specifiable values are from 1 to 65535.

detail

Displays detailed Ring Protocol information.

Behavior when all parameters are omitted:

All summary information about the Ring Protocol is displayed.

Example

The following figure shows an example of displaying the detailed Ring Protocol information.

Figure 25-1: Example of displaying the detailed Ring Protocol information

```
> show axrp detail
Date 20XX/12/10 12:00:00 UTC

Total Ring Counts:1

Ring ID:2
 Name:RING#2
 Oper State:enable           Mode:Transit    Attribute:-
 MAC Clear Mode:system
 Control VLAN ID:15
 Forwarding Shift Time (sec):10
 Last Forwarding:flush request receive

 VLAN Group ID:1
  VLAN ID:26-30,32
  Ring Port:1(ChGr)     Role:-            State:forwarding
  Ring Port:2(ChGr)     Role:-            State:forwarding

 VLAN Group ID:2
  VLAN ID:36-40,42
  Ring Port:1(ChGr)     Role:-            State:forwarding
  Ring Port:2(ChGr)     Role:-            State:forwarding
>
```

Display items

Table 25-1: Displayed items of the detailed Ring Protocol information

Item	Meaning	Displayed information
Total Ring Counts	Number of rings	1 to 24
Ring ID	Ring ID	1 to 65535
Name	Ring identification name	—
Oper State	Whether the ring is enabled or disabled	enable: Enabled disable: Disabled Not Operating: The Ring Protocol function is not working for a reason such as invalid configuration (if all necessary configuration entries for using the Ring Protocol function have not been set, a hyphen (-) is displayed).
Mode	Running mode	Transit: Transit node -: Running mode not set
Attribute	In a multi-ring configuration, the attribute of the Switch in a shared link non-monitoring ring	-: Node that is neither a rift-ring node nor a rift-ring-edge node
MAC Clear Mode	MAC address table clearing mode	system: Device-based clearing -: Ring port-based clearing (This item is displayed when the mode is not set or the Ring Protocol function is disabled.)
Shared Port	Shared-link port number for the transit node on the shared link	Physical port number (switch number/NIF number/port number) or channel group number (ChGr)
Control VLAN ID	Control VLAN ID	2 to 4094
Forwarding Delay Time	Timer value of the forwarding shift time for the control VLAN	1 to 65535 (seconds)
Forwarding Shift Time	Time required to change the status of the data-forwarding VLAN for a ring port to Forwarding	1 to 65535 (seconds), or infinity.
Last Forwarding	Reason of why the ring port was set for forwarding lately	flush request receive: Flash control frames were received. forwarding shift time out: The forwarding shift time expired.
VLAN Group ID	Data transfer VLAN group ID	1 to 2
VLAN ID	Data transfer VLAN ID	1 to 4094
Ring Port	Ring port number	Physical port number (switch number/NIF number/port number) or channel group number (ChGr)
Role	The role of the ring port	A hyphen (-) is always displayed.
State	Ring port status	forwarding: Forwarding status blocking: Blocking status down: The port or channel group is in down status. Note: If Ring Protocol function is not enabled, or if the port is a shared port in a shared link non-monitoring ring, a hyphen (-) is displayed.

Item	Meaning	Displayed information
Multi Fault Detection State	Multi-fault monitoring is enabled	This item is displayed if the multi-fault monitoring function is enabled. "-" is displayed when the monitoring mode is set as transport.
Mode	Multi-fault monitoring mode	transport: transport-only (This item is displayed if the multi-fault monitoring function is enabled. "-" is displayed when the monitoring mode is not set.)
Control VLAN ID	ID of the VLAN used for multi-fault monitoring	2 to 4094 (This item is displayed if the multi-fault monitoring function is enabled. "-" is displayed when this item is not set.)

Impact on communication

None

Notes

None

restart axrp

Restarts a Ring Protocol program.

Syntax

```
restart axrp [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the Ring Protocol program without outputting any restart confirmation messages.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file when the program is restarted.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

After a restart confirmation message is output, the Ring Protocol program is restarted.

Example

Figure 25-2: Example of restarting the Ring Protocol program

```
> restart axrp
axrp program restart OK? (y/n):y
>
```

Figure 25-3: Example of restarting the Ring Protocol program (when the -f parameter is specified)

```
> restart axrp -f
>
```

Display items

None

Impact on communication

The VLANs that belong to the VLAN group for the Ring Protocol become unable to receive frames.

Notes

The storage directory and the name of the core file are as follows:

Storage directory: /usr/var/core/

Core file: axrpd.core

If the file has already been output, the existing file is unconditionally overwritten. If the existing file is necessary, back it up before executing the command.

dump protocols axrp

Outputs to a file detailed event trace information and control table information collected by the Ring Protocol program.

Syntax

```
dump protocols axrp
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure shows an example of taking a Ring Protocol dump.

Figure 25-4: Example of taking a Ring Protocol dump

```
> dump protocols axrp
>
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of the output dump file are as follows.

Storage directory: /usr/var/axrp/

File name: axrp_dump.gz

If the file has already been output, the existing file is unconditionally overwritten. If the existing file is necessary, back it up before executing the command.

26 IGMP/MLD snooping

show igmp-snooping

Shows IGMP snooping information. The following information is displayed for each VLAN:

- Whether the querier function is set, the IGMP querier address, and multicast router ports
- Subscription multicast group information for each VLAN or port, and learned MAC addresses
- Statistics (number of IGMP packets sent and received)
- Information on multicast routers detected by multicast router port auto-learning
- Statistics collected through multicast router port auto-learning

Syntax

```
show igmp-snooping [ <vlan id list> ]
show igmp-snooping { group [<ip address>] [<vlan id list>] | port <port list>
                     | channel-group-number <channel group list> }
show igmp-snooping statistics [<vlan id list>]
show igmp-snooping mrouter [<vlan id list>]
show igmp-snooping mrouter statistics [<vlan id list>]
```

Input mode

User mode and administrator mode

Parameters

<vlan id list>

Specifies a list of VLAN IDs for which you want to display IGMP snooping information.

For details about how to specify <vlan id list>, see "Specifiable values for parameters". Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

Behavior when this parameter is omitted:

IGMP snooping information for all VLANs is displayed.

{ group [<ip address>] [<vlan id list>] | port <port list> | channel-group-number <channel group list> }

group

Displays the subscription multicast group addresses for the VLANs.

<ip address>

Specifies the multicast group address for which you want to display IGMP snooping information.

port <port list>

Displays the subscription multicast group addresses for the specified ports. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters".

channel-group-number <channel group list>

Displays the subscription multicast group addresses for the specified channel groups. For details about how to specify <channel group list> and the specifiable range of values, see "Specifiable values for parameters".

statistics

Shows statistics.

mrouter

Displays multicast router information.

mrouter statistics

Displays statistics collected through multicast router port auto-learning.

Example 1

Figure 26-1: Displaying the IGMP snooping information

```
> show igmp-snooping
Date 20XX/04/10 15:20:00 UTC
VLAN counts: 2
VLAN: 100
  IP address: 192.168.11.20      Querier: enable
  Query interval: 150
  IGMP querying system: 192.168.11.20
  Querier version: V3
  Fast-leave: On
  Port(5): 1/0/1-5
  Mrouter-port: 1/0/1,3
  Group counts: 3
VLAN: 200
  IP address:      Querier: disable
  Query interval: 150
  IGMP querying system:
  Querier version: V2
  Fast-leave: Off
  Port(4): 1/0/6-9
  Mrouter-port: 1/0/6
  Group counts: 0
>
```

Display items in Example 1

Table 26-1: Items displayed for the IGMP snooping information

Item	Meaning	Displayed detailed information
VLAN counts	Number of VLANs on which IGMP snooping is enabled	—
VLAN	VLAN information	—
IP address	IP address used by the querier function	Blank: No IP address has been set.
Querier	Whether the querier function has been set	enable: The function has been set. disable: The function has not been set.
Query interval	Sending interval for Query messages (seconds)	Displays the interval value in operation. However, "-" is displayed when IGMPv2 is used and a device other than this device is working as a representative querier.
IGMP querying system	IGMP querier in the VLAN	Blank: There is no IGMP querier.
Querier version	IGMP version of the querier	V2: Version 2 V3: Version 3
Fast-leave	Whether IGMP instant leave has been set for the VLAN	On: The function has been set. Off: Not set.
Port(n)	Number of ports in the VLAN	n: Number of applicable ports

Item	Meaning	Displayed detailed information
Mrouter-port	Multicast router ports	—
Group counts	Number of multicast groups in the VLAN	—

Example 2

Figure 26-2: Displaying the IGMP group information for each VLAN

```
> show igmp-snooping group
Date 20XX/01/15 15:20:00 UTC
Total Groups: 5
VLAN counts: 2
VLAN: 100  Group counts: 3
  Group Address     MAC Address         Version      Mode
  224.10.10.10      0100.5e0a.0a0a      V2           -
    Port-list:1/0/1-3
  225.10.10.10      0100.5e0a.0a0a      V3           INCLUDE
    Port-list:1/0/1-2
  239.192.1.1       0100.5e40.0101      V2,V3        EXCLUDE
    Port-list:1/0/1
VLAN: 300  Group counts: 2
  Group Address     MAC Address         Version      Mode
  239.168.10.5      0100.5e28.0a05      V2           -
    Port-list:1/0/4,6
  239.192.20.6      0100.5e40.1406      V2           -
    Port-list:1/0/2-4
>
```

Display items in Example 2

Table 26-2: Items displayed for the IGMP group information for each VLAN

Item	Meaning	Displayed detailed information
Total Groups	Number of participating groups on the device	This item is displayed when <ip address> and <vlan id list> are not specified in the "show igmp-snooping group" command.
VLAN counts	Number of VLANs on which IGMP snooping is enabled	—
VLAN	VLAN information	—
Group counts	Number of subscription multicast groups in the VLAN	—
Group Address	Subscription group addresses	—
MAC Address	Learned MAC addresses	—
Version	IGMP version information	V1: IGMP Version 1 V2: IGMP Version 2 V3: IGMP Version 3 Blank: Nothing is displayed if a Report message has not been received after an IGMP General Query message is forwarded or sent. The displayed information is refreshed when an IGMP General Query message is sent or received, and when an IGMP Report message (subscription request) is received.

Item	Meaning	Displayed detailed information
Mode	Group mode	INCLUDE: INCLUDE mode EXCLUDE: EXCLUDE mode Blank: Nothing is displayed if a Report message has not been received after an IGMP General Query message is forwarded or sent. If the IGMP version information does not include V3, "-" is displayed. The displayed information is refreshed when an IGMP General Query message is sent or received, and when an IGMP Report message (subscription request) is received.
Port-list	Relay port number (Switch number/NIF number/port number)	—

Example 3

Figure 26-3: Displaying the IGMP group information for each port

```
> show igmp-snooping port 1/0/1
Date 20XX/05/15 15:20:00 UTC
Port  1/0/1  VLAN counts: 2
  VLAN: 100  Group counts: 2
    Group Address     Last Reporter      Uptime     Expires
    224.10.10.10      192.168.1.3        00:10      04:10
    239.192.1.1       192.168.1.3        02:10      03:00
  VLAN: 150  Group counts: 1
    Group Address     Last Reporter      Uptime     Expires
    239.10.120.1      192.168.15.10      01:10      02:30
>
```

Display items in Example 3

Table 26-3: Items displayed for the IGMP group information for each port

Item	Meaning	Displayed detailed information
Port	Applicable port in the VLAN	—
VLAN counts	Number of VLANs to which the specified port belongs	—
VLAN	VLAN information	—
Group counts	Number of subscription multicast groups for the specified port	—
Group Address	Subscription multicast group addresses	—
Last Reporter	IP address that last subscribed to the group	—
Uptime	Time elapsed since the group information was generated	xx:yy: xx (minutes), yy (seconds) "1hour", "2hours", ... are displayed if the time is 60 minutes or more. However, "1day", "2days", ... are displayed if the time is 24 hours or more.
Expires	Group information aging (remaining time)	xx:yy: xx (minutes), yy (seconds)

Example 4

Figure 26-4: Displaying the IGMP snooping statistics

```
> show igmp-snooping statistics
```

```
Date 20XX/01/26 15:20:00 UTC
VLAN: 100
Port 1/0/1  Rx:  Query(V2)           14353     Tx:  Query(V2)       0
                 Query(V3)              71          Query(V3)      29
                 Report(V1)             15
                 Report(V2)            271
                 Report(V3)             36
                 Leave                 137
                 Error                  14
Port 1/0/2  Rx:  Query(V2)              0     Tx:  Query(V2)      31
                 Query(V3)             12          Query(V3)      42
                 Report(V1)             0
                 Report(V2)            78
                 Report(V3)            24
                 Leave                 28
                 Error                  0
>
```

Display items in Example 4

Table 26-4: Items displayed for the IGMP snooping statistics

Item	Meaning	Displayed detailed information
VLAN	VLAN information	—
Port	Applicable port in the VLAN	This item is displayed on an Ethernet interface basis even if the port belongs to a channel group.
Rx	Number of received IGMP packets	The number of packets is counted on all Ethernet interfaces that belong to a channel group.
Query(V2)	IGMP Version 2 Query message	—
Query(V3)	IGMP Version 3 Query message	—
Tx	Number of sent IGMP packets.	The number of packets is counted on all Ethernet interfaces that belong to a channel group.
Report(V1)	IGMP Version 1 Report message	—
Report(V2)	IGMP Version 2 Report message	—
Report(V3)	IGMP Version 3 Report message	—
Leave	Leave message	—
Error	Error packet	—

Example 5

Figure 26-5: Displaying multicast router information

```
> show igmp-snooping mrouter
Date 20XX/12/13 10:05:36 UTC
Total entry: 16
VLAN ID: 101
  Port     IP address       Type  Expires
  1/0/1    192.168.101.200  PIM   01:27
  ChGr:10  192.168.101.201  IGMP  03:16
VLAN ID: 102
  Port     IP address       Type  Expires
  1/0/10   192.168.102.200  PIM   01:22
  ChGr:20  192.168.102.201  IGMP  02:11
>
```

Display items in Example 5

Table 26-5: Items displayed for the multicast router information

Item	Meaning	Displayed detailed information
Total entry	Total number of items of information on detected multicast routers	—
VLAN ID	VLAN for which multicast router port auto-learning is configured	—
Port	Port number of a port, or channel group number of a channel group, that received monitored packets	Port number ChGr: Channel group number
IP address	IP address of the detected multicast router	—
Type	Detection method	IGMP: Detected through monitoring packet IGMP (IGMP Query message) PIM: Detected through monitoring packet PIM (PIM hello message)
Expires	Remaining time for which the entry is retained	xx:yy: xx (minutes), yy (seconds) "1hour", "2hours", ... are displayed if the time is 60 minutes or more. "1day", "2days", ... are displayed if the time is 24 hours or more. However, "infinity" is displayed for detected entries with the retention time (Holdtime) of 65535 through PIM (PIM Hello message).

Example 6

Figure 26-6: Displaying statistics collected through multicast router port auto-learning

```
> show igmp-snooping mrouter statistics
Date 20XX/12/13 10:05:36 UTC
VLAN ID: 101
  Port            IGMP         PIM     Expired    Overflow
  ChGr:10            3          11           0           0
VLAN ID: 102
  Port            IGMP         PIM     Expired    Overflow
  1/0/10             6          22           0           0
>
```

Display items in Example 6

Table 26-6: Items displayed for statistics collected through multicast router port auto-learning

Item	Meaning	Displayed detailed information
VLAN ID	VLAN for which multicast router port auto-learning is configured	—
Port	Port number of a port, or channel group number of a channel group, that received monitored packets	Port number ChGr: Channel group number
IGMP	Number of items of information on multicast routers detected through monitoring packet IGMP (IGMP Query message)	—
PIM	Number of items of information on multicast routers detected through monitoring packet PIM (PIM hello message)	—

Item	Meaning	Displayed detailed information
Expired	Number of items of information on multicast routers discarded due to the expiration of the retention time	Total value of IGMP and PIM items
Overflow	Number of items of information on multicast routers discarded because the capacity limit was exceeded	Total value of IGMP and PIM items

Impact on communication

None

Notes

None

clear igmp-snooping

Clears IGMP snooping information.

Syntax

```
clear igmp-snooping { all | group [ <vlan id list> ]
                    | statistics [ <vlan id list> ]
                    | mrouter [ <vlan id list> ]
                    | mrouter statistics [ <vlan id list> ]
                    } [ -f ]
```

Input mode

User mode and administrator mode

Parameters

all

Clears all information.

group

Clears the learned MAC address information (group information).

<vlan id list>

Specify a list of VLAN IDs for which you want to clear IGMP snooping information.

For details about how to specify <vlan id list>, see "Specifiable values for parameters". Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

Behavior when this parameter is omitted:

IGMP snooping information for all VLANs is cleared.

statistics

Clears the statistics.

mrouter

Clears multicast router information.

mrouter statistics

Clears statistics collected through multicast router port auto-learning.

-f

Clears statistics without displaying a clear confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example

None

Display items

None

Impact on communication

Note that when the "clear igmp-snooping all", "clear igmp-snooping group", or "clear igmp-snooping mrouter" command is executed, multicast communication temporarily stops.

Notes

None

show mld-snooping

Shows MLD snooping information. The following information is displayed for each VLAN:

- Whether the querier function is set, the MLD querier address, and multicast router ports
- Subscription multicast group information for each VLAN or port, and learned MAC addresses
- Statistics (number of MLD packets sent and received)

Syntax

```
show mld-snooping [ <vlan id list> ]
show mld-snooping { group [<ipv6 address>] [<vlan id list>] | port <port list>
                  | channel-group-number <channel group list> }
show mld-snooping statistics [<vlan id list>]
```

Input mode

User mode and administrator mode

Parameters

<vlan id list>

Specifies a list of VLAN IDs for which you want to display MLD snooping information.

For details about how to specify <vlan id list>, see "Specifiable values for parameters". Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

Behavior when this parameter is omitted:

MLD snooping information for all VLANs is displayed.

{ group [<ipv6 address>] [<vlan id list>] | port <port list> | channel-group-number <channel group list> }

group

Displays the subscription multicast group addresses for the VLANs.

<ipv6 address>

Specifies the multicast group address for which you want to display MLD snooping information.

port <port list>

Displays the subscription multicast group addresses for the specified ports. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters". However, the <switch no.> parameter cannot be specified.

channel-group-number <channel group list>

Displays the subscription multicast group addresses for the specified channel groups. For details about how to specify <channel group list> and the specifiable range of values, see "Specifiable values for parameters".

statistics

Shows statistics.

Example 1

Figure 26-7: Displaying the MLD snooping information

```
> show mld-snooping
Date 20XX/04/10 15:20:00 UTC
VLAN counts: 2
```

```
VLAN: 100
  IP address: fe80::b1  Querier: enable
  MLD querying system: fe80::b1
  Querier version: V2
  Port(5):  0/1-5
  Mrouter-port: 0/1,0/3
  Group counts: 3
VLAN: 200
  IP address:      Querier: disable
  MLD querying system:
  Querier version: V1
  Port(4): 0/6-9
  Mrouter-port: 0/6
  Group counts: 0
>
```

Display items in Example 1

Table 26-7: Items displayed for the MLD snooping information

Item	Meaning	Displayed detailed information
VLAN counts	Number of VLANs on which MLD snooping is enabled	—
VLAN	VLAN information	—
IP address	IP address used by the querier function	Blank: No IP address has been set.
Querier	Whether the querier function has been set	enable: The function has been set. disable: The function has not been set.
MLD querying system	MLD querier in the VLAN	Blank: There is no MLD querier.
Querier version	MLD version of the querier	V1: Version1 V2: Version2
Port(n)	Number of ports in the VLAN	n: Number of applicable ports
Mrouter-port	Multicast router ports	—
Group counts	Number of subscription multicast groups in the applicable VLAN	—

Example 2

Figure 26-8: Displaying the MLD group information for each VLAN

```
> show mld-snooping group
Date 20XX/01/15 15:20:00 UTC
Total Groups: 3
VLAN counts: 2
VLAN: 100  Group counts: 2
  Group Address     MAC Address         Version      Mode
  ff35::1           3333:0000:0001      V1           -
    Port-list:0/1-3
  ff35::2           3333:0000:0002      V2           EXCLUDE
    Port-list:0/1-2
VLAN: 300  Group counts: 1
  Group Address     MAC Address         Version      Mode
  ff35::3           3333:0000:0003      -            -
    Port-list:0/4,0/6
>
```

Display items in Example 2

Table 26-8: Items displayed for the MLD group information for each VLAN

Item	Meaning	Displayed detailed information
Total Groups	Number of participating groups on the device	This item is displayed when <ipv6 address> and<vlan id list> are not specified in the "show mld-snooping group" command.
VLAN counts	Number of VLANs on which MLD snooping is enabled	—
VLAN	VLAN information	—
Group counts	Number of subscription multicast groups in the VLAN	—
Group Address	Subscription group addresses	—
MAC Address	Learned MAC addresses	—
Version	MLD version information	V1: MLD Version 1 V2: MLD Version 2 Blank: Nothing is displayed if a Report message has not been received after an MLD General Query message is forwarded or sent. The displayed information is refreshed when an MLD General Query message is sent or received, and when an MLD Report message (subscription request) is received.
Mode	Group mode	INCLUDE: INCLUDE mode EXCLUDE: EXCLUDE mode Blank: Nothing is displayed if a Report message has not been received after an MLD General Query message is forwarded or sent. If the MLD version information is V1, "-" is displayed. The displayed information is refreshed when an MLD General Query message is sent or received, and when an MLD Report message (subscription request) is received.
Port-list	Relay port number (NIF number/port number)	—

Example 3

Figure 26-9: Displaying the MLD group information for each port

```
> show mld-snooping port 0/1
Date 20XX/05/15 15:20:00 UTC
Port 0/1  VLAN counts: 1
  VLAN: 100  Group counts: 2
    Group Address     Last Reporter      Uptime     Expires
    ff35::2           fe80::b1           00:10      04:10
    ff35::3           fe80::b2           02:10      03:00
>
```

Display items in Example 3

Table 26-9: Items displayed for the MLD group information for each port

Item	Meaning	Displayed detailed information
Port	Applicable port in the VLAN	—
VLAN counts	Number of VLANs to which the specified port belongs	—
VLAN	VLAN information	—
Group counts	Number of subscription multicast groups for the specified port	—
Group Address	Subscription multicast group addresses	—
Last Reporter	IP address that last subscribed to the group	—
Uptime	Time elapsed since the group information was generated	xx:yy: xx (minutes), yy (seconds) "1hour", "2hours", ... are displayed if the time is 60 minutes or more. However, "1day", "2days", ... are displayed if the time is 24 hours or more.
Expires	Group information aging (remaining time)	xx:yy: xx (minutes), yy (seconds)

Example 4

Figure 26-10: Displaying the MLD snooping statistics

```
> show mld-snooping statistics
Date 20XX/05/15 15:20:00 UTC
VLAN: 100
Port 0/1   Rx:  Query(V1)              22     Tx:  Query(V1)     233
                Query(V2)              12          Query(V2)     123
                Report(V1)             32
                Report(V2)             15
                Done                   28
                Error                   0
Port 0/2   Rx:  Query(V1)              32     Tx:  Query(V1)     234
                Query(V2)              19          Query(V2)     115
                Report(V1)             48
                Report(V2)             26
                Done                   45
                Error                   1
```

Display items in Example 4

Table 26-10: Items displayed for the MLD snooping statistics

Item	Meaning	Displayed detailed information
VLAN	VLAN information	—
Port	Applicable port in the VLAN	This item is displayed on an Ethernet interface basis even if the port belongs to a channel group.
Rx	Number of received MLD packets	The number of packets is counted on all Ethernet interfaces that belong to a channel group.

Item	Meaning	Displayed detailed information
Tx	Number of sent MLD packets.	The number of packets is counted on all Ethernet interfaces that belong to a channel group.
Query(V1)	MLD Version 1 Query message	—
Query(V2)	MLD Version 2 Query message	—
Report(V1)	MLD Version 1 Report message	—
Report(V2)	MLD Version 2 Report message	—
Done	Done message	—
Error	Error packet	—

Impact on communication

None

Notes

None

clear mld-snooping

Clears MLD snooping information.

Syntax

```
clear mld-snooping { all | group [ <vlan id list> ] | statistics
                   [ <vlan id list> ] } [ -f ]
```

Input mode

User mode and administrator mode

Parameters

all

Clears all information.

group

Clears the learned MAC address information (group information).

<vlan id list>

Specify a list of VLAN IDs for which you want to clear MLD snooping information.

For details about how to specify <vlan id list>, see "Specifiable values for parameters". Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

Behavior when this parameter is omitted:

MLD snooping information for all VLANs is cleared.

statistics

Clears the statistics.

-f

Clears statistics without displaying a clear confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example and display items

None

Impact on communication

Note that when the "clear mld-snooping all" or "clear mld-snooping group" command is executed, multicast communication temporarily stops.

Notes

None

restart snooping

Restarts the IGMP snooping/MLD snooping program.

Syntax

```
restart snooping [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the snooping program without outputting any restart confirmation messages.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the snooping program's core file when the program is restarted.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

After a restart confirmation message is output, the snooping program is restarted.

Example

None

Display items

None

Impact on communication

After the snooping program has been restarted, multicast communication stops until multicast groups are learned again.

Notes

The storage directory and name of the core file are as follows:

Storage directory: /usr/var/core/

File name: snoopd.core

If the file has already been output, the existing file is unconditionally overwritten. If the existing file is necessary, back it up before executing the command.

dump protocols snooping

Exports the detailed event trace information and control table information for the IGMP snooping/MLD snooping program to a file.

Syntax

```
dump protocols snooping
```

Input mode

User mode and administrator mode

Parameters

None

Example

None

Impact on communication

None

Notes

The following shows the output files for the Switch and the directory to which the files are output.

Directory: /usr/var/mrp/

Dump information file: snoopd_dump.gz

Trace information file: snoopd_trace

If the file has already been output, the existing file is unconditionally overwritten. If the existing file is necessary, back it up before executing the command.

27 IPv4 Communication

show ip-dual interface

Displays the status of IPv4 and IPv6 interfaces.

Syntax

```
show ip-dual interface
show ip-dual interface summary
show ip-dual interface up
show ip-dual interface down
show ip-dual interface <interface type> <interface number>
```

Input mode

User mode and administrator mode

Parameters

summary

Displays a summary of the status of all interfaces.

up

Displays detailed information about interfaces in the UP status.

down

Displays detailed information about interfaces in the DOWN status.

<interface type> <interface number>

Displays detailed information about the applicable interface.

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below. For details, see "■How to specify an interface" in "Specifiable values for parameters".

- VLAN interface
- Loopback interface

Behavior when all parameters are omitted:

The detailed status of all interfaces is displayed.

Example 1

Displays a summary of the status of all interfaces.

```
>show ip-dual interface summary
```

Figure 27-1: Example of displaying a summary of all interfaces

```
> show ip-dual interface summary
Date 20XX/12/10 12:00:00 UTC
VLAN0002: UP  2001:db8::1:1/64
              fe80::200:87ff:fe98:a21c%VLAN0002/64
VLAN0003: UP  192.0.2.64/24
VLAN0004: UP  2001:db8::1234:1/64
>
```

Display format

```
Interface name : Status IP-address Subnet-mask
Interface name : Status IPv6-address Prefix-len
```

Display items in Example 1

Table 27-1: Information displayed for a summary of all interfaces

Item	Meaning	Displayed information
Interface name	Interface name	—
Status	Status of the interface	UP/DOWN
IP-address	IPv4 address	—
Subnet-mask	Subnet mask	—
IPv6-address	IPv6 address	—
Prefix-len	Prefix length	—

Example 2

- This example shows how to display detailed information about interfaces in the UP status.

```
> show ip-dual interface up
```

- Display the detailed status of an interface.

```
> show ip-dual interface vlan 10
```

The following shows an example of executing the command with an interface specified.

Figure 27-2: Example of executing the command with an interface specified

```
> show ip-dual interface vlan 10
Date 20XX/12/10 12:00:00 UTC
VLAN0010: flags=1063<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST>
   mtu 1500
   inet 158.214.178.30/25 broadcast 158.214.178.127
   inet6  2001:db8::1:1/64
   inet6 fe80::60:972e:1d4c%VLAN0010/64
   Switch01/NIF01/Port01: UP media 100BASE-TX full(auto) 0012.e22e.1d4c
   Switch01/NIF01/Port02: UP media ----- 0012.e22f.1d4f ChGr:5 (-)  <--------1
   Time-since-last-status-change: 30,00:10:00
   Last down at: 12/01 11:45:00            <--------------------------------2
   VLAN: 10          <-----------------------------------------------------3
```

1. The example above is displayed for a link aggregation line.
2. The reason that the interface is down is a line failure or a change in the configuration of the IP information or the line. If the configuration is changed during a line failure, the time the line failure occurred is displayed instead of the time the information was updated because the status when the configuration was changed was the Down status.
3. The VLAN ID is displayed for a VLAN.

Display items in Example 2

Table 27-2: Displayed detailed information (common display items)

Item	Meaning	Displayed information
flags	Status of the target interface, and the configuration items	—
mtu	MTU for the interface	Shows the MTU of the IP interface.
inet	IPv4 address	—

Item	Meaning	Displayed information
inet6	IPv6 address	duplicated: The address is duplicated. tentative: The address is being checked for duplication.
broadcast	Broadcast address	Displayed when the IP interface type is broadcast.
UP/DOWN	Status of the interface	UP: In operation (Normal running state) DOWN: In operation (line has failed), or not in operation
media	Line type	For details about line types, see "Table 20-2: List of line types" in the "show interfaces" command.
Time-since-last-status-change	Time elapsed since the status changed to UP or DOWN.	Time elapsed since the status of the interface last changed. The display format is hour:minute:second or number-of-days,hour:minute:second. "Over 100 days" is displayed if the number of days exceeds 100. "-----" is displayed if there has never been an UP or DOWN status.
Last down at	Time the interface went down	Time the interface last went down. The display format is month/day hour:minute:second. "-----" is displayed if the interface has never gone down.
VLAN	VLAN ID	—

Table 27-3: Displayed detailed information (Ethernet interface display items)

Item	Meaning	Displayed information
Switch<switch no.>	Switch number	—
NIF<nif no.>	NIF number	—
Port<port no.>	Port number	—
media	Line type/line speed	For details about line types, see "Table 20-2: List of line types" in the "show interfaces" command.
xxxx.xxxx.xxxx	MAC address	The MAC address used by packets sent from the interface. For a VLAN interface, a MAC address of all zeros might be displayed if the line cannot communicate.
ChGr	Channel group number. The status of the channel group is displayed enclosed in parentheses.	—

Impact on communication

None

Notes

None

show ip interface

Shows the status of IPv4 interfaces.

Syntax

```
show ip interface
show ip interface summary
show ip interface up
show ip interface down
show ip interface <interface type> <interface number>
```

Input mode

User mode and administrator mode

Parameters

summary

Displays a summary of the status of all interfaces.

up

Displays detailed information about interfaces in the UP status.

down

Displays detailed information about interfaces in the DOWN status.

<interface type> <interface number>

Displays detailed information about the applicable interface.

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below. For details, see "■How to specify an interface" in "Specifiable values for parameters".

- VLAN interface
- Loopback interface

Behavior when all parameters are omitted:

The detailed status of all interfaces is displayed.

Example 1

Displays a summary of the status of all interfaces.

```
>show ip interface summary
```

Figure 27-3: Example of displaying a summary of all interfaces

```
> show ip interface summary
Date 20XX/12/10 12:00:00 UTC
VLAN0010: UP 158.215.100.1/24
VLAN0020: UP 192.168.0.60/24
>
```

Display format

```
Interface name : Status IP-address Subnet-mask
```

Display items in Example 1

Table 27-4: Information displayed for a summary of all interfaces

Item	Meaning	Displayed information
Interface name	Interface name	—
Status	Status of the interface	UP/DOWN
IP-address	IPv4 address	—
Subnet-mask	Subnet mask	—

Example 2

- This example shows how to display detailed information about interfaces in the UP status.

```
>show ip interface up
```

- Display the detailed status of an interface.

```
> show ip interface vlan 3
```

The following shows an example of executing the command with an interface specified.

Figure 27-4: Example of executing the command with an interface specified

```
>show ip interface vlan 3
Date 20XX/12/10 12:00:00 UTC
VLAN0003: flags=1063<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST>
   mtu 1500
   inet 158.214.178.30/25 broadcast 158.214.178.127
   Switch01/NIF00/Port01: UP media 100BASE-TX full(auto) 0012.e22e.1d4c
   Switch01/NIF00/Port02: UP media ----- 0012.e22f.1d4f ChGr:5 (-)   <------1
   Time-since-last-status-change: 30,00:10:00
   Last down at: 11/10 11:45:00           <--------------------------------2
   VLAN: 3              <-------------------------------------------------3
```

1. The example above is displayed for a link aggregation line.
2. The reason that the interface is down is a line failure or a change in the configuration of the IP information or the line. If the configuration is changed during a line failure, the time the line failure occurred is displayed instead of the time the information was updated because the status when the configuration was changed was the Down status.
3. The VLAN ID is displayed for a VLAN.

Display items in Example 2

Table 27-5: Displayed detailed information (common display items)

Item	Meaning	Displayed information
flags	Status of the target interface, and the configuration items	—
mtu	MTU for the interface	Shows the MTU of the IP interface.
inet	IPv4 address	—
broadcast	Broadcast address	Displayed when the IP interface type is broadcast.
UP/DOWN	Status of the interface	UP: In operation (Normal running state) DOWN: In operation (line has failed), or not in operation

Item	Meaning	Displayed information
media	Line type	For details about line types, see <line type> in the display items of the "show interfaces" command.
Time-since-last-status-change	Time elapsed since the status changed to UP or DOWN.	Time elapsed since the status of the interface last changed. The display format is hour:minute:second or number-of-days,hour:minute:second. "Over 100 days" is displayed if the number of days exceeds 100. "-----" is displayed if there has never been an UP or DOWN status.
Last down at	Time the interface went down	Time the interface last went down. The display format is month/day hour:minute:second. "-----" is displayed if the interface has never gone down.
VLAN	VLAN ID	—

Table 27-6: Displayed detailed information (Ethernet interface display items)

Item	Meaning	Displayed information
Switch<switch no.>	Switch number	—
NIF<nif no.>	NIF number	—
Port<port no.>	Port number	—
media	Line type/line speed	For details about line types, see <line type> in the display items of the "show interfaces" command.
xxxx.xxxx.xxxx	MAC address	The MAC address used by packets sent from the interface. For a VLAN interface, a MAC address of all zeros might be displayed if the line cannot communicate.
ChGr	Channel group number. The status of the channel group is displayed enclosed in parentheses.	—

Impact on communication

None

Notes

None

show ip arp

Shows ARP information.

Syntax

```
show ip arp
show ip arp interface <interface type> <interface number>
show ip arp <ip address>
show ip arp <host>
```

Input mode

User mode and administrator mode

Parameters

interface <interface type> <interface number>

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below. For details, see "■How to specify an interface" in "Specifiable values for parameters".

- VLAN interface

<ip address>

Specifies an IP address.

<host>

Specifies the destination host name.

Behavior when all parameters are omitted:

The ARP information registered on all interfaces is displayed.

Example

Figure 27-5: Command execution result when a VLAN interface is specified

```
>show ip arp interface vlan 100
Date 20XX/07/14 12:00:00 UTC
Total: 6 entries
 IP Address       Linklayer Address  Netif            State      Type
 192.0.0.1        0012.e240.0a00     VLAN0100         PERMANENT  arpa
 192.0.0.2        0012.e240.0a01     VLAN0100         STALE      arpa
 192.0.0.3        0012.e240.0a02     VLAN0100         STALE      arpa
 192.0.1.1        0012.e240.0a10     VLAN0100         PERMANENT  arpa
 192.0.2.1        0012.e240.0a20     VLAN0100         PERMANENT  arpa
 192.0.2.2        0012.e240.0a21     VLAN0100         REACHABLE  arpa
>
```

Figure 27-6: Command execution result when all ARP information is displayed

```
>show ip arp
Date 20XX/07/14 12:00:00 UTC
Total: 12 entries
 IP Address       Linklayer Address  Netif            State      Type
 192.0.0.1        0012.e240.0a00     VLAN0100         STALE      arpa
 192.0.0.2        0012.e240.0a01     VLAN0100         STALE      arpa
 192.0.0.3        0012.e240.0a02     VLAN0100         STALE      arpa
 192.0.1.1        0012.e240.0a10     VLAN0100         PERMANENT  arpa
 192.0.2.1        0012.e240.0a20     VLAN0100         PERMANENT  arpa
 192.0.2.2        0012.e240.0a21     VLAN0100         REACHABLE  arpa
 192.0.10.1       0012.e240.0b01     VLAN0101         PERMANENT  arpa
 192.0.10.2       0012.e240.0b02     VLAN0101         STALE      arpa
```

```
 192.0.10.3       0012.e240.0b03     VLAN0101          REACHABLE  arpa
 192.0.20.1       0012.e240.0c10     VLAN0102          PREMANENT  arpa
 192.0.20.2       0012.e240.0c20     VLAN0102          STALE      arpa
 192.0.20.3       0012.e240.0c20     VLAN0102          STALE      arpa
 >
```

Figure 27-7: Command execution result when an IP address is specified

```
>show ip arp 192.0.0.1
Date 20XX/07/14 12:00:00 UTC
 IP Address       Linklayer Address  Netif             State      Type
 192.0.0.1        0012.e240.0a00     VLAN0100          PERMANENT  arpa
 >
```

Figure 27-8: Command execution result when a host name is specified

```
>show ip arp Department-3
Date 20XX/07/14 12:00:00 UTC
 IP Address       Linklayer Address  Netif             State      Type
 192.0.0.3        0012.e240.0a02     VLAN0100          STALE      arpa
 >
```

Display items

Display format of the result of executing the "show ip arp" command is as follows:

```
Total: <entry> entries
IP Address   Linklayer Address  Netif           State        Type
<IP Address> <MAC Address>      <interface name> <Entry Type> <Hardware Type>
```

Table 27-7: Items displayed for ARP information

Item	Displayed information	Displayed detailed information
Total: <entry> entries	Number of entries	Number of used ARP table entries
<IP Address>	Next hop IP address	—
<MAC Address>	MAC address of a neighboring device	• INCOMPLETE status (incomplete): Resolution of the address is incomplete. • FAILED status (deleting): Entries are being deleted. • Other status MAC address of a neighboring device learned
<interface name>	Interface name	—
<Entry Type>	Entry status	INCOMPLETE: Not resolved REACHABLE: Reachability confirmed STALE: Reachability not confirmed DELAY: Waiting for reachability check PROBE: Reachability check in progress FAILED: Waiting for deletion PERMANENT: Static entry
<Hardware Type>	Hardware type	arpa: Ethernet interface

Impact on communication

None

Notes

1. Entries that are created by learning from other devices are not displayed in the following cases:

- There has been no communication since the interface started up.
- The aging time since registration in the ARP cache table has been exceeded.

2. When an ARP entry is deleted on the Switch, it is temporarily displayed as an entry in FAILED status. An entry in FAILED status is automatically deleted as time elapses.

clear arp-cache

Clears the ARP information registered dynamically.

Syntax

```
clear arp-cache [interface <interface type> <interface number>]
```

Input mode

User mode and administrator mode

Parameters

interface <interface type> <interface number>

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below. For details, see "■How to specify an interface" in "Specifiable values for parameters".

- VLAN interface

Behavior when this parameter is omitted:

The ARP information registered on all interfaces is cleared.

Example

The following shows an example of clearing the ARP information registered on a specific VLAN interface.

Figure 27-9: Result of clearing ARP information

```
>show ip arp interface vlan 100
Date 20XX/07/14 12:00:00 UTC
Total: 6 entries
 IP Address       Linklayer Address  Netif            State     Type
 192.0.0.1        0012.e240.0a00     VLAN0100         PERMANENT arpa
 192.0.0.2        0012.e240.0a01     VLAN0100         STALE     arpa
 192.0.0.3        0012.e240.0a02     VLAN0100         STALE     arpa
 192.0.1.1        0012.e240.0a10     VLAN0100         PERMANENT arpa
 192.0.2.1        0012.e240.0a20     VLAN0100         PERMANENT arpa
 192.0.2.2        0012.e240.0a21     VLAN0100         REACHABLE arpa
>clear arp-cache interface vlan 100
Deleted arp entry
>show ip arp interface vlan 100
Date 20XX/07/14 12:00:00 UTC
Total: 3 entries
 IP Address       Linklayer Address  Netif            State      Type
 192.0.0.1        0012.e240.0a00     VLAN0100         PERMANENT  arpa
 192.0.1.1        0012.e240.0a10     VLAN0100         PERMANENT  arpa
 192.0.2.1        0012.e240.0a20     VLAN0100         PERMANENT  arpa
>
```

Display items

None

Impact on communication

Communication might stop temporarily until the ARP entry is created again.

Notes

1. An ARP entry deleted with this command will temporarily be in FAILED status, but will be automatically deleted as time elapses.

show netstat(netstat)

Shows the network status and statistics.

Syntax

```
[show] netstat [numeric] [addressfamily <address family>]
[show] netstat interface
[show] netstat statistics [addressfamily <address family>]
[show] netstat routing-table [numeric] [addressfamily <address family>]
```

Input mode

User mode and administrator mode

Parameters

numeric

Displays network addresses by their address numbers, not by their host names, and displays ports by their port numbers, not by their service names. This parameter can be used in any display format.

Behavior when this parameter is omitted:

Network addresses are displayed by host names, and ports by service names.

addressfamily <address family>

Reports address control blocks for the specified address family.

For <address family>, you can specify inet, inet6, local, or unix. The specifiable address families vary depending on the combination with other parameters.

Behavior when this parameter is omitted:

The information for all address families is displayed.

interface

Displays the status of interfaces.

statistics

Displays statistics for each protocol.

If no address family is specified, IPv4-related statistics are output.

routing-table

Displays the routing table.

If no address family is specified, the IPv4 routing table is displayed.

Behavior when all parameters are omitted:

The status of all sockets is displayed.

Example

Figure 27-10: Displaying the statistics for the show netstat statistics command

```
> show netstat
Ip:
    7010 total packets received
    0 forwarded
    0 incoming packets discarded
    7010 incoming packets delivered
    5033 requests sent out
```

```
Icmp:
    4 ICMP messages received
    4 input ICMP message failed.
    ICMP input histogram:
        destination unreachable: 4
    0 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
IcmpMsg:
    InType3: 4
Tcp:
    8 active connections openings
    24 passive connection openings
    0 failed connection attempts
    0 connection resets received
    4 connections established
    7006 segments received
    5265 segments send out
    2 segments retransmited
    0 bad segments received.
    1 resets sent
Udp:
    0 packets received
    0 packets to unknown port received.
    0 packet receive errors
    4 packets sent
        :
        :
```

Display items

Table 27-8: Information displayed for the show netstat statistics command

Item	Displayed information
Ip	IP statistics
Ip6	IPv6 statistics
Icmp	ICMP statistics
Icmp6	ICMPv6 statistics
IcmpMsg	Statistics on ICMP messages
Tcp	TCP statistics
Udp	UDP statistics
Udp6	Statistics on UDP over IPv6

Impact on communication

None

Notes

None

ping

The "ping" command is used to determine whether communication is possible to the device with the specified IP address.

Syntax

```
ping <host> [numeric] [summary] [record-route] [direct]
     [count <count>] [interval <wait>] [pad-byte <pattern>]
     [packetsize <size>] [source <source address>] [ttl <ttl>]
     [broadcast]
```

Input mode

User mode and administrator mode

Parameters

<host>

Specifies the destination host name or IP address.

numeric

Displays the IP address of the host without converting it to a name.

Behavior when this parameter is omitted:

Displays the name converted from the host IP address if an ICMP error has occurred.

summary

Restricts the output. Only the summary lines of the first and last lines are displayed.

Behavior when this parameter is omitted:

Displays one line for one response as regular display mode.

record-route

Records the route to the specified host. The RECORD_ROUTE option is assigned to the ECHO_REQUEST packet, and the route buffer on the reply packet is displayed. Note that the IP header can contain only a maximum of nine routes. Most hosts ignore or discard this option.

Behavior when this parameter is omitted:

The RECORD_ROUTE option is not used.

direct

Ignores the normal routing table and sends data to the hosts on the directly connected network. If no host exists on the specified network connected, an error is returned. This option is used to send ping to the local host via an interface that has no routing information.

Behavior when this parameter is omitted:

Uses the normal routing table to send data.

count <count>

Sends packets for the number of times specified for <count>, and then finishes the processing. To interrupt the processing, press Ctrl+C. The specifiable values are from 1 to 2147483647.

Behavior when this parameter is omitted:

Sends packets indefinitely.

interval <wait>

Sets the packet sending interval to the number of seconds specified for <wait>. The specifiable values are from 1 to 214782.

Behavior when this parameter is omitted:

The sending interval defaults to 1 second.

pad-byte <pattern>

Specifies the pad bytes for packets to be sent. The maximum size of the pad is 16 bytes. This is effective for diagnosing data-dependent problems on the network. For example, specify pad-byte ff to generate an all-ones packet to be sent. You can specify a hexadecimal number consisting of 1 to 32 digits.

Behavior when this parameter is omitted:

Generates pad characters by incrementing from 00 to ff.

packetsize <size>

Specifies how many bytes of data are to be sent. The specifiable values are from 1 to 65467.

Behavior when this parameter is omitted:

The number of bytes of data to be sent is 56. By adding 8 bytes of ICMP header data, a total of 64 bytes will be sent.

source <source address>

Uses the IP address specified for <source address> as the source address of an output packet. Only the IP addresses set on the Switch can be specified.

Behavior when this parameter is omitted:

The source IP address selected by the Switch is used.

ttl <ttl>

Sets the value specified for <ttl> to the ttl field of the IP header. The specifiable values are from 1 to 255.

Behavior when this parameter is omitted:

If a unicast address is specified for <host>, 64 is set. If a multicast address is specified, 1 is set.

broadcast

Specify this parameter if a broadcast address is specified for <host>.

Behavior when this parameter is omitted:

None

Behavior when all parameters are omitted:

Displays one line for one response as regular display mode.

Example

- This example shows how to execute an echo test by specifying the default values (unlimited attempts, data size of 56 bytes, and sending interval of 1 second).

  Figure 27-11: Example of executing the ping command with default values

```
>ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1): 56(84) data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=255 time=0.286 ms
64 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=0.271 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=0.266 ms
^C
--- 192.168.0.1 PING statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.266/0.274/0.286 /0.334ms
>
```

- This example shows how to execute an echo test by specifying 3attempts, data size of 120 bytes, and sending interval of 2 seconds.

  Figure 27-12: Example of executing the ping command by specifying 3 attempts, data size of 120 bytes, and sending interval of 2 seconds

```
>ping 192.168.0.1 count 3 packetsize 120 interval 2
```

Display items

None

Impact on communication

None

Notes

- To halt execution of the "ping" command, press Ctrl + C. If you interrupt the command with the simple parameter specified, "no response" symbols (.) corresponding to echo replies which have not been received are displayed after the command is interrupted. As a result, the number of "no response" symbols might not be exactly correct.
- If you specify a broadcast address as the destination, a warning message is output, but the command is executed.
- If a broadcast address is specified as the destination, packets that are equal to or larger than (MTU length - 27) bytes cannot be sent.

traceroute

Displays the route (the route of gateways that have been passed through and the response time between the gateways) over which UDP messages are sent to the destination host.

Syntax

```
traceroute <host> [numeric] [direct] [gateway <gateway address>...] [ttl <ttl>] [port <port>]
[probes <Count>] [source <source address>] [waittime <time>] [packetsize<size>]
```

Input mode

User mode and administrator mode

Parameters

<host>

Specifies the destination host name or host IP address of the test target (IP destination).

numeric

Displays the gateway address by the IP address alone, not by the host name and IP address.

Behavior when this parameter is omitted:

Displays the name converted from the host IP address.

direct

Directly sends the probe packet to the host on the connected network. The normal routing table is not used. If the host does not exist on the directly connected network, an error is returned. You can use this option when using an interface without routes to execute the traceroute command on the host.

Behavior when this parameter is omitted:

Uses the normal routing table to send data.

gateway <gateway address>

Specifies a source route gateway. A maximum of eight gateways can be specified.

Behavior when this parameter is omitted:

A source route gateway is not specified.

ttl <ttl>

Specify the maximum time-to-live (the maximum number of hops) for the probe packets to be sent. The specifiable values are from 2 to 255.

Behavior when this parameter is omitted:

The maximum number of hops is 30.

port <port>

Specifies the port number of the UDP packet to be used. The port number for a probe packet starts with the <port> value, and is incremented by one for each probe packet.

Behavior when this parameter is omitted:

The port number is set to 33434 (the port number for probe packets starts from 33435).

probes <Count>

Specify the number of times a search is performed for each "ttl" in <Count>. The specifiable values are from 1 to 10.

Behavior when this parameter is omitted:

A search is performed 3 times.

source <source address>

Uses the IP address of an argument (specified by number, not by host name) as the source address of the probe packet to be sent (address to be sent). For a host with multiple IP addresses, this parameter can be used to assign another source address to the probe packet. If the specified IP address is not one of the interface addresses of that host, an error is returned and not data is sent.

Behavior when this parameter is omitted:

The source IP address selected by the Switch is used.

waittime <time>

Specify the time (in seconds) to wait for a probe packet. The specifiable values are from 2 to 86400.

Behavior when this parameter is omitted:

The wait time for a response is 5 seconds.

packetsize <size>

Specify, in bytes, the data size of a probe packet. The specifiable values are from 40 to 32768.

Behavior when this parameter is omitted:

The data size is set to 60 bytes.

Behavior when all parameters are omitted:

Displays the route to the specified <host>.

Example

```
>traceroute 192.168.3.24 numeric
traceroute to 192.168.3.24 (192.168.3.24), 30 hops max, 60 byte packets
 1  192.168.2.101  0.612 ms *  0.532 ms
 2  192.168.3.24  0.905 ms  0.816 ms  0.807 ms
>
```

Display items

None

Impact on communication

None

Notes

None

show ip route

Displays the IPv4 routing table.

Syntax

```
show ip route
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 27-13: Route information stored in the routing table

```
> show ip route
Date 20XX/12/17 12:00:00 UTC
Total: 5
Destination           Nexthop           Interface   Protocol
192.168.0.0/24        192.168.0.100     VLAN0001    Connected
192.168.4.0/24        192.168.4.10      VLAN4094    Connected
192.168.5.0/24        192.168.5.10      VLAN3005    Connected
192.168.54.0/24       192.168.54.100    VLAN3254    Connected
192.168.55.0/24       192.168.55.100    VLAN3255    Connected
```

Display items

Table 27-9: Displayed route information stored in the routing table

Item	Meaning	Displayed detailed information
Total	Number of registered routes	—
Destination	Destination network (IP address)	—
Next Hop	Next hop IP address	—
Interface	Interface name	Displays VLANxxxx. xxxx: VLAN ID
Protocol	Protocol	Static: Static route Connected: Directly connected route

Impact on communication

None

Notes

None

show tcpdump (tcpdump)

Monitors incoming and outgoing packets.

This command can be used to check the communication status of incoming and outgoing Layer 3 traffic. For example, you can monitor packets, such as those sent to or from the Switch.

Syntax

<Monitoring interface packets>

```
show tcpdump interface <interface type> <interface number> [{no-resolv | no-domain}] [abs-s
eq] [no-time] [{brief | detail | extensive | debug}] [{hex | hex-ascii}] [count <count>] [s
naplen <snaplen>] [writefile <file name>] [<expression>]
```

<Displaying the packet monitoring file>

```
show tcpdump readfile <file name> [{ no-resolv | no-domain }] [abs-seq] [no-time] [{ brief
| detail | extensive | debug }] [{ hex | hex-ascii }] [count <count>] [writefile <file name
>] [<expression>]
```

#: show tcpdump can be abbreviated as tcpdump. To use tcpdump, enter the following parameters:

```
tcpdump -i <interface type> <interface number> [{-n | -N}] [-S] [-t] [-q] [-v[v[v]]] [{-x | -X}
] [-c <count>] [-s <snaplen>] [-w <file name>] [<expression>]
tcpdump -r <file name> [{-n | -N}] [-S] [-t] [-q] [-v[v[v]]] [{-x | -X}] [-c <count>] [-w <file
 name>] [<expression>]
```

Input mode

User mode and administrator mode

Parameters

interface <interface type> <interface number> (-i <interface type> <interface number>)

Specifies the type (<interface type>) and number (<interface number>) of the interface that you want to monitor.

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below. For details, see "■How to specify an interface" in "Specifiable values for parameters".

- VLAN interface
- Loopback interface

readfile <file name> (-r <file name>)

Reads a packet from <file name> (created by the writefile option).

{no-resolv | no-domain}

no-resolv (-n)

Addresses (host addresses, port numbers, or others) are not converted into names.

no-domain (-N)

The domain name of the host is not displayed. For example, server is displayed rather than server.example.com.

Behavior when this parameter is omitted:

Addresses (host addresses, port numbers, or others) are converted into names. A host address is displayed including the domain name.

abs-seq (-S)

Displays the TCP sequence number as an absolute value rather than a relative value.

Behavior when this parameter is omitted:

The TCP sequence number is displayed as a relative value.

no-time (-t)

Does not display time information on each line of a dump.

Behavior when this parameter is omitted:

Time information is displayed on each line of a dump.

{brief | detail | extensive | debug}

brief (-q)

Partially omits the display of protocol information, such as TCP or UDP, to simplify the displayed information more than usual. The Layer 2 section (address family) is also not displayed.

detail (-v)

Displays the information in a little more detail than usual.

For example, the information about the time to live, identification, total length, or options of IP packets is displayed. Furthermore, a check of the integrity of packets is also added. For example, the checksum of the IP or ICMP header is checked.

extensive (-vv)

Displays the information in more detail than the detail parameter.

For example, the extended fields of NFS response packets are displayed.

debug (-vvv)

Displays the most detailed information.

For example, the sub option of the telnet protocol is also displayed.

Behavior when this parameter is omitted:

Normal information is displayed rather than displaying the information briefly or in detail.

{hex | hex-ascii}

hex (-x)

Displays each packet in hexadecimal except for the link layer.

hex-ascii (-X)

In hexadecimal notation, ASCII characters are also displayed.

Behavior when this parameter is omitted:

Only the result of analyzing each line of a dump is displayed, without hexadecimal or ASCII.

count <count> (-c <count>)

Exits after receiving <count> packets. The specifiable values are from 1 to 2147483647.

Behavior when this parameter is omitted:

The command can be exited by pressing the Ctrl + C key.

snaplen <snaplen> (-s <snaplen>)

Retrieves <snaplen> bytes from each packet and dumps them. The specifiable values are 0 and from 4 to 65535. This value should be set at a minimum required to obtain protocol information. In the Switch, set 4 or more for <snaplen> because the Layer 2 section of a packet is treated as a 4-byte Null/Loopback header including the address family.

Packets truncated by the restriction set by <snaplen> are output in the format "[|<proto>]" (<proto> is the protocol name corresponding to the level where the truncation occurs).

When <snaplen> is specified as 0, length (65535) is used (to ensure capturing the whole packet).

Behavior when this parameter is omitted:

From each packet, 96 bytes are retrieved and dumped.

writefile <file name> (-w <file name>)

Writes monitored information to <file name> instead of analyzing or displaying packets.

The <file name> can be displayed later by using the readfile <file name> option.

Behavior when this parameter is omitted:

The result of analyzing each dump is displayed on the screen.

<expression>

Selects the type of packets to be dumped. When <expression> is specified, only the packets that match <expression> are monitored.

When the Switch receives or sends a large number of packets, specify this parameter to monitor only required packets.

The following is an example of how <expression> is specified:

Specify one basic element or a combination of multiple basic elements for <expression>.

The basic element consists of four qualifiers <protocol>, <direction>, <type>, and <identification>.

The basic element is specified by placing <type> in front of <identification> and placing <direction>, <protocol>, or <protocol> <direction> qualifiers without conflict in front of <type> and <identification>.

The pattern of the basic elements is as follows:

Pattern of the basic elements:

<type> <identification>

<direction> <type> <identification>

<protocol> <type> <identification>

<protocol> <direction> <type> <identification>

<identification>

Indicates the name or number of addresses or port numbers.

Example: 10.10.10.10, serverA, 23, telnet

<type>

Indicates the type of target for which <identification> is specified. The usable <type> is host, net, and port.

Example: host serverA, net 192.168, port 22

When the <type> qualifier is omitted depending on combination with other qualifiers, it is assumed that host is specified.

Example: src serverA represents src host serverA.

<direction>

Indicates the communication direction, such as from <identification>, to <identification>, or both ways.

Usable values are src, dst, src or dst, and src and dst.

Example: src serverA, dst net fe80::/64, src or dst port telnet

When the <direction> qualifier is not specified, it is assumed that src or dst is specified.

Example: port telnet represents src or dst port telnet.

<protocol>

This qualifier is specified to limit the use of protocols to specific protocols.

Usable protocol values are ip, ip6, tcp, and udp.

Example: ip6 src fec0::1, ip net 192.168, tcp port 23

When the <protocol> qualifier is not specified, it is assumed that all the protocols that are consistent with the <type>

qualifier are specified.

Example: port 53 represents tcp port 53 or udp port 53.

Example of the basic elements:

dst host <host>

This is true when the IPv4/IPv6 destination of packets is <host>.

src host <host>

This is true when the IPv4/IPv6 source of packets is <host>.

host <host>

This is true when the IPv4/IPv6 destination or source of packets is <host>.

IPv4 or IPv6 can be limited by adding ip or ip6 to the front of the above conditional expression indicating each host.

Example: ip host <host>

Example: ip6 src host <host>

dst net <network>/<length>

This is true when the IPv4/IPv6 destination address of packets is included in the specified <length>-bit netmask <network>.

src net <network>/<length>

This is true when the IPv4/IPv6 source address of packets is included in the specified <length>-bit netmask <network>.

net <network>/<length>

This is true when the IPv4/IPv6 destination address of packets is included in the specified <length>-bit netmask <network>.

dst port <port>

This is true when a packet is ip/tcp, ip/udp, ipv6/tcp, or ipv6/udp, if the destination port number is <port>.

src port <port>

This is true when a packet is ip/tcp, ip/udp, ipv6/tcp, or ipv6/udp, if the source port number is <port>.

port <port>

This is true when a packet is ip/tcp, ip/udp, ipv6/tcp, or ipv6/udp, if the destination or source port number is <port>.

tcp or udp can be limited by adding tcp or udp to the front of the above conditional expression indicating each port.

Example: tcp src port <port>

Furthermore, basic elements for which <identification> or other qualifiers are not specified are as fol-

lows:

ip proto <protocol number>

This is true when a packet is the IPv4 packet of the <protocol number> protocol.

Note that, when the protocol header is chained, it is not traced.

ip6 proto <protocol number>

This is true when a packet is the IPv6 packet of the <protocol number> protocol.

Note that, when the protocol header is chained, it is not traced.

ip multicast

This is true when a packet is an IPv4 multicast packet.

ip6 multicast

This is true when a packet is an IPv6 multicast packet.

ip, ip6, arp (Specify any of them)

This is true when a packet is ip, ip6, or arp.

tcp, udp, icmp, icmp6 (Specify any of them)

This is true when a packet is tcp, udp, icmp, or icmp6.

Note that, when the protocol header is chained, it is not traced.

ip protochain <protocol number>

The conditional expression is the same as that of ip proto <protocol number>, but the chain of the protocol header is traced.

ip6 protochain <protocol number>

The conditional expression is the same as that of ip6 proto <protocol number>, but the chain of the protocol header is traced.

Combinations of basic elements

A complicated filter conditional expression is represented by combining basic elements by using and, or, not.

To combine conditional expressions, enclose them in parentheses **( )**.

Example: host server1 and not **(** port ssh or port http **)**

The above expression filters packets for which host server1 is true, and port ssh or port http is false.

Explicit qualifiers can be omitted.

Example: tcp dst port ftp or ssh or domain is

the same meaning as that of tcp dst port ftp **or** tcp dst port ssh or tcp dst port domain.

Example of specifying <expression>

host serverA

Monitors packets communication with serverA.

tcp port telnet

Monitors telnet communication packets.

not tcp port ssh

Monitors packets other than SSH communication.

host serverA and tcp port bgp

Monitors BGP4/BGP4+ communication (IPv4 and IPv6) packets with serverA.

ip6 and host serverA and tcp port bgp

Monitors BGP4+ communication (IPv6) packets with serverA.

ip and not net 192.168.1/24

Monitors IPv4 packets whose destination and source are not the network 192.168.1/24.

udp port 520 or 521

Monitors RIP/RIPng communication (IPv4/IPv6) packets.

ip6 proto 89

Monitors OSPFv3 communication (IPv6) packets.

Behavior when this parameter is omitted:

All packets are dumped without filtering received packets.

Example 1

When IPv4 packets are monitored

Figure 27-14: Monitoring IPv4 packets

```
# show tcpdump interface vlan 10
Date 20XX/01/20 18:36:00 UTC
tcpdump: listening on VLAN0010
18:36:54.220039 IP hostA.example.com > hostB.example.com:
      1          2                      3
ICMP echo request, id 55146, seq 43, length 64
                   4
^C
1 packets received by filter      <--5
0 packets dropped by kernel       <--6
```

Display items in Example 1

Table 27-10: Information displayed when IPv4 packets are monitored

Displayed information	Description
1. Time stamp	Displays a time stamp when a packet is captured (not displayed when no-time is specified).
2. Protocol	Displays the protocol name and packet length except four bytes of the null/loopback header section (not displayed when brief is specified).
3. IP address pair	Displays a pair of the source address and destination address.
4. Upper-layer protocol	Displays upper-layer protocols for packet types, such as ICMP or TCP.
5. Monitor statistics	Displays the number of received packets.
6. Monitor statistics	Displays the number of dropped packets.

Example 2

When ARP packets are monitored

Figure 27-15: Monitoring ARP packets

```
# show tcpdump interface vlan 10
Date 20XX/01/20 16:07:00 UTC
tcpdump: listening on VLAN0010
16:07:29.683632 ARP: Request who-has 100.100.100.1 tell 100.100.100.2, length 46
16:07:29.683758 ARP: Reply 100.100.100.1 is-at 0:12:e2:98:dc:1 (oui Unknown), length 28
      1          2                                    3
```

```
^C
2 packets received by filter      <--4
0 packets dropped by kernel       <--5
```

Display items in Example 2

Table 27-11: Information displayed when ARP packets are monitored

Displayed information	Description
1. Time stamp	Displays a time stamp when a packet is captured (not displayed when no-time is specified).
2. Protocol	Displays arp and the packet length except four bytes of the null/loopback header section (not displayed when brief is specified).
3. Upper-layer protocol	Displays the information of the ARP protocol.
4. Monitor statistics	Displays the number of received packets.
5. Monitor statistics	Displays the number of dropped packets.

Impact on communication

None

Notes

1. This command can monitor software processing packets sent to or from the Switch.
2. Packets that are not sent to or from the Switch cannot be monitored. Note that filtered packets or packets that are not processed by software (various Layer 2 packets), which are one type of packet sent to or from the Switch, cannot be monitored.
3. This command can monitor the Layer 3 segment of packets. The Layer 2 segment of packets, such as the ethernet header, cannot be monitored. The Layer 2 segment is replaced with the loopback header (data link type) regardless of the type of the specified vlan <vlan id>.
4. The address family (ip/ip6/arp) is displayed in the information of the loopback header section.
5. The length of the loopback header is four bytes. This is displayed as [|null] when the <snaplen> setting is set to less than four bytes.
6. When the no-resolv parameter is not specified, if the dns-resolver configuration is wrong, displaying the monitoring status takes some time.
7. When there is a large amount of traffic, there might be too many packets to be monitored and packets might be dropped (Count of packets dropped by kernel is displayed after the command execution ends). In such a case, specify <expression> to monitor only required packets.

28 IPv6 Communication

show ip-dual interface

See "27 IPv4 Communication, show ip-dual interface".

show ipv6 interface

Shows the status of the IPv6 interface.

Syntax

```
show ipv6 interface
show ipv6 interface summary
show ipv6 interface up
show ipv6 interface down
show ipv6 interface <interface type> <interface number>
```

Input mode

User mode and administrator mode

Parameters

summary

Displays a summary of the status of all interfaces.

up

Displays detailed information about interfaces in the UP status.

down

Displays detailed information about interfaces in the DOWN status.

<interface type> <interface number>

Displays detailed information about the applicable interface.

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below. For details, see "■How to specify an interface" in "Specifiable values for parameters".

- VLAN interface
- Loopback interface

Behavior when all parameters are omitted:

The detailed status of all interfaces is displayed.

Example 1

Displays a summary of the status of all interfaces.

```
>show ipv6 interface summary
```

Figure 28-1: Example of displaying a summary of all interfaces

```
> show ipv6 interface summary
Date 20XX/12/10 12:00:00 UTC
VLAN0010: UP  2001:db8::1:1/64
              fe80::200:87ff:fe98:a21c%VLAN0010/64
>
```

Display format

```
Interface name: Status IPv6-address prefix-len
```

Display items in Example 1

Table 28-1: Information displayed for a summary of all interfaces

Item	Meaning	Displayed information
Interface name	Interface name	—
Status	Status of the interface	UP/DOWN
IPv6-address	IPv6 address	—
Prefix-len	Prefix length	—

Example 2

- This example shows how to display detailed information about interfaces in the UP status.
  ```
  >show ipv6 interface up
  ```
- Display the detailed status of an interface.
  ```
  > show ipv6 interface vlan 10
  ```

The following figure shows an example of executing the command with an interface specified.

Figure 28-2: Example of executing the command with an interface specified

```
>show ipv6 interface vlan 10
Date 20XX/12/10 12:00:00 UTC
VLAN0010: flags=1063<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST>
   mtu 1500
   inet6 2001:db8::1:1/64
   inet6 fe80::60:972e:1d4c%VLAN0010/64
   Switch01/NIF00/Port01: UP media 100BASE-TX full(auto) 0012.e22e.1d4c
   Switch01/NIF00/Port02: UP media ----- 0012.e22f.1d4f ChGr:5 (-)  <--------1
   Time-since-last-status-change: 30,00:10:00
   Last down at: 11/10 11:45:00         <-------------------------------------2
   VLAN: 10                   <-----------------------------------------------3
```

1. The example above is displayed for a link aggregation line.
2. The reason that the interface is down is a line failure or a change in the configuration of the IP information or the line. If the configuration is changed during a line failure, the time the line failure occurred is displayed instead of the time the information was updated because the status when the configuration was changed was the Down status.
3. The VLAN ID is displayed for a VLAN.

Display items in Example 2

The following describes the detailed information items.

Table 28-2: Displayed detailed information (common display items)

Item	Meaning	Displayed information
flags	Status of the target interface, and the configuration items	—
mtu	MTU for the interface	Shows the MTU of the IP interface.
inet6	IPv6 address	duplicated: The address is duplicated. tentative: The address is being checked for duplication.
broadcast	Broadcast address	Displayed when the IP interface type is broadcast.

Item	Meaning	Displayed information
UP/DOWN	Status of the interface	UP: In operation (Normal running state) DOWN: In operation (line has failed), or not in operation
media	Line type	For details about line types, see item <line type> of the "show interfaces" command in "20 Ethernet".
Time-since-last-status-change	Time elapsed since the status changed to UP or DOWN.	Time elapsed since the status of the interface last changed. The display format is hour:minute:second or number-of-days,hour:minute:second. "Over 100 days" is displayed if the number of days exceeds 100. "-----" is displayed if there has never been an UP or DOWN status.
Last down at	Time the interface went down	Time the interface last went down. The display format is month/day hour:minute:second. "-----" is displayed if the interface has never gone down.
VLAN	VLAN ID	—

Table 28-3: Displayed detailed information (Ethernet interface display items)

Item	Meaning	Displayed information
Switch<switch no.>	Switch number	—
NIF<nif no.>	NIF number	—
Port<port no.>	Port number	—
media	Line type/line speed	For details about line types, see item <line type> of the "show interfaces" command in "20 Ethernet".
xxxx.xxxx.xxxx	MAC address	The MAC address used by packets sent from the interface. For a VLAN interface, a MAC address of all zeros might be displayed if the line cannot communicate.
ChGr	Channel group number. The status of the channel group is displayed enclosed in parentheses.	—

Impact on communication

None

Notes

None

show ipv6 neighbors

Shows NDP information.

Syntax

```
show ipv6 neighbors [interface <interface type> <interface number>]
```

Input mode

User mode and administrator mode

Parameters

interface <interface type> <interface number>

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below. For details, see "■How to specify an interface" in "Specifiable values for parameters".

- VLAN interface

Behavior when this parameter is omitted:

The NDP information registered on all interfaces is displayed.

Example

Figure 28-3: Command execution result when a VLAN interface is specified

```
>show ipv6 neighbors interface vlan 100
Date 20XX/12/14 12:00:00 UTC
Total: 4 entries
Neighbor                          Linklayer Address Netif    State     Flags
2001:db8:100:10:1dff:fe22:f298    0012.e222.f298    VLAN0100 PERMANENT S
2001:db8:100:10:2a0:c9ff:fe6b:8e1b 0012.e26b.8e1b    VLAN0100 REACHABLE R
fe80::260:1dff:fe22:f298%VLAN0100  0012.e222.f298    VLAN0100 PERMANENT S
fe80::2a0:c9ff:fe6b:8e1b%VLAN0100  0012.e26b.8e1b    VLAN0100 REACHABLE R
>
```

Display items

Table 28-4: Information displayed about interfaces

Item	Displayed information	
	Detailed information	Meaning
Total: <entry> entries	Number of entries	Number of used NDP table entries
Neighbor	Next hop IP address	—
Linklayer Address	MAC address of a neighboring device	If the State item is INCOMPLETE, (incomplete) is displayed, and if it is FAILED, (deleting) is displayed.
Netif	Interface name	Interface name for the device

Item	Displayed information	
	Detailed information	Meaning
State	INCOMPLETE REACHABLE STALE DELAY PROBE FAILED PERMANENT UNKNOWN	NDP status INCOMPLETE: In incomplete status REACHABLE: In reachable status STALE: In stale status DELAY: In delay status PROBE: In probe status FAILED: Being deleted PERMANENT: Static entry UNKNOWN: The status is unknown.
Flags	R, S	Entry information R: Router S: Static

Impact on communication

None

Notes

None

clear ipv6 neighbors

Clears dynamic NDP information.

Syntax

```
clear ipv6 neighbors [interface <interface type> <interface number>]
```

Input mode

User mode and administrator mode

Parameters

interface <interface type> <interface number>

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below. For details, see "■How to specify an interface" in "Specifiable values for parameters".

- VLAN interface

Behavior when this parameter is omitted:

The NDP information registered on all interfaces is cleared.

Example

Figure 28-4: Execution result of clearing the NDP information (deleting the NDP information for a specific VLAN interface)

```
> show ipv6 neighbors interface vlan 100
Date 20XX/12/14 12:00:00 UTC
Total: 4 entries
Neighbor                          Linklayer Address Netif    State     Flags
2001:db8:100:10:1dff:fe22:f298    0012.e222.f298    VLAN0100 PERMANENT S
2001:db8:100:10:2a0:c9ff:fe6b:8e1b 0012.e26b.8e1b    VLAN0100 REACHABLE R
fe80::260:1dff:fe22:f298%VLAN0100  0012.e222.f298    VLAN0100 PERMANENT S
fe80::2a0:c9ff:fe6b:8e1b%VLAN0100  0012.e26b.8e1b    VLAN0100 REACHABLE R
>
> clear ipv6 neighbors interface vlan 100
> show ipv6 neighbors interface vlan 100
> show ipv6 neighbors interface vlan 100
Date 20XX/12/14 12:02:00 UTC
Total: 2 entries
Neighbor                          Linklayer Address Netif    State     Flags
2001:db8:100:10:1dff:fe22:f298    0012.e222.f298    VLAN0100 PERMANENT S
fe80::260:1dff:fe22:f298%VLAN0100  0012.e222.f298    VLAN0100 PERMANENT S
>
```

Display items

None

Impact on communication

Communication might stop temporarily until the NDP entry is created again.

Notes

None

show netstat(netstat)

See "27. IPv4 Communication, show netstat(netstat)".

ping ipv6

The "ping ipv6" command is used to determine whether communication is possible with the device with the specified IPv6 address. This command is used with IPv6 only.

Syntax

```
ping ipv6 <host> [numeric] [summary] [count <count>]
     [interval <wait>] [pad-byte <pattern>]
     [interface <interface type> <interface number>]
     [source <source address>] [packetsize <size>]
     [hoplimit <hops>]
```

Input mode

User mode and administrator mode

Parameters

<host>

Specifies the destination host name, an IPv6 address, or an IPv6 address with an interface name (for a link-local address only).

numeric

Displays the host IPv6 address without converting it to a name. If a standard host name is registered on the host, the standard host name is displayed at the end of the command.

Behavior when this parameter is omitted:

Displays the name converted from the host IPv6 address.

summary

Restricts the output. Only the summary lines of the first and last lines are displayed.

Behavior when this parameter is omitted:

Displays one line for one response as regular display mode.

count <count>

Sends packets for the number of times specified for <count>, and then finishes the processing. To interrupt the processing, press Ctrl+C. The specifiable values are from 1 to 2147483647.

Behavior when this parameter is omitted:

Sends packets indefinitely.

interval <wait>

Sets the packet sending interval to the number of seconds specified for <wait>. The specifiable values are from 1 to 2147482.

Behavior when this parameter is omitted:

The sending interval defaults to 1 second.

pad-byte <pattern>

Specifies the pad bytes for packets to be sent. The maximum size of the pad is 16 bytes. This is effective for diagnosing data-dependent problems on the network. For example, specify pad-byte ff to generate an all-ones packet to be sent. You can specify a hexadecimal number consisting of 1 to 32 digits.

Behavior when this parameter is omitted:

Generates pad characters by incrementing from 00 to ff.

interface <interface type> <interface number>

If the destination IPv6 address specified for <host>is a multicast address or link-local address, specify the source interface.

If the destination IPv6 address specified for <host>is a unicast address, packets will be sent only when active routes to the interface specified by <interface type> and <interface number> are retained.

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below. For details, see "■How to specify an interface" in "Specifiable values for parameters".

- VLAN interface
- Loopback interface

Behavior when this parameter is omitted:

Packets are sent from the interface selected by the Switch.

source <source address>

Uses the IPv6 address specified for <source address> as the source address of an output packet. Only the IPv6 addresses set on the Switch can be specified.

Behavior when this parameter is omitted:

The source IPv6 address selected by the Switch is used.

packetsize <size>

Specifies how many bytes of data are to be sent. The specifiable values are from 1 to 65527.

Behavior when this parameter is omitted:

The number of bytes of data to be sent is 56.

By adding 8 bytes of ICMPv6 header data, a total of 64 bytes will be sent.

hoplimit <hops>

Sets the value specified for <hops> to the hops field of the IPv6 header. The specifiable values are from 1 to 255.

Behavior when this parameter is omitted:

64 is set.

Behavior when all parameters are omitted:

Displays one line for one response as regular display mode.

Example

- This example shows how to execute an echo test by specifying the default values (unlimited attempts, data size of 56 bytes, and sending interval of 1 second).

  Figure 28-5: Result of executing the ping ipv6 command with default values

```
> ping ipv6 2001:db8::10
PING 2001:db8::10 (2001:db8::10) 56 data bytes
64 bytes from 2001:db8::10: icmp_seq=1 ttl=64 time=0.468 ms
64 bytes from 2001:db8::10: icmp_seq=2 ttl=64 time=0.45 ms
64 bytes from 2001:db8::10: icmp_seq=3 ttl=64 time=0.301 ms
^C
--- 2001:db8::10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.301/0.406/0.468/0.334 ms
>
```

- This examples shows how to execute an echo test by specifying 3 attempts, data size of 120 bytes, and sending interval of 2 seconds.

  Figure 28-6: Example of executing the ping ipv6 command by specifying 3 attempts, data size of 120 bytes, and sending interval of 2 seconds

```
>ping ipv6 2001:db8::10 count 3 packetsize 120 interval 2
```

Impact on communication

None

Notes

- To halt execution of the "ping ipv6" command, press Ctrl+C.
- In IPv6, unlike IPv4, the address defined for the sending interface might not be a starting point address.

  To use the "ping ipv6" command to perform continuity confirmation, make sure that which address is selected for the starting point address. If a connection cannot be established, use the source parameter to specify another IPv6 address set on the interface for the device, and then perform continuity confirmation again.
- If the "ping ipv6" command is executed for an IPv6 address that is also used by another device, an IPv6 address that is different from the specified IPv6 address might return response messages.

  In addition, if the command is executed for the IPv6 address of an interface that has just started, response messages might be sent from a different IPv6 address for several seconds after the command is executed.

traceroute ipv6

Displays the route (route of the passed gateways and response time between the gateways) over which UDP6 messages are sent to the destination host. This command is used with IPv6 only.

Syntax

```
traceroute ipv6 <host> [numeric] [direct]
[hoplimit <hops>] [port <port>]
[probes <nqueries>] [source <source address>]
[waittime <time>] [packetsize <size>]
```

Input mode

User mode and administrator mode

Parameters

<host>

Specifies the destination host name, a host IPv6 address, or an IPv6 address with an interface name (for a link-local address only) for the test target (IP destination).

numeric

Displays the gateway address by the IPv6 address, not by the host name.

Behavior when this parameter is omitted:

Displays the name converted from the host IPv6 address.

direct

Directly sends the probe packet to the host on the connected network. The normal routing table is not used. You can use this option when using an interface without routes to execute the "traceroute ipv6" command on the host.

Behavior when this parameter is omitted:

Uses the normal routing table to send data.

hoplimit <hops>

Sets the maximum number of hops for the probe packets to be sent. The specifiable values are from 1 to 255.

Behavior when this parameter is omitted:

The maximum number of hops is 30.

port <port>

Specifies the port number of the UDP6 packet to be used. The specifiable values are from 1 to 65535. The port number for a probe packet starts with the <port> value, and is incremented by one for each probe packet.

Behavior when this parameter is omitted:

Port number 33434 is used.

probes <nqueries>

Specify the number of times a search is performed for each hop in <nqueries>. The specifiable values are from 1 to 10.

Behavior when this parameter is omitted:

A search is performed 3 times.

source <source address>

Uses the IPv6 address of an argument (specified by number, not by host name) as the source address of the probe packet to be sent (address to be sent). For a host with multiple IPv6 addresses, this parameter can be used to assign another source address to the probe packet. If the specified IPv6 address is not one of the interface addresses of that host, an error is returned and not data is sent.

Behavior when this parameter is omitted:

The source IPv6 address selected by the Switch is used.

waittime <time>

Specify the time (in seconds) to wait for a probe packet. The specifiable values are from 2 to 2147483647.

Behavior when this parameter is omitted:

The wait time for a response is 5 seconds.

packetsize <size>

Specify, in bytes, the data size of a probe packet. The specifiable values are from 48 to 65000. If a value from 0 to 47 is specified, 48 is assumed.

Behavior when this parameter is omitted:

The data size is set to 80 bytes.

Behavior when all parameters are omitted:

Displays the route to the specified <host>.

Example

Figure 28-7: Execution result of the traceroute ipv6 command

```
> traceroute ipv6 2001:db8::100 numeric
traceroute to 2001:db8::100 (2001:db8::100), 30 hops max, 80 byte packets
 1  2001:db8:22::1  0.612 ms *  0.532 ms
 2  2001:db8::100 0.905 ms  0.816 ms  0.807 ms
```

Impact on communication

None

Notes

- In IPv6, unlike IPv4, the address defined for the sending interface might not be a starting point address. To use the "traceroute ipv6" command to perform forwarding route confirmation, check which address is selected for the starting point address. If a connection cannot be established, use the source parameter to specify another IPv6 address set on the interface for the device, and then confirm everything again.
- If there is a global host route for the destination host, the direct parameter does not take effect for that host.
- If the "traceroute ipv6" command is executed for an IPv6 address that is also used by another device, an IPv6 address that is different from the specified IPv6 address might return response messages.

  In addition, if the command is executed for the IPv6 address of an interface that has just started, response messages might be sent from a different IPv6 address.
- If ICMPv6 messages are continuously issued to the Switch during execution of the "traceroute ipv6" command from the Switch, the command might appear to send no response.

show ipv6 route

Displays the IPv6 routing table.

Syntax

```
show ipv6 route
```

Input mode

User mode and administrator mode

Parameters

None

Example: show ipv6 route command

Figure 28-8: Command execution result when IPv6 route information is displayed

```
> show ipv6 route
Date 20XX/12/14 12:00:00 UTC
Total: 4 routes
Destination                   Next Hop                 Interface  Protocol
2001:db8:100:10::/64                                   VLAN0100   Connected
2001:db8:200:10::/64                                   VLAN0200   Connected
2001:db8:300:10::/64          2001:db8:100:10::1       VLAN0100   Static
::/0                          fe80::212:e2ff:fe3e:f3db VLAN0200   RA
>
```

Display items

Table 28-5: Displayed route information stored in the routing table

Item	Meaning	Displayed detailed information
Total	Number of routes	—
Destination	Destination network	destination address/prefix length
Next Hop	Next hop address	It is not displayed for a directly connected route.
Interface	Sending interface name	—
Protocol	The protocol that was used to learn the routing information	Connected: Directly connected route
		Static: Static route
		RA: Default route created from router advertisement messages
		Any: Other

Impact on communication

None

Notes

None

show ipv6 router-advertisement

Displays address and default route information based on received router advertisement messages.

Syntax

```
show ipv6 router-advertisement
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 28-9: Execution result of the show ipv6 router-advertisement command

```
> show ipv6 router-advertisement
Date 20XX/12/14 12:00:00 UTC
Auto-configured addresses from RA:
Address                                 Interface  ValidLife  PrefLife
2001:db8:100:1:212:e2ff:e203:ab60/64    VLAN0100   2591985    604785
2001:db8:200:1:212:e2ff:e203:ab60/64    VLAN0200   2456331    469131

Default gateway:
Nexthop                                 Interface  Expires    hoplimit
fe80::212:e2ff:fe3e:f3db                VLAN0100   1744       64
>
```

Display items

Table 28-6: Items displayed for the show ipv6 router-advertisement command

Item	Meaning	Displayed detailed information
Auto-configured addresses from RA	Address automatically generated from a router advertisement message	Displays "none" if the address generated from the router advertisement message does not exist.
Address	IPv6 address	—
Interface	Name of the receiving interface of router advertisements	—
ValidLife	Validity period	How long this address is valid (in seconds). If the validity period is infinite, "forever" is displayed. The initial value uses the number of seconds specified in the validity period field information of the prefix information option of the router advertisement message.
PrefLife	Preferred period	How long this address is preferred (in seconds). If the preferred period is infinite, "forever" is displayed. The initial value is the number of seconds specified in the preferred period field information of the prefix information option of the router advertisement message.
Default gateway	Default route information set from the router advertisement message	If there is no default route set from the router advertisement message, "none" is displayed.

Item	Meaning	Displayed detailed information
Nexthop	Next-hop IPv6 address of the default route	—
Expires	Time-to-live value of the default route	How long the default route survives (in seconds). The initial value is the number of seconds specified in the router time-to-live field of the router advertisement message.
hoplimit	Hop limit	The default value for the hop limit used for communication on the interface for this next hop. It is specified from the Cur Hop Limit field of the router advertisement message.

Impact on communication

None

Notes

None

show tcpdump (tcpdump)

See "27 IPv4 Communication, show tcpdump (tcpdump)".

29 DHCP Server Function

show ip dhcp binding

Shows the binding information on the DHCP server.

Syntax

```
show ip dhcp binding [ {<IP Address> | sort } ]
```

Input mode

User mode and administrator mode

Parameters

{<IP Address> | sort }

<IP Address>

Displays the binding information for the specified IP address.

sort

Displays the binding information sorted in ascending order using the IP address as the key.

Behavior when this parameter is omitted:

Displays all binding information on the DHCP server without sorting.

Example

Figure 29-1: Execution result of displaying binding information on the DHCP server

```
> show ip dhcp binding
Date 20XX/10/15 12:00:00 UTC
<IP address>      <MAC address>    <Lease expiration>   <Type>
192.168.200.9     0012.e248.e92d   XX/12/06 19:59:40    Automatic
192.168.200.99    0012.e292.f7b9                        Manual
>
```

Display items

Table 29-1: Items displayed for biding information on the DHCP server

Item	Meaning	Detailed information
IP address	Current IP address connected to the DHCP server	—
MAC address	MAC address	—
Lease expiration	Lease expiration date and time (year/month/day hour:minute:second) However, this item is not displayed for the Manual connection type.	—
Type	Connection type (Manual or Automatic)	Manual: Binding information assigned based on host settings Automatic: Binding information assigned dynamically

Impact on communication

None

Notes

Binding information for which the lease has been expired is not displayed.

clear ip dhcp binding

Deletes the binding information from the DHCP server database.

Syntax

```
clear ip dhcp binding [ {<IP Address> | all } ]
```

Input mode

User mode and administrator mode

Parameters

{<IP Address> | all }

<IP Address>

Deletes binding information for the specified IP address.

all

Deletes all the binding information on the DHCP server.

Behavior when this parameter is omitted:

Deletes all the binding information on the DHCP server.

Example

Figure 29-2: Execution result of deleting binding information on the DHCP server

```
> clear ip dhcp binding
>
```

Display items

None

Impact on communication

When dynamic DNS linkage is enabled, the corresponding entry records are deleted from a dynamic DNS server (DNS updates) concurrently, so name resolution cannot be performed.

Notes

None

show ip dhcp import

Shows additional information to be distributed to clients specified in the DHCP address pool definition for the DHCP server.

Syntax

```
show ip dhcp import
```

Input mode

User mode and administrator mode

Parameters

None

Example

This example shows how to display additional information to be distributed to clients specified in the DHCP address pool definition for the DHCP server. Additional information is not displayed unless additional information to be distributed to clients has been set.

Figure 29-3: Execution result of displaying the DHCP server configuration (additional information)

```
> show ip dhcp import
Date 20XX/10/15 12:00:00 UTC
subnet 192.168.200.0 netmask 255.255.255.0
        routers 192.168.200.1
        domain-name-servers 200.10.10.2
        domain-name "Tokyo1"
        netbios-name-servers 192.168.200.30
subnet 200.10.10.0 netmask 255.255.255.0
        routers 200.10.10.1
        domain-name-servers 200.10.10.2
        domain-name "Tokyo2"
        netbios-name-servers 200.10.10.3
        netbios-node-type 4
host Nagoya1
        routers 192.168.200.1
        domain-name-servers 200.10.10.2
        host-name "Nagoya1"
        domain-name "Tokyo1"
        netbios-name-servers 192.168.200.30
        netbios-node-type 1
host Nagoya2
        routers 200.10.10.1,200.10.1.1
        domain-name-servers 200.10.10.5
        domain-name "Tokyo2"
        netbios-name-servers 200.10.10.3
        netbios-node-type 4
>
```

Display items

Table 29-2: Items displayed for the DHCP server configuration (additional information)

Item	Meaning	Detailed information
subnet	Information set by the "network" configuration command	—
host	DHCP address pool name of the DHCP address pool definition in which the "host" configuration command is defined	—
routers	Information set by the "default-router" configuration command	—

Item	Meaning	Detailed information
domain-name-servers	Information set by the "dns-server" configuration command	—
domain-name	Information set by the "domain-name" configuration command	—
host-name	Information set by the "client-name" configuration command	—
netbios-name-server	Information set by the "netbios-name-server" configuration command	—
netbios-node-type	Information set by the "netbios-node-type" configuration command	—

Impact on communication

None

Notes

None

show ip dhcp conflict

Shows an IP address conflict detected by the DHCP server. An IP address conflict refers to an IP address assigned to a terminal over the network, although it is blank as a DHCP address pool on the DHCP server. Before the DHCP server assigns the IP address to a DHCP client, the DHCP server detects an IP address conflict by checking for a response to a sent ICMP packet.

Syntax

```
show ip dhcp conflict [ <IP Address> ]
```

Input mode

User mode and administrator mode

Parameters

<IP Address>

Displays the IP address conflict information for the specified IP address.

Behavior when this parameter is omitted:

Shows all IP address conflict detected by the DHCP server.

Example

Figure 29-4: Execution result of displaying IP address conflict information detected by the DHCP server

```
> show ip dhcp conflict
Date 20XX/10/15 12:00:00 UTC
<IP address>      <Detection time>
192.168.200.9     XX/10/05 15:39:55
192.168.200.15    XX/10/05 16:51:45
>
```

Display items

Table 29-3: Items displayed for IP address conflict information detected by DHCP server

Item	Meaning	Detailed information
IP address	Conflict IP address detected by the DHCP server	—
Detection time	Detection time (year/month/day hour:minute:second)	—

Impact on communication

None

Notes

A maximum of 200 items of IP address conflict information are stored in the DHCP server.

clear ip dhcp conflict

Clears the IP address conflict information from the DHCP server.

Syntax

```
clear ip dhcp conflict [ {<IP Address> | all} ]
```

Input mode

User mode and administrator mode

Parameters

{<IP Address> | all}

<IP Address>

Deletes IP address conflict information for the specified IP address.

all

Deletes all IP address conflict information on the DHCP server.

Behavior when this parameter is omitted:

Deletes all IP address conflict information on the DHCP server.

Example

Figure 29-5: Execution result of deleting IP address conflict information on the DHCP server

```
> clear ip dhcp conflict 172.16.1.11
>
```

Display items

None

Impact on communication

None

Notes

None

show ip dhcp server statistics

Shows statistics about the DHCP server.

Syntax

```
show ip dhcp server statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 29-6: Execution result of displaying DHCP server statistics

```
> show ip dhcp server statistics
Date 20XX/10/15 12:00:00 UTC
   < DHCP Server use statistics >
     address pools          :19
     automatic bindings     :170
     manual bindings        :1
     expired bindings       :3
     over pools request     :0
     discard packets        :0
   < Receive Packets >
     BOOTREQUEST            :0
     DHCPDISCOVER           :178
     DHCPREQUEST            :178
     DHCPDECLINE            :0
     DHCPRELEASE            :1
     DHCPINFORM             :0
   < Send Packets >
     BOOTREPLY              :0
     DHCPOFFER              :178
     DHCPACK                :172
     DHCPNAK                :6
>
```

Display items

Table 29-4: Items displayed for the DHCP server statistics

Category	Item	Meaning
DHCP Server use statistics	address pools	Number of unassigned DHCP addresses
	automatic bindings	Number of DHCP addresses automatically assigned
	manual bindings	Number of DHCP addresses fixed assigned
	expired bindings	Number of DHCP addresses already assigned
	over pools request	Number of insufficient DHCP addresses that has been detected
	discard packets	Number of discarded packets
Receive Packets	BOOTREQUEST	Number of received BOOTREQUEST packets
	DHCPDISCOVER	Number of received DHCPDISCOVER packets

Category	Item	Meaning
	DHCPREQUEST	Number of received DHCPREQUEST packets
	DHCPDECLINE	Number of received DHCPDECLINE packets
	DHCPRELEASE	Number of received DHCPRELEASE packets
	DHCPINFORM	Number of received DHCPINFORM packets
Send Packets	BOOTREPLY	Number of sent BOOTREPLY packets
	DHCPOFFER	Number of sent DHCPOFFER packets
	DHCPACK	Number of sent DHCPACK packets
	DHCPNAK	Number of sent DHCPNAK packets

Impact on communication

None

Notes

None

clear ip dhcp server statistics

Resets statistics on the DHCP server.

Syntax

```
clear ip dhcp server statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 29-7: Execution result of resetting DHCP server statistics

```
> clear ip dhcp server statistics
>
```

Display items

None

Impact on communication

None

Notes

None

restart dhcp

Restarts the DHCP server daemon process.

Syntax

```
restart dhcp [ -f ][ core-file ]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the DHCP server program without displaying a restart confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file (dhcp_server.core) for the DHCP server program during restart.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

Displays a restart confirmation message and then restarts the DHCP server program.

Example

Figure 29-8: Execution result of restarting the DHCP server daemon

```
> restart dhcp
DHCP Server program restart OK? (y/n):y
dhcp_server terminated.
>
```

Display items

None

Impact on communication

Distribution, update, and release of IP addresses cannot be performed, because the sending and receiving of DHCP packets temporarily stops.

Notes

Core output file: /usr/var/core/dhcp_server.core

dump protocols dhcp

Outputs the server log data and the packet sending and receiving log data collected by the DHCP server program to a file.

Syntax

```
dump protocols dhcp
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 29-9: Execution result of outputting DHCP server log data

```
> dump protocols dhcp
>
```

Display items

None

Impact on communication

None

Notes

Server log data is always collected. Packet sending and receiving log data is collected only when requested.

Output file: /usr/var/dhcp/dhcp.trc

dhcp server monitor

Starts collection of sending and receiving log data for packets which are sent and received by the DHCP server.

Syntax

```
dhcp server monitor
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 29-10: Execution result of starting the collection of sending and receiving packet log data on the DHCP server

```
> dhcp server monitor
>
```

Display items

None

Impact on communication

None

Notes

To collect packet log data, execute the "dump protocols dhcp" command after execution of this command.

no dhcp server monitor

Stops collection of the sending and receiving log data for packets on the DHCP server.

Syntax

```
no dhcp server monitor
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 29-11: Execution result of stopping the collection of sending and receiving packet log data on the DHCP server

```
> no dhcp server monitor
>
```

Display items

None

Impact on communication

None

Notes

None

30 Filters

show access-filter

Displays the filter conditions applied on the Ethernet interface or VLAN interface by the access group commands (ip access-group, ipv6 traffic-filter, and mac access-group), the number of packets that met the filter conditions, and the number of packets discarded because they did not match any filter conditions in the access list.

Syntax

```
show access-filter
show access-filter <switch no.>/<nif no.>/<port no.>
            [ { <access list number> | <access list name> } ]
            [ { in | out } ]
show access-filter interface vlan <vlan id>
            [ { <access list number> | <access list name> } ]
            [ { in | out } ]
```

Input mode

User mode and administrator mode

Parameters

{ <switch no.>/<nif no.>/<port no.> | interface vlan <vlan id> } [{ <access list number> | <access list name> }]

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

Displays statistics for the specified Ethernet interface. For the specifiable ranges of <switch no.>, <nif no.>, and <port no.> values, see "Specifiable values for parameters".

interface vlan <vlan id>

Displays statistics for the specified VLAN interface.

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

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

access list number: Access list number

access list name: Access list name

The command with this parameter displays statistics for the specified interface that has the specified access list number or access list name.

Behavior when this parameter is omitted:

Statistics for all access lists applied to the specified interface are displayed.

Behavior when this parameter is omitted:

Statistics for all interfaces are displayed.

{ in | out }

in: Inbound (Specifies the receiving side of the filter)

out: Outbound (Specifies the sending side of the filter)

Statistics on the receiving side or sending side of the filter of the specified interface are displayed.

Behavior when this parameter is omitted:

Statistics for the receiving side and the sending side of the specified interface are displayed.

Example

Figure 30-1: Result of displaying the extended MAC access list

```
> show access-filter 1/0/3 only-appletalk
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/3 in
Extended MAC access-list:only-appletalk
      remark "permit only appletalk"
      10 permit any any appletalk(0x809b)
         matched packets       :    74699826
      20 permit any any 0x80f3
         matched packets       :      718235
      implicitly denied packets:        2698
>
```

Figure 30-2: Result of displaying the standard IPv4 access list

```
> show access-filter 1/0/7 12
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/7 in
Standard IP access-list:  12
      remark "permit only host pc"
      10 permit host 10.10.10.1
         matched packets       :    74699826
      20 permit host 10.10.10.254
         matched packets       :      264176
      implicitly denied packets:        2698
>
```

Figure 30-3: Result of displaying the extended IPv4 access list

```
> show access-filter 1/0/11 128
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/11 in
Extended IP access-list: 128
      remark "permit only http server"
      10 permit tcp(6) any host 10.10.10.2 eq http(80)
         matched packets       :    74699826
      implicitly denied packets:        2698
>
```

Figure 30-4: Result of displaying the IPv6 access list

```
> show access-filter 1/0/15 telnet-server
Date 20XX/12/14 12:00:00 UTC
Using Port:1/0/15 in
IPv6 access-list:telnet-server
      remark "permit only telnet server"
      10 permit ipv6(41) any host 3ffe:501:811:ff00::1
         matched packets       :    74699826
      implicitly denied packets:        2698
>
```

Figure 30-5: Result of displaying the information when the access list ID is omitted

```
> show access-filter 1/0/19
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/19 in
Standard IP access-list:pc-a1024
      remark "permit only pc-a1024"
      10 permit host 192.168.1.254
         matched packets       :    74699826
      implicitly denied packets:        2698
IPv6 access-list:smtp-server
      remark "permit only smtp server"
      20 permit ipv6(41) any host 3ffe:501:811:ff00::1
         matched packets       :    74699826
      implicitly denied packets:        2698
>
```

Figure 30-6: Result of displaying the information when in or out is omitted

```
> show access-filter interface vlan 1500
Date 20XX/09/01 12:00:00 UTC
```

```
Using Interface:vlan 1500 in
Standard IP access-list:pc-a1024
      remark "permit only pc-a1024"
      10 permit host 192.168.1.254
         matched packets       :    74699826
      implicitly denied packets:        2698
IPv6 access-list:only-smtp
      remark "permit only smtp ipv6"
      20 permit ipv6(41) any host 3ffe:501:811:ff00::1 eq smtp(25)
         matched packets       :    74699826
      implicitly denied packets:        2698

Using Interface:vlan 1500 out
Extended IP access-list:only-ssh
      remark "permit only ssh"
      10 permit tcp(6) any any eq ssh(22)
         matched packets       :    74699826
      implicitly denied packets:        2698
>
```

Figure 30-7: Result of displaying the information when all parameters are omitted

```
> show access-filter
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/7 in
Standard IP access-list:  12
      remark "permit only host pc"
      10 permit host 10.10.10.1
         matched packets       :    74699826
      20 permit host 10.10.10.254
         matched packets       :      264176
      implicitly denied packets:        2698

Using Port:1/0/11 in
Extended IP access-list: 128
      remark "permit only http server"
      10 permit tcp(6) any host 10.10.10.2 eq http(80)
         matched packets       :    74699826
      implicitly denied packets:        2698

Using Port:1/0/15 in
IPv6 access-list:telnet-server
      remark "permit only telnet server"
      10 permit ipv6(41) any host 3ffe:501:811:ff00::1
         matched packets       :    74699826
      implicitly denied packets:        2698

Using Port:1/0/19 in
Standard IP access-list:pc-a1024
      remark "permit only pc-a1024"
      10 permit host 192.168.1.254
         matched packets       :    74699826
      implicitly denied packets:        2698
IPv6 access-list:smtp-server
      remark "permit only smtp server"
      20 permit ipv6(41) any host 3ffe:501:811:ff00::1
         matched packets       :    74699826
      implicitly denied packets:        2698
>
```

Display items

Table 30-1: Statistical items for the access list

Item	Displayed information	
	Detailed information	Meaning
Interface information	Using Port:<switch no.>/<nif no.>/<port no.> in	Information about an Ethernet interface to which an access list has been applied on the inbound side
	Using Port:<switch no.>/<nif no.>/<port no.> out	Information about an Ethernet interface to which an access list has been applied on the outbound side
	Using Interface:vlan <vlan id> in	Information about a VLAN interface to which an access list has been applied on the inbound side
	Using Interface:vlan <vlan id> out	Information about a VLAN interface to which an access list has been applied on the outbound side
Access list ID	Extended MAC access-list:<access list name>	Extended MAC access list ID
	Standard IP access-list:{ <access list number> | <access list name> }	Standard IPv4 access list ID
	Extended IP access-list:{ <access list number> | <access list name> }	Extended IPv4 access list ID
	IPv6 access-list:<access list name>	IPv6 access list ID
Access list information	Displays supplementary information and filter conditions set by access list commands. (For details, see "Configuration Command Reference, 27 Access Lists".)	
Statistics	matched packets:<packets>	Number of packets that meet the filter conditions in the access list
	implicitly denied packets:<packets>	Number of packets that were discarded because they did not meet any of the filter conditions in the access list

Impact on communication

None

Notes

None

clear access-filter

For the access list information displayed by the "show access-filter" command, this command resets the number of packets that met the filter conditions (indicated in matched packets) and the number of packets discarded because they did not meet the filter conditions (indicated in implicitly denied packets).

Syntax

```
clear access-filter
clear access-filter <switch no.>/<nif no.>/<port no.>
             [ { <access list number> | <access list name> } ]
             [ { in | out } ]
clear access-filter interface vlan <vlan id>
             [ { <access list number> | <access list name> } ]
             [ { in | out } ]
```

Input mode

User mode and administrator mode

Parameters

{ <switch no.>/<nif no.>/<port no.> | interface vlan <vlan id> } [{ <access list number> | <access list name> }]

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

Clears statistics for the specified Ethernet interface to zero. For the specifiable ranges of <switch no.>, <nif no.>, and <port no.> values, see "Specifiable values for parameters".

interface vlan <vlan id>

Clears statistics for the specified VLAN interface to zero.

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

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

access list number: Access list number

access list name: Access list name

Resets statistics for the specified access list number or access list name of the specified interface.

Behavior when this parameter is omitted:

Statistics for all access lists applied to the specified interface are cleared to zero.

Behavior when this parameter is omitted:

Statistics for all interfaces are cleared to zero.

{ in | out }

in: Inbound (Specifies the receiving side of the filter)

out: Outbound (Specifies the sending side of the filter)

Statistics on the receiving side or sending side of the filter of the specified interface are cleared to zero.

Behavior when this parameter is omitted:

Statistics for the receiving side and the sending side of the specified interface are reset to zero.

Example

Figure 30-8: Result of resetting the statistics about the standard IPv4 access list to zero

```
> clear access-filter 1/0/7 12
Date 20XX/07/14 12:00:00 UTC
>
```

Display items

None

Impact on communication

None

Notes

1. If this command is executed, the MIB information of the axsAccessFilterStats group is also cleared to zero.

31 QoS

show qos-flow

Displays the number of packets that meet the flow detection conditions corresponding to the flow detection conditions and specified actions in the QoS flow list applied to the Ethernet interface or VLAN interface by QoS flow group commands (ip qos-flow-group, ipv6 qos-flow-group, and mac qos-flow-group).

Syntax

```
show qos-flow [ { <switch no.>/<nif no.>/<port no.> | interface vlan <vlan id> }
                [ <qos flow list name> ] ]
```

Input mode

User mode and administrator mode

Parameters

{ <switch no.>/<nif no.>/<port no.> | interface vlan <vlan id> } [<qos flow list name>]

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

Displays statistics for the specified Ethernet interface. For the specifiable ranges of <switch no.>, <nif no.>, and <port no.> values, see "Specifiable values for parameters".

interface vlan <vlan id>

Displays statistics for the specified VLAN interface.

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

<qos flow list name>

<qos flow list name>: Specify the QoS flow list name.

Statistics for the specified QoS flow list of the specified interface are displayed.

Behavior when this parameter is omitted:

Statistics for all QoS flow lists applied to the specified interface are displayed.

Behavior when this parameter is omitted:

Statistics for all interfaces are displayed.

Example

Figure 31-1: Result of displaying the MAC QoS flow list information

```
> show qos-flow 1/0/3 apple-talk-qos
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/3 in
MAC qos-flow-list:apple-talk-qos
      remark "cos 5 discard-class 2"
      10 any any appletalk(0x809b) action cos 5 discard-class 2
         matched packets               :     74699826
>
```

Figure 31-2: Result of displaying the IPv4 QoS flow list information

```
> show qos-flow 1/0/7 http-qos
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/7 in
IP qos-flow-list:http-qos
      remark "cos 4"
      10 tcp(6) any host 10.10.10.2 eq http(80) action cos 4
```

```
         matched packets                :     74699826
>
```

Figure 31-3: Result of displaying the IPv6 QoS flow list information

```
> show qos-flow 1/0/11 telnet-qos
Date 20XX/12/14 12:00:00 UTC
Using Port:1/0/11 in
IPv6 qos-flow-list:telnet-qos
      remark "cos 6 discard-class 2"
      10 ipv6(41) any host 13ffe:501:811:ff00::1 action cos 6 discard-class 2
         matched packets                :     74699826
>
```

Display items

Table 31-1: Statistical items for the QoS flow list

Item	Displayed information	
	Detailed information	Meaning
Interface information	Using Port:<switch no.>/<nif no.>/<port no.> in	Information about an Ethernet interface to which a QoS flow list is applied on the inbound side
	Using Interface:vlan <vlan id> in	Information about a VLAN interface to which a QoS flow list is applied on the inbound side
QoS flow list name	MAC qos-flow-list: <qos flow list name>	MAC QoS flow list name
	IP qos-flow-list: <qos flow list name>	IPv4 QoS flow list name
	IPv6 qos-flow-list: <qos flow list name>	IPv6 QoS flow list name
QoS flow list information	Displays supplementary information, flow detection conditions, and actions set by QoS flow list commands. (For details, see "Configuration Command Reference, 28 QoS".)	
Statistics	matched packets:<packets>	Number of packets that meet the flow detection conditions in the QoS flow list

Impact on communication

None

Notes

None

clear qos-flow

Clears the number of packets (indicated by matched packets) that met the flow detection conditions in the QoS flow list, which is displayed by the "show qos-flow" command.

Syntax

```
clear qos-flow [ { <switch no.>/<nif no.>/<port no.> | interface vlan <vlan id> }
                 [ <qos flow list name> ] ]
```

Input mode

User mode and administrator mode

Parameters

{ <switch no.>/<nif no.>/<port no.> | interface vlan <vlan id> } [<qos flow list name>]

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

Clears statistics for the specified Ethernet interface to zero. For the specifiable ranges of <switch no.>, <nif no.>, and <port no.> values, see "Specifiable values for parameters".

interface vlan <vlan id>

Clears statistics for the specified VLAN interface to zero.

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

<qos flow list name>

<qos flow list name>: Specify the QoS flow list name.

Clears statistics for the specified QoS flow list of the specified interface to zero.

Behavior when this parameter is omitted:

Statistics for all QoS flow lists applied to the specified interface are cleared to zero.

Behavior when this parameter is omitted:

Statistics for all interfaces are cleared to zero.

Example

Figure 31-4: Result of clearing the information

```
> clear qos-flow 1/0/7 http-qos
Date 20XX/07/14 12:00:00 UTC
>
```

Display items

None

Impact on communication

None

Notes

1. If this command is executed, the MIB information of the axsQosFlowStats group is also cleared to zero.

show qos queueing

Displays information about the send queue of the port.

The send queue length, the maximum queue length, and the number of packets discarded without being accumulated in the send queue are displayed to enable monitoring of the traffic status.

Syntax

```
show qos queueing [ <switch no.>/<nif no.>/<port no.> ]
```

Input mode

User mode and administrator mode

Parameters

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

Displays information about the send queue of the specified port. For the specifiable ranges of <switch no.>, <nif no.>, and <port no.> values, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

Displays information about the send queues of all ports implemented on the device, and about the send queues for traffic from the ports to the CPU.

Example

Figure 31-5: Result of displaying the information about all send queues (for AX2340S-48T4X)

```
> show qos queueing

Date 20XX/01/01 12:00:00 UTC
Switch1 To-CPU (outbound)
Max_Queue=10
  Queue  1: Qlen=    0, Limit_Qlen=   36, HOL1=         0
  Queue  2: Qlen=    0, Limit_Qlen=   64, HOL1=         0
  Queue  3: Qlen=    0, Limit_Qlen=   64, HOL1=         0
  Queue  4: Qlen=    0, Limit_Qlen=   64, HOL1=         0
  Queue  5: Qlen=    3, Limit_Qlen=  256, HOL1=         0
 Tail_drop=         0
  Queue  6: Qlen=    0, Limit_Qlen=   36, HOL1=         0
  Queue  7: Qlen=    0, Limit_Qlen=   64, HOL1=         0
  Queue  8: Qlen=    0, Limit_Qlen=   64, HOL1=         0
  Queue  9: Qlen=    0, Limit_Qlen=   64, HOL1=         0
  Queue 10: Qlen=    3, Limit_Qlen=  256, HOL1=         0
 Tail_drop=         0

Switch1 SW (outbound)
 Max_Queue=16
  Queue  1: Qlen=    0, Limit_Qlen=  192, HOL1=         0
  Queue  2: Qlen=    0, Limit_Qlen=  192, HOL1=         0
  Queue  3: Qlen=    0, Limit_Qlen=  192, HOL1=         0
  Queue  4: Qlen=    0, Limit_Qlen=  192, HOL1=         0
  Queue  5: Qlen=    0, Limit_Qlen=  192, HOL1=         0
  Queue  6: Qlen=    0, Limit_Qlen=  192, HOL1=         0
  Queue  7: Qlen=    0, Limit_Qlen=  192, HOL1=         0
  SQueue 1: Qlen=    0, Limit_Qlen=  192, HOL1=         0
 Tail_drop=         0
  Queue  8: Qlen=    0, Limit_Qlen=  192, HOL1=         0
  Queue  9: Qlen=    0, Limit_Qlen=  192, HOL1=         0
  Queue 10: Qlen=    0, Limit_Qlen=  192, HOL1=         0
  Queue 11: Qlen=    0, Limit_Qlen=  192, HOL1=         0
  Queue 12: Qlen=    0, Limit_Qlen=  192, HOL1=         0
  Queue 13: Qlen=    0, Limit_Qlen=  192, HOL1=         0
  Queue 14: Qlen=    0, Limit_Qlen=  192, HOL1=         0
  SQueue 2: Qlen=    0, Limit_Qlen=  192, HOL1=         0
```

```
 Tail_drop=         0
Switch1/NIF0/Port1 (outbound)
 Max_Queue=8, Rate_limit=100Mbit/s, Burst_size= -, Qmode=pq/tail_drop
  Queue  1: Qlen=     0, Limit_Qlen=   192, HOL1=    230925
  Queue  2: Qlen=     0, Limit_Qlen=   192, HOL1=         0
  Queue  3: Qlen=     0, Limit_Qlen=   192, HOL1=         0
  Queue  4: Qlen=     0, Limit_Qlen=   192, HOL1=         0
  Queue  5: Qlen=     0, Limit_Qlen=   192, HOL1=         0
  Queue  6: Qlen=     0, Limit_Qlen=   192, HOL1=         0
  Queue  7: Qlen=     0, Limit_Qlen=   192, HOL1=         0
  Queue  8: Qlen=     0, Limit_Qlen=   192, HOL1=         0
 Tail_drop=         0
           :
           :
           :
Switch1/NIF0/Port54 (outbound)
 Max_Queue=8, Rate_limit= -, Burst_size= -, Qmode=pq/tail_drop
  Queue  1: Qlen=     0, Limit_Qlen=   192, HOL1=         0
  Queue  2: Qlen=     0, Limit_Qlen=   192, HOL1=         0
  Queue  3: Qlen=     0, Limit_Qlen=   192, HOL1=         0
  Queue  4: Qlen=     0, Limit_Qlen=   192, HOL1=         0
  Queue  5: Qlen=     0, Limit_Qlen=   192, HOL1=         0
  Queue  6: Qlen=     0, Limit_Qlen=   192, HOL1=         0
  Queue  7: Qlen=     0, Limit_Qlen=   192, HOL1=         0
  Queue  8: Qlen=     0, Limit_Qlen=   192, HOL1=         0
 Tail_drop=         0
```

Display items

Table 31-2: Display items of the statistics

Item	Displayed information	
	Detailed information	**Meaning**
Interface information	Switch<switch no.>/NIF<nif no.>/Port<port no.> (outbound)	Port send queues
	Switch<switch no.> To-CPU (outbound)	Send queue for CPU
	Switch<switch no.> SW (outbound)	Send queues for traffic among internal LSIs (This item is displayed only on AX2340S-48T4X or AX2340S-48P4X.)
QoS information	Max_Queue=<number of queue>	Number of send queues
	Rate_limit=<rate>	Bandwidth set for the port • When auto-negotiation is unresolved (including when processing is in progress): -- is displayed. • When auto-negotiation has been resolved or the port bandwidth control is specified for the specified speed: The specified bandwidth is displayed. • When auto-negotiation has been resolved or the port bandwidth control is not specified for the specified speed: The line speed is displayed.
	Burst_size=<byte>	Burst size for port bandwidth control. • If port bandwidth control is enabled, the specified burst size is displayed. • If port bandwidth control is disabled, a hyphen (-) is displayed. For details about the port bandwidth control settings, see "Configuration Command Reference, traffic-shape rate".

Item	Displayed information	
	Detailed information	Meaning
	Qmode=<schedule name>/<drop name>	Scheduling (pq, 2pq+6drr)/drop control (tail_drop) For details on scheduling, see "Configuration Command Reference, qos-queue-list".
Queue information	Queue<queue no.>:	Send queue number#1
	SQueue<queue no.>:	System queue number
	Qlen=<queue length>	Number of buffers used by send queue
	Limit_Qlen=<queue length>	Maximum number of send queues
Queue statistics	HOL1=<packets> (HOL: Stands for head of line blocking.)	Number of packets discarded because: 1. There is no space in the send queue. (The queue length exceeds the drop threshold based on the queuing priority.)#2, #3, #4 2. There is no space in the packet buffer.#5
Port statistics	Tail_drop=<packets>	The number of packets discarded because the drop threshold for queuing priority 1 or 2 is exceeded#2, #3

#1

The send queue number of the send queue in which frames are queued is determined based on the CoS value for each frame.

#2

Some control packets are handled with a queuing priority other than 3.

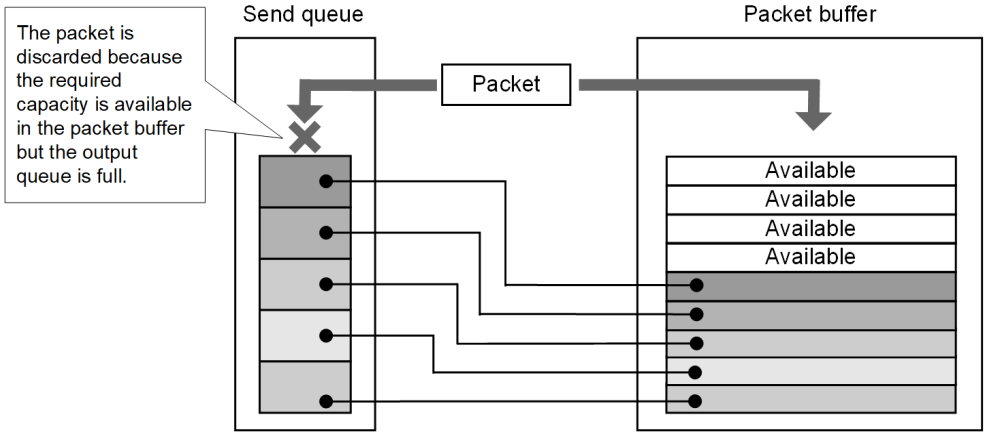
#3

If packets are dropped due to an exceeded drop threshold with queuing priority set to 1 or 2, the HOL1 and Tail_drop values are incremented.

#4

The following figure shows an overview of processing that discards packets because the send queue is full.

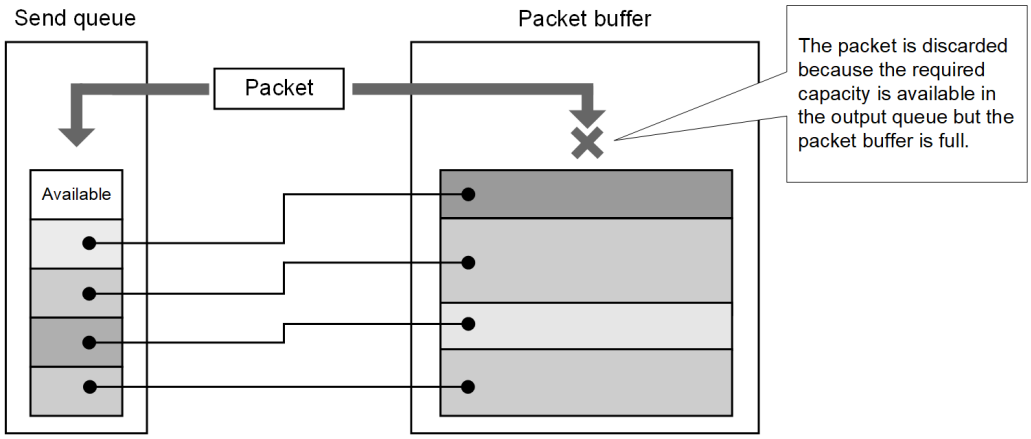
Figure 31-6: Overview of processing that discards packets because the send queue is full



#5

The following figure shows an overview of processing that discards packets because the packet buffer is full.

Figure 31-7: Overview of processing that discards packets because the packet buffer is full



Impact on communication

None

Notes

None

clear qos queueing

For the information displayed by the "show qos queueing" command, this command clears to 0 the number of packets (HOL1 and Tail_drop) that were not placed in the send queue and were discarded.

Syntax

```
clear qos queueing [ <switch no.>/<nif no.>/<port no.> ]
```

Input mode

User mode and administrator mode

Parameters

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

The number of packets discarded without being put into the send queue of the specified port is reset to 0. For the specifiable ranges of <switch no.>, <nif no.>, and <port no.> values, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

The number of packets discarded is reset to 0 for the following queues: the send queues of all ports on the device and the queue for sending packets to the CPU.

Example

Figure 31-8: Result of clearing the port statistics to zero

```
> clear qos queueing 1/0/3
Date 20XX/07/14 12:00:00 UTC
>
```

Display items

None

Impact on communication

None

Notes

1. If this command is executed, the MIB information of the axsEtherTxQoS and axsToCpuQoS groups is also cleared to zero.

32 IEEE 802.1X

show dot1x statistics

Shows statistics about IEEE 802.1X authentication.

Syntax

```
show dot1x statistics [{ port <port list> | channel-group-number <channel group list>}]
```

Input mode

User mode and administrator mode

Parameters

{ port <port list> | channel-group-number <channel group list>}

port <port list>

Displays statistics for the specified ports in list format.

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

channel-group-number <channel group list>

Displays statistics for the specified channel group in list format.

For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

Statistics for all the above types are displayed.

Example

Figure 32-1: Displaying statistics for all types of IEEE 802.1X authentication

```
> show dot1x statistics
Date 20XX/06/10 07:52:58 UTC
[EAPOL frames]
Port  1/0/2  TxTotal   :        42 TxReq/Id  :         5 TxReq     :        30
             TxSuccess :         5 TxFailure :         2 TxNotify  :         0
             RxTotal   :        47 RxStart   :        12 RxLogoff  :         0
             RxResp/Id :         5 RxResp    :        30 RxNotify  :         0
             RxInvalid :         0 RxLenErr  :         0
ChGr  10     TxTotal   :         0 TxReq/Id  :         0 TxReq     :         0
             TxSuccess :         0 TxFailure :         0 TxNotify  :         0
             RxTotal   :         0 RxStart   :         0 RxLogoff  :         0
             RxResp/Id :         0 RxResp    :         0 RxNotify  :         0
             RxInvalid :         0 RxLenErr  :         0

[EAPoverRADIUS frames]
Port  1/0/2  TxTotal   :         0 TxNakResp :         0 TxNoNakRsp:         0
             RxTotal   :         0 RxAccAccpt:         0 RxAccRejct:         0
             RxAccChllg:         0 RxInvalid :         0
ChGr  10     TxTotal   :         0 TxNakResp :         0 TxNoNakRsp:         0
             RxTotal   :         0 RxAccAccpt:         0 RxAccRejct:         0
             RxAccChllg:         0 RxInvalid :         0
>
```

Display items

Table 32-1: Display items for the statistics concerning IEEE 802.1X authentication

Item	Meaning	Displayed detailed information
Port/ChGr	Indicates the type of authentication. Port <switch no.>/<nif no.>/<port no.>: Indicates a port. ChGr <channel group number>: Indicates a channel group.	
[EAPOL frames]	Statistics for EAPOL frames. For details about the items, see the next and subsequent rows.	
TxTotal	The total number of EAPOL frames that have been sent	
TxReq/Id	The number of EAPOL Request/Identity frames that have been sent	
TxReq	The number of EAP Request frames (excluding Identity and Notification frames) that have been sent	
TxSuccess	The number of EAP Success frames that have been sent	
TxFailure	The number of EAP Failure frames that have been sent	
TxNotify	The number of EAP Request/Notification frames that have been sent	
RxTotal	The total number of EAPOL frames (excluding RxInvalid and RxLenErr frames) that have been received	
RxStart	The number of EAPOL Start frames that have been received	
RxLogoff	The number of EAPOL Logoff frames that have been received	
RxResp/Id	The number of EAP Response/Identity frames that have been received	
RxResp	The number of EAP Response frames (excluding Identity and Notification frames) that have been received	
RxNotify	The number of EAP Response/Notification frames that have been received	
RxInvalid	The number of invalid EAPOL frames that have been received (the number of discarded frames)	
RxLenErr	The number of invalid-length EAPOL frames that have been received (the number of discarded frames)	
[EAPoverRADIUS frames]	Statistics for EAPoverRADIUS frames. For details about the items, see the next and subsequent rows.	
TxTotal	The total number of EAPoverRADIUS frames that have been sent	
TxNakResp	The number of AccessRequest/EAP Response/NAK frames that have been sent	
TxNoNakRsp	The number of AccessRequest/EAP Response frames (excluding NAK frames) that have been sent	
RxTotal	The total number of EAPoverRADIUS frames that have been received	
RxAccAccpt	The number of AccessAccept/EAP Success frames that have been received	
RxAccRejct	The number of AccessReject/EAP Failure frames that have been received	
RxAccChllg	The number of AccessChallenge frames that have been received	

Item	Meaning	Displayed detailed information
RxInvalid	The number of invalid EAPoverRADIUS frames that have been received	

Impact on communication

None

Notes

None

show dot1x

Displays status information about IEEE 802.1X authentication.

Syntax

```
show dot1x [{ port <port list> | channel-group-number <channel group list>}] [detail]
```

Input mode

User mode and administrator mode

Parameters

{ port <port list> | channel-group-number <channel group list>}

port <port list>

Displays status information for the specified ports in list format.

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

channel-group-number <channel group list>

Displays status information for the specified channel group in list format.

For details about how to specify <channel group list>, see "Specifiable values for parameters".

detail

Displays detailed information. The status information about each supplicant (user) that has already been authenticated is displayed.

Behavior when all parameters are omitted:

The status information for the entire device is displayed.

Example

Figure 32-2: Displaying the status information for all types of IEEE 802.1X authentication

```
> show dot1x
Date 20XX/06/10 08:03:21 UTC
System 802.1X : Enable
   AAA Authentication Dot1x   : Enable
       Authorization Network  : Disable
       Accounting Dot1x       : Enable
   Auto-logout                : Enable

Port/ChGr         AccessControl    PortControl         Status       Supplicants
Port  1/0/2       Multiple-Auth    Auto                ---          1
ChGr  10          Multiple-Auth    Auto                ---          0
>
```

Figure 32-3: Displaying the detailed status information for all types of IEEE 802.1X authentication

```
> show dot1x detail
Date 20XX/06/10 06:24:27 UTC
System 802.1X : Enable
   AAA Authentication Dot1x   : Enable
       Authorization Network  : Disable
       Accounting Dot1x       : Enable
   Auto-logout                : Enable
Port  1/0/2
AccessControl  : Multiple-Auth            PortControl   : Auto
Status         : ---                      Last EAPOL    : 0012.e200.0011
Supplicants    : 1 / 1 / 1024             ReAuthMode    : Enable
TxTimer(s)     : ---   / 30               ReAuthTimer(s): 3484  / 3600
```

```
ReAuthSuccess  : 0                          ReAuthFail    : 0
SuppDetection  : Auto

 Supplicants MAC     Status         AuthState      BackEndState   ReAuthSuccess
 VLAN                Class          SessionTime(s) Date/Time
 0012.e200.0011      Authorized     Authenticated  Idle           0
 8                   0              118            20XX/06/10 06:22:29

ChGr  10
AccessControl  : Multiple-Auth              PortControl   : Auto
Status         : ---                        Last EAPOL    : 0000.0000.0000
Supplicants    : 0 / 0 / 1024               ReAuthMode    : Enable
TxTimer(s)     : ---   / 30                 ReAuthTimer(s): ---   / 3600
ReAuthSuccess  : 0                          ReAuthFail    : 0
SuppDetection  : Auto
>
```

Display items

Table 32-2: Display items for the status information about IEEE 802.1X authentication

Item		Meaning	Displayed detailed information
System 802.1X		Displays whether IEEE 802.1X authentication is enabled or disabled.	1. Enable (IEEE 802.1X authentication is enabled.) 2. Disable (IEEE 802.1X authentication is not operating.)
AAA	Authentication Dot1x	Displays whether authentication requests to RADIUS are enabled or disabled.	1. Enable (Authentication requests RADIUS are enabled.) 2. Disable (Authentication requests to RADIUS are disabled.)
	Authorization Network	This item is not used in the Switch.	
	Accounting Dot1x	Displays whether the accounting function is enabled or disabled.	1. Enable (The accounting function is enabled.) 2. Disable (The accounting function is disabled.)
Auto-logout		Indicates how automatic authentication cancellation by non-communication monitoring is working.	1. Enable (The non-communication monitoring function is enabled.) 2. Disable (The non-communication monitoring function is disabled)
Port/ChGr		Indicates the type of authentication. Port <switch no.>/<nif no.>/<port no.>: Port ChGr <channel group number>: Channel group number	
AccessControl		Displays the authentication submode set for the relevant type of authentication. -----: Indicates the single mode. Multiple-Hosts: Indicates the multi-mode. Multiple-Auth: Indicates the terminal authentication mode.	1. --- 2. Multiple-Hosts 3. Multiple-Auth
PortControl		Displays the authentication control setting. Auto: Authentication control is applied. Force-Authorized: Communication is always authorized. Force-Unauthorized: Communication is never authorized.	1. Auto 2. Force-Authorized 3. Force-Unauthorized

Item	Meaning	Displayed detailed information
Status	Displays the authentication status of the port. Authorized: Already authenticated. Unauthorized: Not authenticated. ---: Terminal authentication mode	1. Authorized 2. Unauthorized 3. ---
Last EAPOL	Displays the source MAC address of the last received EAPOL.	
Supplicants	Displays the number of supplicants that have already been authenticated or assigned for authentication. [For the entire device] The number of supplicants to be authenticated is displayed. [For each type of authentication] For single mode or multi-mode: <Number of authenticated supplicants> / <number of supplicants to be authenticated> For terminal authentication mode: <Number of authenticated supplicants> / <number of supplicants to be authenticated> / <maximum number of supplicants within an authentication type>	
ReAuthMode	Displays the status of the self-issuance of "EAPOL Request/ID" re-authentication requests.	1. Enable 2. Disable
TxTimer(s)	Displays the timer for sending "EAPOL Request/ID" authentication requests prior to authentication. ---: The timer on a Switch is disabled because any of the following applies: • The number of supplicants to be authenticated reached the maximum value for the authentication type. • A supplicant was authenticated even though the new terminal detection mode was in Disable. • The new terminal detection mode was in Auto. • The following authentication types are disabled: Port or a channel group to be authenticated <current timer value> / <tx_period seconds>	
ReAuthTimer(s)	Displays the timer for sending "EAPOL Request/ID" re-authentication requests after a successful authentication. ---: The timer is disabled because authentication has not been successful. <current timer value> / <reauth_period seconds>	
ReAuthSuccess	The number of times that re-authentication has been successful	
ReAuthFail	The number of times that re-authentication has failed	
KeepUnauth	The authentication status was changed to the unauthenticated state because multiple terminals were detected on a single mode port. The time is displayed in seconds, and indicates how long the terminal remained in this status waiting for authentication processing to become available again. ---: The timer is disabled because the port is functioning properly. <current timer value> / <keepunauth_period seconds>	
SuppDetection	(For terminal authentication mode only) This item displays the mode for detecting a new terminal. Disable: The detection of new terminals is stopped. Full: Complete search mode Shortcut: Omission mode Auto: Automatic detection mode	1. Disable 2. Full 3. Shortcut 4. Auto

Item	Meaning	Displayed detailed information
Supplicant MAC	The supplicant's MAC address. Supplicants with an asterisk (*) on the left are being quarantined.	
Status	Displays the authentication status of the supplicant. Authorized: Already authenticated. Unauthorized: Not authenticated.	1. Authorized 2. Unauthorized
AuthState	Displays the status of authentication processing for the supplicant. Connecting: The supplicant is connecting. Authenticating: Authentication is in progress. Authenticated: Authentication has been completed. Aborting: Authentication processing has stopped. Held: The authentication request has been rejected.	1. Connecting 2. Authenticating 3. Authenticated 4. Aborting 5. Held
BackEndState	Displays the status of authentication processing for the supplicant by the RADIUS server. Idle: The supplicant is waiting for processing. Response: The supplicant is responding to the server. Request: A request is being sent to the supplicant. Success: Authentication processing has finished successfully. Fail: The authentication processing failed. Timeout: A timeout occurred during an attempt to connect to the server.	1. Idle 2. Response 3. Request 4. Success 5. Fail 6. Timeout
ReAuthSuccess	Displays the number of times re-authentication was successful.	
VLAN	Post-authentication VLAN of the supplicant It appears blank when authentication is not completed.	
Class	Indicates the user class of the supplicant. "-" is displayed in the first step of multistep authentication or while quarantine is in progress.	
SessionTime	Displays the time (in seconds for each supplicant) required to establish a session after a successful authentication.	
Date/Time	Displays the time that authentication of the supplicant was successful.	

Impact on communication

None

Notes

None

clear dot1x statistics

Clears the IEEE 802.1X authentication statistics to zero.

Syntax

```
clear dot1x statistics [{ port <port list> | channel-group-number <channel group list>}]
```

Input mode

User mode and administrator mode

Parameters

{ port <port list> | channel-group-number <channel group list>}

port <port list>

Clears statistics for the specified ports in list format to zero.

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

channel-group-number <channel group list>

Clears statistics for the specified channel group numbers in list format to zero.

For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

Statistics for all types of authentication are cleared to zero.

Example

Figure 32-4: Clearing the IEEE 802.1X authentication statistics to zero

```
> clear dot1x statistics
>
```

Display items

None

Impact on communication

None

Notes

- If this command is executed, the MIB information of the IEEE 802.1X MIB group is also cleared to zero.
- Executing this command also clears the Last EAPOL item (source MAC address of the last EAPOL frame received) of the "show dot1x" command.

clear dot1x auth-state

Initializes the IEEE 802.1X authentication status.

Syntax

```
clear dot1x auth-state [{ port <port list> | channel-group-number <channel group list> | suppli
cant-mac <mac address> }] [-f]
```

Input mode

User mode and administrator mode

Parameters

{ port <port list> | channel-group-number <channel group list> | supplicant-mac <mac address> }

port <port list>

Initializes the authentication status for the ports specified in list format. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters".

channel-group-number <channel group list>

Initializes the authentication status for the channel groups specified in list format. For details about how to specify <channel group list>, see "Specifiable values for parameters".

supplicant-mac <mac address>

Initializes the authentication status for the specified MAC address.

-f

Initializes the authentication status without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Behavior when all parameters are omitted:

After the confirmation message for initialization is displayed, all the IEEE 802.1X authentication statuses are initialized.

Example

Figure 32-5: Initializing all the IEEE 802.1X authentication status on a device

```
> clear dot1x auth-state
Initialize all 802.1X Authentication Information. Are you sure? (y/n) :y
>
```

Display items

None

Impact on communication

If initialization is performed, the IEEE 802.1X authentication status on the relevant ports is initialized, and communication is lost. To restore communication, re-authentication is necessary.

Notes

When the authentication status is initialized, an EAP-Failure or EAP-Req/Id frame might be sent according to the specified parameter.

- If the parameter is omitted, EAP-Failure and EAP-Req/Id frames are multicasted once to all types of IEEE 802.1X authentication in a device.
- If the parameter is port <port list> or channel-group-number <channel group list>, EAP-Failure and EAP-Req/Id frames are multicast once to the specified type of IEEE 802.1X authentication.
- If the parameter is supplicant-mac <mac address>, an EAP-Failure frame is unicast to the specified authentication terminal. If there is no authentication terminal under the IEEE 802.1X authentication to which the specified authentication terminal belongs, an EAP-Req/Id frame is multicasted once to the type of IEEE 802.1X authentication to which the specified authentication terminal belongs.

reauthenticate dot1x

Re-authenticates the status of IEEE 802.1X authentication. Even if re-authentication timer (reauth-period) is 0 (disabled), re-authentication is forcibly performed.

Syntax

```
reauthenticate dot1x [{ port <port list> | channel-group-number <channel group list> | supplicant-mac <mac address> }] [-f]
```

Input mode

User mode and administrator mode

Parameters

{ port <port list> | channel-group-number <channel group list> | supplicant-mac <mac address> }

port <port list>

Re-authenticates the authentication status for the ports specified in list format. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters".

channel-group-number <channel group list>

Re-authenticates the authentication status for the channel groups specified in list format. For details about how to specify <channel group list>, see "Specifiable values for parameters".

supplicant-mac <mac address>

Re-authenticates the authentication status of the specified MAC address.

-f

Initiates re-authentication without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Behavior when all parameters are omitted:

After the confirmation message for re-authentication is displayed, all the IEEE 802.1X authentication statuses are re-authenticated.

Example

Figure 32-6: Re-authenticating all the IEEE 802.1X-authenticated ports on a device

```
> reauthenticate dot1x
Reauthenticate all 802.1X ports and vlans. Are you sure? (y/n) :y
>
```

Display items

None

Impact on communication

When re-authentication is initiated, no problems with communication arise if re-authentication is successful. If re-authentication fails, however, communication will be lost.

Notes

None

restart dot1x

Restarts the IEEE 802.1X program.

Syntax

```
restart dot1x [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the IEEE 802.1X program without displaying a restart confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

When the IEEE 802.1X program is restarted, the core file of the program is output.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

After the restart confirmation message is output, the IEEE 802.1X program is restarted.

Example

Figure 32-7: Restarting the IEEE 802.1X program

```
> restart dot1x
802.1X restart OK?  (y/n) : y
>
```

Figure 32-8: Restarting the IEEE 802.1X program (with the –f parameter specified)

```
> restart dot1x -f
>
```

Display items

None

Impact on communication

All the IEEE 802.1X authentication statuses on a device are initialized and communication is lost. To restore communication, re-authentication is necessary.

Notes

The storage directory and the name of the core file are as follows:

Storage directory: /usr/var/core

Core file: dot1xd.core

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

dump protocols dot1x

Outputs the control table information and detailed statistics gathered by the IEEE 802.1X program to a file.

Syntax

```
dump protocols dot1x
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 32-9: Taking an online dump of the IEEE 802.1X program

```
> dump protocols dot1x
>
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of the dump file are as follows:

Storage directory: /usr/var/dot1x

Dump file: dot1x_dump.gz

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

show dot1x logging

Displays action log messages collected by the IEEE 802.1X program.

Syntax

```
show dot1x logging [{ error | warning | notice | info }]
```

Input mode

User mode and administrator mode

Parameters

{error | warning | notice | info}

Specify the level of action log message to be displayed. Of the output messages, only logs whose priority level is higher than the level specified by the "dot1x loglevel" configuration command are displayed.

Note, however, that if notice is specified, NORMAL level log messages are also displayed.

If info is specified, all log messages are displayed.

Behavior when this parameter is omitted:

The same action log messages as those displayed when info is specified are displayed.

Example

Figure 32-10: Displaying IEEE 802.1X action log messages

```
> show dot1x logging
Date 20XX/06/10 07:36:05 UTC
No=1:Jun 10 07:34:24:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=1/0/2 VLAN=13 Login succeeded. ; New
 Supplicant Auth Success.
No=11:Jun 10 07:33:40:NORMAL:LOGOUT: MAC=0012.e200.0001 PORT=1/0/2 VLAN=13 Force logout. ; "cle
ar dot1x auth-state" command succeeded.
No=1:Jun 10 07:28:47:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=1/0/2 VLAN=13 Login succeeded. ; New
 Supplicant Auth Success.
```

Display items

The following shows the display format of a message:

```
No=10:Dec  1 10:09:50:NORMAL:LOGOUT: MAC=0012.e200.0001 PORT=0/1 VLAN=3 Logout succeeded.
 (1)   (2)     (3)     (4)    (5)                (6)                          (7)
```

(1) Message number: Indicates the number assigned to each message shown in "Table 32-5: List of action log messages".

(2) Date: Indicates the date recorded in the IEEE 802.1X program.

(3) Time: Indicates the time recorded in the IEEE 802.1X program.

(4) Log ID: Indicates the level of the action log message.

(5) Log type: Indicates the type of operation that outputs the log message.

(6) Additional information: Indicates supplementary information provided in the message.

(7) Message body

Action log messages show the following information:

- Log ID: "Table 32-3: Log ID and type of action log messages"
- Log type: "Table 32-3: Log ID and type of action log messages"

- Additional information: "Table 32-4: Additional information"
- List of messages: "Table 32-5: List of action log messages"

Table 32-3: Log ID and type of action log messages

Log ID	Log type	Meaning
NORMAL	LOGIN	Indicates that login was successful.
	LOGOUT	Indicates that logout was successful.
	SYSTEM	Indicates a runtime notification.
NOTICE	LOGIN	Indicates that authentication failed.
	LOGOUT	Indicates that logout failed.
WARNING	SYSTEM	Indicates alternative behavior in case of communication failure, or a communication failure.
ERROR	SYSTEM	Indicates a failure while IEEE 802.1X program is running.

Table 32-4: Additional information

Display format	Meaning
MAC=xxxx.xxxx.xxxx	Indicates the MAC address.
VLAN=xxxx	Indicates the VLAN ID. Note, however, that this is not displayed if VLAN ID information could not be acquired.
PORT=xx/xx/xx CHGR=xx	Indicates the port number or channel group number. Note, however, that this information is not displayed if port information could not be acquired.
ServerIP=xxx.xxx.xxx.xxx	Indicates the server IP address.
ServerIPv6=xxxx::xxxx:xxxx	Indicates the server IPv6 address.
ServerName=cccccc	Indicates the server name.

Table 32-5: List of action log messages

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
1	NORMAL	LOGIN	Login succeeded. ; New Supplicant Auth Success.
	A new supplicant was authenticated successfully. [Action] None.		
	MAC address, port number or channel group number, VLAN ID		
2	NORMAL	LOGIN	Login succeeded. ; Supplicant Re-Auth Success.
	A supplicant was re-authenticated successfully. [Action] None.		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
	MAC address, port number or channel group number, VLAN ID		
3	NORMAL	LOGIN	Login succeeded. ; Limited by ACL.
	A supplicant was authenticated, but a pre-authentication filter is enabled. [Action] Clear the quarantine conditions.		
	MAC address, port number or channel group number, VLAN ID		
10	NORMAL	LOGOUT	Logout succeeded.
	Authentication has been canceled by a request from the supplicant or because the terminal was moved. [Action] None.		
	MAC address, port number or channel group number, VLAN ID		
11	NORMAL	LOGOUT	Force logout. ; "clear dot1x auth-state" command succeeded.
	Authentication has been canceled by a command. [Action] None.		
	MAC address, port number or channel group number, VLAN ID		
13	NORMAL	LOGOUT	Force logout. ; The supplicant was cleared, because it was registered to mac-address-table with the configuration.
	An attempt to authenticate the relevant supplicant was canceled because the MAC address was configured for the MAC address table. [Action] None.		
	MAC address, port number or channel group number, VLAN ID		
14	NORMAL	LOGOUT	Force logout. ; The status of port was changed to Unauthorized, because another supplicant was detection in single mode.
	The authentication status has been changed to Unauthorized because multiple supplicants were detected on a single mode port. [Action] None.		
	MAC address, port number or channel group number, VLAN ID		
15	NORMAL	LOGOUT	Force logout. ; Dot1x configuration deleted.
	Authentication has been canceled because the IEEE 802.1X authentication configuration was deleted. [Action] If you want to use IEEE 802.1X authentication, set the configuration.		
	MAC address, port number or channel group number, VLAN ID		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
16	NORMAL	LOGOUT	Force logout. ; Port link down.
	Authentication has been canceled because the port is in link-down state. [Action] None.		
	MAC address, port number or channel group number, VLAN ID		
17	NORMAL	LOGOUT	Force logout. ; VLAN status down.
	Authentication has been canceled because the VLAN has gone down or the relevant VLAN is not set up in the configuration of the port. [Action] None.		
	MAC address, port number or channel group number, VLAN ID		
18	NORMAL	LOGOUT	Force logout. ; Re-Auth failed.
	Re-authentication processing failed. [Action] None.		
	MAC address, port number or channel group number, VLAN ID		
19	NORMAL	LOGOUT	Force logout. ; Could not be registered to hardware.
	Authentication has been canceled because registration of a supplicant in the hardware failed. [Action] If this message appears frequently, use the "restart dot1x" command to restart the IEEE 802.1X program.		
	MAC address, port number or channel group number, VLAN ID		
20	NOTICE	LOGIN	Login failed. ; Failed to authenticate the supplicant because MAC authentication reject.
	Authentication failed because MAC-based authentication failed in multistep authentication. [Action] Set the target MAC address on the RADIUS server.		
	MAC address, port number or channel group number, VLAN ID		
21	NORMAL	LOGOUT	Force logout. ; Multi-step finished.
	IEEE 802.1X authentication was canceled in response to the completion of multistep authentication. [Action] None.		
	MAC address, port number or channel group number, VLAN ID		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
22	NORMAL	LOGOUT	Force logout. ; Authentic method changed.
	Multistep authentication settings for the target port were changed. [Action] None.		
	MAC address, port number or channel group number, VLAN ID		
23	NORMAL	LOGOUT	Force logout. ; Mac-address-table aging.
	Authentication was canceled because a MAC address was deleted due to MAC address table aging. [Action] The terminal is not in use. Check the terminal.		
	MAC address, port number or channel group number, VLAN ID		
30	NOTICE	LOGIN	Login failed. ; RADIUS authentication failed.
	Authentication of a new supplicant failed. [Action] Correctly set the user name and password sent from the supplicant and the user settings of the RADIUS server.		
	MAC address, port number or channel group number, VLAN ID		
31	NOTICE	LOGIN	Login failed. ; RADIUS authentication failed. (Re-Auth)
	Re-authentication of a supplicant failed. [Action] Correctly set the user name and password sent from the supplicant and the user settings of the RADIUS server.		
	MAC address, port number or channel group number, VLAN ID		
33	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: No Tunnel-Type Attribute.)
	Assignment of a post-authentication VLAN failed because there was no Tunnel-Type attribute. [Action] Set the Tunnel-Type attribute in the Accept packet to be sent by the RADIUS server.		
	MAC address, port number or channel group number		
34	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Tunnel-Type Attribute is not VLAN(13).)
	Assignment of a post-authentication VLAN failed because the value of the Tunnel-Type attribute was not VLAN(13). [Action] Set the Tunnel-Type attribute in the Accept packet to be sent by the RADIUS server to VLAN(13).		
	MAC address, port number or channel group number		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
35	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: No Tunnel-Medium-Type Attribute.)
	Assignment of a post-authentication VLAN failed because there was no Tunnel-Medium-Type attribute. [Action] Set the Tunnel-Medium-Type attribute in the Accept packet to be sent by the RADIUS server.		
	MAC address, port number or channel group number		
36	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Tunnel-Medium-Type Attribute is not IEEE802(6).)
	Assignment of a post-authentication VLAN failed because the value of the Tunnel-Medium-Type attribute was not IEEE 802(6). [Action] Set the Tunnel-Medium-Type attribute in the Accept packet to be sent by the RADIUS server to IEEE 802(6).		
	MAC address, port number or channel group number		
37	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: No Tunnel-Private-Group-ID Attribute.)
	Assignment of a post-authentication VLAN failed because there was no Tunnel-Private-Group-ID attribute. [Action] Set the Tunnel-Private-Group-ID attribute in the Accept packet to be sent by the RADIUS server.		
	MAC address, port number or channel group number		
38	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Invalid Tunnel-Private-Group-ID Attribute.)
	Assignment of a post-authentication VLAN failed because an invalid value was set for the Tunnel-Private-Group-ID attribute. [Action] Check the setting of the Tunnel-Private-Group-ID attribute in the Accept packet to be sent by the RADIUS server.		
	MAC address, port number or channel group number		
39	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The VLAN ID is out of range.)
	Assignment of a post-authentication VLAN failed because the VLAN ID was not in the normal range. [Action] Check the range of the VLAN IDs set for the Tunnel-Private-Group-ID attribute in the Accept packet to be sent by the RADIUS server.		
	MAC address, port number or channel group number, VLAN ID		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
40	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The Port doesn't belong to VLAN.)
	The post-authentication VLAN sent from the RADIUS server does not exist, or it is not a MAC VLAN. Alternatively, the post-authentication VLAN sent from the RADIUS server is not included in the vlan parameter of the "switchport mac" configuration command set for the authentication port. [Action] Check the VLAN IDs set for the Tunnel-Private-Group-ID attribute in the Accept packet to be sent by the RADIUS server.		
	MAC address, port number or channel group number, VLAN ID		
42	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The VLAN status is disabled.)
	Assignment of a post-authentication VLAN failed because the VLAN is in disable status. [Action] Execute the "state" configuration command to set the status of the VLAN to be assigned to active.		
	MAC address, port number or channel group number, VLAN ID		
43	NOTICE	LOGIN	Login failed. ; The number of supplicants on the switch is full.
	Authentication was not available because there were too many supplicants for the device. [Action] Attempt authentication again when the total number of authenticated supplicants falls below the capacity limit.		
	MAC address, port number or channel group number, VLAN ID		
44	NOTICE	LOGIN	Login failed. ; The number of supplicants on the interface is full.
	Authentication was not available because there were too many supplicants on the interface. [Action] Attempt authentication again when the number of authenticated supplicants on the interface falls below the capacity limit.		
	MAC address, port number or channel group number, VLAN ID		
45	NOTICE	LOGIN	Login failed. ; Failed to authenticate the supplicant because it could not be registered to mac-address-table.(code=x)
	Authentication failed because the registration of a supplicant in the MAC address table failed. [Action] If the total number of supplicants to be authenticated including other types of authentication exceeds the capacity limit of a device or the set maximum number of authentication terminals, perform authentication again when the number of authenticated supplicants goes below the capacity limit.		
	MAC address, port number or channel group number, VLAN ID		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
46	NOTICE	LOGIN	Login failed. ; Failed to authenticate the supplicant because it could not be registered to MAC VLAN.(code=x)
	Authentication failed because the registration of a supplicant in the MAC VLAN failed. [Action] If the total number of supplicants to be authenticated including other types of authentication exceeds the capacity limit of a device or the set maximum number of authentication terminals, perform authentication again when the number of authenticated supplicants goes below the capacity limit. In addition, make sure that the supplicants have not been authenticated by any other methods.		
	MAC address, port number or channel group number, VLAN ID		
47	NOTICE	LOGIN	Login failed. ; Failed to connect to RADIUS server.
	Authentication failed because an attempt to connect to the RADIUS server failed. [Action] Check the following: • Communication between the Switch and the RADIUS server is available. • The RADIUS server function is enabled.		
	MAC address, port number or channel group number, VLAN ID		
48	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Could not be registered to hardware.)
	Authentication failed because registration of a supplicant in the hardware failed. [Action] If this message appears frequently, use the "restart dot1x" command to restart the IEEE 802.1X program.		
	MAC address, port number or channel group number, VLAN ID		
80	WARNING	SYSTEM	Invalid EAPOL frame received.
	An invalid EAPOL frame has been received. [Action] Check whether there is any problem with the following: • The contents of EAPOL frames sent by the supplicant • Transmission line quality		
	—		
81	WARNING	SYSTEM	Invalid EAP over RADIUS frame received.
	An invalid EAP over RADIUS frame has been received. [Action] Check whether there is any problem with the following: • The contents of packets sent by the RADIUS server • Transmission line quality		
	—		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
82	WARNING	SYSTEM	Failed to connect to RADIUS server.
	An attempt to connect to the RADIUS server failed. [Action] Check the following: • Communication between the Switch and the RADIUS server is available. • The RADIUS server function is enabled.		
	Server IP address		
83	WARNING	SYSTEM	Failed to connect to RADIUS server.
	An attempt to connect to the RADIUS server failed. [Action] Check the following: • Communication between the Switch and the RADIUS server is available. • The RADIUS server function is enabled.		
	Server IPv6 address		
84	WARNING	SYSTEM	Failed to connect to Accounting server.
	An attempt to connect to the accounting server failed. [Action] Check the following: • Communication between the Switch and the accounting server is available. • The accounting server function is enabled.		
	Server IP address		
85	WARNING	SYSTEM	Failed to connect to Accounting server.
	An attempt to connect to the accounting server failed. [Action] Check the following: • Communication between the Switch and the accounting server is available. • The accounting server function is enabled.		
	Server IPv6 address		
86	WARNING	SYSTEM	Failed in the name resolution with the DNS server.
	Name resolution by the DNS server failed. [Action] Execute the "radius-server host" configuration command with the IP address of the server specified to change the setting to the IP address.		
	Server name		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
87	WARNING	SYSTEM	Invalid user class. [class]
	An invalid user class was set on the RADIUS server. [Action] Check the RADIUS server setting.		
	—		
90	ERROR	SYSTEM	Failed to open socket.
	An attempt to open a socket has failed. [Action] If this message appears frequently, use the "restart dot1x" command to restart the IEEE 802.1X program.		
	—		

Legend: —: Not applicable

Impact on communication

None

Notes

None

clear dot1x logging

Clears action log messages collected by the IEEE 802.1X program.

Syntax

```
clear dot1x logging
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 32-11: Clearing IEEE 802.1X action log messages

```
> clear dot1x logging
>
```

Display items

None

Impact on communication

None

Notes

None

33 Web Authentication

set web-authentication user

Adds a user for Web authentication. At this time, specify the VLAN to which the user belongs.

To apply the change to the authentication information, execute the "commit web-authentication" command.

Syntax

```
set web-authentication user <user name> <password> <vlan id>
```

Input mode

Administrator mode

Parameters

<user name>
Specify a user name to be registered.

Only alphanumeric characters can be used, and the characters are case sensitive. Specify it with 1 to 128 characters.

<password>
Specify a password.

Only alphanumeric characters can be used, and the characters are case sensitive. Specify it with 1 to 32 characters.

<vlan id>
For details about the specifiable range of values, see "Specifiable values for parameters". Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

- When the dynamic VLAN mode is used

  Specify the VLAN ID of the VLAN to which the user will move after authentication.

- When the fixed VLAN mode is used

  Specify a VLAN ID.

Example

When "USER01" is added as the user name, "user0101" as the password, and "10" as the VLAN ID:

```
# set web-authentication user USER01 user0101 10
```

Display items

None

Impact on communication

None

Notes

- This command cannot be used concurrently by multiple users.
- The settings are available as authentication information only after the "commit web-authentication" command has been executed.

set web-authentication passwd

Changes the password of a Web-authenticated user.

To apply the change to the authentication information, execute the "commit web-authentication" command.

Syntax

```
set web-authentication passwd <user name> <old password> <new password>
```

Input mode

Administrator mode

Parameters

<user name>

Specify the user name of the user whose password is to be changed.

Only alphanumeric characters can be used, and the characters are case sensitive. Specify it with 1 to 128 characters.

<old password>

Specify the password before the change.

Only alphanumeric characters can be used, and the characters are case sensitive. Specify it with 1 to 32 characters.

<new password>

Specify the password after the change.

Only alphanumeric characters can be used, and the characters are case sensitive. Specify it with 1 to 32 characters.

Example

To change the password for user "USER01":

```
# set web-authentication passwd USER01 user0101 user1111
```

Display items

None

Impact on communication

None

Notes

- This command cannot be used concurrently by multiple users.
- The settings are available as authentication information only after the "commit web-authentication" command has been executed.

set web-authentication vlan

Changes the VLAN to which a Web-authenticated user belongs.

To apply the change to the authentication information, execute the "commit web-authentication" command.

Syntax

```
set web-authentication vlan <user name> <vlan id>
```

Input mode

Administrator mode

Parameters

<user name>

Specify the user name of the user for which the VLAN is being changed.

Only alphanumeric characters can be used, and the characters are case sensitive. Specify it with 1 to 128 characters.

<vlan id>

Specify the VLAN ID of the VLAN to be changed.

For details about the specifiable range of values, see "Specifiable values for parameters". Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

Example

To change the VLAN to which user "USER01" belongs to 30:

```
# set web-authentication vlan USER01 30
```

Display items

None

Impact on communication

None

Notes

- This command cannot be used concurrently by multiple users.
- The settings are available as authentication information only after the "commit web-authentication" command has been executed.

remove web-authentication user

Deletes a user for Web authentication.

To apply the change to the authentication information, execute the "commit web-authentication" command.

Syntax

```
remove web-authentication user {<user name> | -all} [-f]
```

Input mode

Administrator mode

Parameters

<user name>

Deletes the specified user.

Only alphanumeric characters can be used, and the characters are case sensitive. Specify it with 1 to 128 characters.

-all

Deletes all users.

-f

Deletes the user without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example

- To delete the user "USER01":
```
# remove web-authentication user USER01
Remove web-authentication user.  Are you sure? (y/n): y
```
- To delete all users registered in the local authentication data:
```
# remove web-authentication user -all
Remove all web-authentication user.  Are you sure? (y/n): y
```

Display items

None

Impact on communication

None

Notes

The settings are available as authentication information only after the "commit web-authentication" command has been executed.

show web-authentication user

Displays user information registered on the device used for Web authentication. This command can also display user information that is being entered or edited by using the following commands:

- set web-authentication user
- set authentication passwd
- set authentication vlan
- remove web-authentication user

User information is displayed in ascending order of user name.

Syntax

```
show web-authentication user {edit | commit}
```

Input mode

Administrator mode

Parameters

{edit | commit}

edit

Displays user information being edited.

commit

Displays operating user information.

Example

- To display the user information being edited:

```
# show web-authentication user edit
 Date 20XX/10/14 10:52:49 UTC
 Total user counts:2
 VLAN username
    3 0123456789012345
 4091 USER01
```

- To display the information of the user who is performing operation:

```
# show web-authentication user commit
 Date 20XX/10/14 10:52:49 UTC
 Total user counts:3
 VLAN username
    4 0123456789012345
 4094 USER02
    2 USER03
```

Display items

Table 33-1: Display items of users registered for Web authentication

Item	Meaning	Displayed detailed information
Total user counts	Total number of registered users	The number of registered users

Item	Meaning	Displayed detailed information
VLAN	VLAN	The VLAN set for the registered user
username	User name	A registered user name

Impact on communication

None

Notes

None

show web-authentication login

Displays the users currently logged in (users that have already been authenticated) in ascending order by log-in date and time.

Syntax

```
show web-authentication login
```

Input mode

Administrator mode

Parameters

None

Example

The following commands show examples of displaying authenticated users:

- When only users whose authentication mode is the dynamic VLAN mode have logged in

```
# show web-authentication login
Date 20XX/06/10 08:14:42 UTC
Dynamic-VLAN total user counts:1
F Username
  VLAN    Class   MAC address      Login time               Limit time
  USER01
  4089    63      0012.e268.7527   20XX/06/10 08:13:38 UTC  00:58:56

Static-VLAN total user counts:0
```

- When only users whose authentication mode is the fixed VLAN mode have logged in

```
# show web-authentication login
Date 20XX/06/10 03:38:06 UTC
Dynamic-VLAN total user counts:0

Static-VLAN total user counts:1
F Username
  VLAN    Class   MAC address      Port    IP address
  Login time               Limit time
  USER16
  4089    63      0012.e268.7527   1/0/2   192.168.14.2
  20XX/06/10 03:37:49 UTC  00:59:43
```

- When users whose authentication mode is the dynamic VLAN mode or the fixed VLAN mode have logged in

```
# show web-authentication login
Date 20XX/06/10 03:38:06 UTC
Dynamic-VLAN total user counts:1
F Username
  VLAN    Class   MAC address      Login time               Limit time
  USER01
  4088    63      0012.e268.7526   20XX/06/10 08:13:38 UTC  00:58:56

Static-VLAN total user counts:1
F Username
  VLAN    Class   MAC address      Port    IP address
  Login time               Limit time
  USER16
  4089    63      0012.e268.7527   1/0/2   192.168.14.2
  20XX/06/10 03:37:49 UTC  00:59:43
```

Display items

Table 33-2: Items displayed for authenticated users

Item	Meaning	Displayed detailed information
Dynamic-VLAN total user counts	Total number of users in dynamic VLAN mode	The number of the authenticated, currently logged-in users in dynamic VLAN mode
Static-VLAN total user counts	Total number of users in fixed VLAN mode	The number of the authenticated, currently logged-in users in fixed VLAN mode
F	Forced authentication indication	Forcibly authenticated terminals *: Indicates that the terminal was forcibly authenticated.
Username	User name	The user names of the authenticated, currently logged-in users
VLAN	VLAN	The VLANs set for the authenticated, currently logged-in users
Class	User class	Displays the user class.
MAC address	MAC address	The MAC addresses of the authenticated, currently logged-in users
Port	Port number or channel group number	The port number of the port accommodating the authenticated, currently logged-in user, or the channel group number (displayed in fixed VLAN mode) <switch no.>/<nif no.>/<port no.>: Indicates the port number. CH:<channel group number>: Indicates the channel group number.
IP address	IP address	The IP addresses of the authenticated, currently logged-in users (displayed for fixed VLAN mode)
Login time	Login date and time	The login times of the authenticated, currently logged-in users
Limit time	Remaining login time	The remaining login times of the authenticated, currently logged-in users. When a user is logged in, the remaining time might be displayed as 00:00:00 immediately before the user is logged out due to a timeout. When the maximum connection time is 10 to 1440 minutes: hh:mm:ss hour:minute:second When the maximum connection time is set to infinity: infinity

Impact on communication

None

Notes

None

show web-authentication logging

Displays action log messages collected by the Web authentication program.

Syntax

```
show web-authentication logging [user]
```

Input mode

Administrator mode

Parameters

user

Specify the type of action log message to be displayed.

If this parameter is specified, user authentication information is displayed.

Behavior when this parameter is omitted:

The action log of the Web authentication program and the user authentication information is displayed in chronological order.

Example

- When the parameter is omitted:

```
# show web-authentication logging
Date 20XX/06/10 03:35:56 UTC
No=82:Jun 10 03:35:45:NORMAL:SYSTEM: Accepted clear auth-state command.
No=2:Jun 10 03:34:39:NORMAL:LOGOUT: MAC=0012.e200.0001 USER=USER01 IP=192.168.14.2 PORT=1/0
/2 VLAN=4089 Logout succeeded.
No=1:Jun 10 02:36:23:NORMAL:LOGIN: MAC=0012.e200.0001 USER=USER01 IP=192.168.14.2 PORT=1/0/
2 VLAN=4089 Login succeeded.
```

- When "user" is specified for the parameter:

```
# show web-authentication logging user
Date 20XX/06/10 03:36:08 UTC
No=2:Jun 10 03:34:39:NORMAL:LOGOUT: MAC=0012.e200.0001 USER=USER01 IP=192.168.14.2 PORT=1/0
/2 VLAN=4089 Logout succeeded.
No=1:Jun 10 02:36:23:NORMAL:LOGIN: MAC=0012.e200.0001 USER=USER01 IP=192.168.14.2 PORT=1/0/
2 VLAN=4089 Login succeeded.
```

Display items

The following shows the display format of a message:

```
No=1:Nov 15 00:09:50:NORMAL:LOGIN: MAC=0012.e200.0001 USER=testdata1 Login succeeded.
(1)   (2)     (3)     (4)    (5)              (6)                          (7)
```

(1) Message number: Indicates the number assigned to each message shown in "Table 33-5: List of action log messages".

(2) Date: Indicates the date recorded in the Web authentication program.

(3) Time: Indicates the time recorded in the Web authentication program.

(4) Log ID: Indicates the level of the action log message.

(5) Log type: Indicates the type of operation that outputs the log message.

(6) Additional information: Indicates supplementary information provided in the message.

(7) Message body

Action log messages show the following information:

- Log ID: "Table 33-3: Log ID and type of action log messages"
- Log type: "Table 33-3: Log ID and type of action log messages"
- Additional information: "Table 33-4: Additional information"
- List of messages: "Table 33-5: List of action log messages"

Table 33-3: Log ID and type of action log messages

Log ID	Log type	Meaning
NORMAL	LOGIN	Indicates that login was successful.
	LOGOUT	Indicates that logout was successful.
	SYSTEM	Indicates a runtime notification.
NOTICE	LOGIN	Indicates that authentication failed.
	LOGOUT	Indicates that logout failed.
	SYSTEM	Indicates alternative behavior in case of communication failure.
ERROR	SYSTEM	Indicates a communication failure or a failure while the Web authentication program is running.

Table 33-4: Additional information

Display format	Meaning
MAC=xxxx.xxxx.xxxx	Indicates the MAC address.
USER=xxxxxxxxxx	Indicates the user ID.
IP=xxx.xxx.xxx	Indicates the IP address.
VLAN=xxxx	Indicates the VLAN ID. Note, however, that this is not displayed if VLAN ID information could not be acquired.
PORT=xx/xx/xx CHGR=xx	Indicates the port number or channel group number. Note, however, that this information is not displayed if port information could not be acquired.

Table 33-5: List of action log messages

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
1	NORMAL	LOGIN	Login succeeded.
	The client was successfully authenticated. [Action] None.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
2	NORMAL	LOGOUT	Logout succeeded.

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
	The client successfully canceled authentication. [Action] None.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
3	NORMAL	LOGIN	Login update succeeded.
	The user's login time was successfully updated. [Action] None.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
4	NORMAL	LOGOUT	Force logout ; clear web-authentication command succeeded.
	Authentication has been canceled by a command. [Action] None.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
5	NORMAL	LOGOUT	Force logout ; Connection time was beyond a limit.
	Authentication was canceled because the maximum connection time was exceeded. [Action] None.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
6	NORMAL	LOGOUT	Force logout ; mac-address-table aging.
	Authentication was canceled because a MAC address was deleted due to MAC address table aging. [Action] The terminal is not in use. Check the terminal.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
8	NORMAL	LOGOUT	Force logout ; Authentic method changed (RADIUS <-> Local).
	Authentication was canceled because the authentication method was switched between the RADIUS authentication and local authentication. [Action] None.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
10	NOTICE	LOGIN	Login failed ; User name not found to web authentication DB.
	Authentication failed because the specified user ID was not registered in the internal DB, or the number of characters for the user ID was out of range. [Action] Use the correct user ID to log in.		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
	User name		
11	NOTICE	LOGIN	Login failed ; Password not found to web authentication DB. [Password=[password]]
	Authentication failed because a password was not entered or the entered password was incorrect. [Action] Use the correct password to log in.		
	User name, password		
13	NOTICE	LOGOUT	Logout failed ; ARP resolution.
	Authentication could not be canceled because ARP resolution of the client PC's IP address failed. Alternatively, the VLAN, MAC address, and port were unable to be identified from the client PC's IP address. [Action] Log out again. If the client PC's MAC address has been authenticated on a different port, the port number may not be able to be determined from the MAC address. In this case, use the "clear web-authentication auth-state" command to cancel the authentication of the different port.		
	User name, IP address		
14	NOTICE	LOGIN	Login failed ; Double login.
	Authentication failed because duplicated login operation was performed. The cause is either of the following: • A user with a different user ID has already logged in from the same client PC. • In dynamic VLAN mode, the user has already logged in the same client PC in a different VLAN [Action] Log in from another PC. Alternatively, log out from the same client PC, and then log in again.		
	MAC address, user name		
15	NOTICE	LOGIN	Login failed ; Number of login was beyond limit.
	Authentication cannot be performed because the number of logins exceeded the maximum allowable number. The cause is either of the following: • The capacity limit for Web authentication has already been exceeded. • The total number of IEEE 802.1X authentications, Web authentications, and MAC-based authentications exceeded the capacity limit. [Action] Log in again when the number of authenticated users drops low enough.		
	MAC address, user name		
16	NOTICE	LOGIN	Login failed ; The login failed because of hardware restriction.
	Authentication cannot be performed because the MAC address could not be registered due to hardware specifications. [Action] Log in from another PC.		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
	MAC address, user name		
17	NOTICE	LOGIN	Login failed ; VLAN not specified.
	Authentication could not be performed because the VLAN ID did not match the VLAN ID set for Web authentication. [Action] Set the correct VLAN ID in the configuration.		
	MAC address, user name, VLAN ID		
18	NOTICE	LOGIN	Login failed ; MAC address could not register.
	Authentication could not be performed because registration of the MAC address failed. [Action] Log in again.		
	MAC address, user name		
19	NOTICE	LOGOUT	Logout failed ; MAC address could not delete.
	Authentication could not be performed because deletion of the MAC address failed. [Action] Log out again.		
	MAC address#, user name#, VLAN ID#, port number or channel group number#		
20	NOTICE	LOGIN	Login failed ; RADIUS authentication failed.
	Authentication could not be performed because RADIUS authentication failed. [Action] Use the correct user ID to log in.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
21	NOTICE	LOGIN	Login failed ; Failed to connection to RADIUS server.
	Authentication failed because an attempt to communicate with the RADIUS server failed. [Action] Check whether communication is possible between the Switch and the RADIUS server. After the Switch can communicate with the RADIUS server, make an authentication attempt again.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
22	NOTICE	LOGIN	Login failed ; Connection failed L2MacManager.
	Authentication failed because an attempt to communicate with the L2MAC manager program failed. [Action] Log in again. If this message appears frequently, execute the "restart vlan mac-manager" command.		
	MAC address, user name		
25	NOTICE	LOGIN	Login failed ; Double login. (L2MacManager)

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
	Authentication failed because a notification from the L2MAC manager program was received indicating that authentication could not performed. The cause is either of the following: • The terminal for which Web authentication was performed had already been authenticated by IEEE 802.1X or MAC-based authentication. • The same MAC address as that of the client PC had already been registered by the "mac-address" configuration command. [Action] Use another terminal to log in.		
	MAC address, user name, VLAN ID		
26	NORMAL	LOGOUT	Force logout ; VLAN deleted.
	When the mode is in fixed VLAN mode or dynamic VLAN mode, authentication of a user who logged in to a VLAN was canceled because the VLAN set for the interface was deleted or the mode of the VLAN was changed. [Action] Configure the VLAN again.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
28	NORMAL	LOGOUT	Force logout ; Polling time out.
	Authentication was canceled because disconnection of an authenticated terminal was detected. [Action] None.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
29	NORMAL	LOGOUT	Force logout ; Client moved.
	Authentication was canceled because it was detected that the port of an authenticated terminal was moved. [Action] Log in again.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
31	NORMAL	LOGOUT	Force logout ; Port not specified.
	Authentication has been canceled because the setting for the authentication port was deleted. [Action] Check the configuration.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
32	NOTICE	LOGIN	Login update failed.
	The login time could not be updated because re-authentication of the user failed. [Action] Log in again using the correct user ID and password.		
	MAC address, user name, IP address		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
33	NORMAL	LOGOUT	Force logout ; Port link down.
	Authentication of all users logged in for the port was canceled because the link for the applicable port was down. [Action] After confirming that the port status is link-up, log in again.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
34	NOTICE	LOGIN	Login failed ; Port not specified.
	Authentication cannot be performed because the request was not issued from the port set for the fixed VLAN mode or dynamic VLAN mode. [Action] Connect the terminal to the port to be authenticated, and then log in again.		
	MAC address, user name, port number or channel group number		
39	NOTICE	LOGIN	Login failed ; VLAN not specified.
	When the mode is in fixed VLAN mode or dynamic VLAN mode, authentication cannot be performed because the authentication request was issued by a VLAN which is not set for the interface. [Action] Set a correct configuration, and log in again.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
40	NORMAL	LOGOUT	Force logout ; Ping packet accepted.
	Authentication of the user was canceled because a logout ping was received. [Action] None.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
41	NORMAL	LOGOUT	Force logout ; Other authentication program.
	Authentication was canceled because it was overwritten by another authentication operation. [Action] Make sure other authentication methods are not used for login from the same terminal.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
48	NORMAL	LOGOUT	Force logout ; Program stopped.
	Authentication of all users was canceled because the Web authentication program has stopped. [Action] If you still want to authenticate users through Web authentication, set the configuration.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
49	NORMAL	LOGOUT	Force logout ; Authentic mode had changed (dynamic vlan -> static vlan).
	Authentication of all users was canceled because the authentication mode changed from the dynamic VLAN mode to the fixed VLAN mode. [Action]		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
	None.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
50	NORMAL	LOGOUT	Force logout ; Authentic mode had changed (static vlan -> dynamic vlan).
	Authentication of all users was canceled because the authentication mode changed from the fixed VLAN mode to the dynamic VLAN mode. [Action] None.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
51	NOTICE	LOGIN	Login failed ; IP address is not right.
	In fixed VLAN mode or dynamic VLAN mode, login operation was performed by using an IP address other than Web authentication IP address. Alternatively, the VLAN, MAC address, and port were unable to be identified from the client PC's IP address. [Action] Log in by using the Web authentication IP address. If this log entry is recorded when you log in using a Web authentication IP address, check the client PC's IP address and then log in again. If the client PC's MAC address has been authenticated on a different port, the port number may not be able to be determined from the MAC address. In this case, use the "clear web-authentication auth-state" command to cancel the authentication of the different port.		
	User name, IP address		
54	NORMAL	LOGIN	Force login succeeded.
	Forced authentication succeeded. [Action] None.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
55	NORMAL	LOGIN	Force login update succeeded.
	Updating of the user's login time by forced authentication was successful. [Action] None.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
56	NOTICE	LOGIN	Login failed ; Number of login was beyond limit of port.
	Authentication cannot be performed because the maximum login limit for a port was exceeded. [Action] Reduce the number of terminals to be authenticated.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
57	NORMAL	LOGOUT	Force logout ; Number of login was beyond limit of port.
	Authentication was canceled because the number of ports after moving terminals exceeded the maximum allowable number.		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
	[Action] Reduce the number of terminals to be authenticated.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
82	NORMAL	SYSTEM	Accepted clear auth-state command.
	A request issued by the "clear web-authentication auth-state" command to cancel authentication was received. [Action] None.		
	—		
83	NORMAL	SYSTEM	Accepted clear statistics command.
	A request issued by the "clear web-authentication statistics" command to clear statistics was received. [Action] None.		
	—		
84	NORMAL	SYSTEM	Accepted commit command.
	A commit notification issued by the "commit web-authentication" command for the internal DB was received. [Action] None.		
	—		
85	NORMAL	SYSTEM	Accepted dump command.
	A dump output request issued by the "dump protocols web-authentication" command was received. [Action] None.		
	—		
86	NORMAL	LOGOUT	Force logout ; MAC address not found L2MacManager.
	A MAC address is available for Web authentication, but it is not available for the L2MAC manager program. Therefore, an attempt was made to register a MAC address in the L2MAC manager program, but it failed and authentication is canceled. [Action] Log in again.		
	MAC address, user name		
87	NORMAL	SYSTEM	MAC address existed in the L2MacManager.
	A MAC address, which is available for the L2MAC manager program, but it is not available for Web authentication, was detected. [Action] No action is available because Web authentication falls in the unauthenticated state.		
	MAC address, user name		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
88	ERROR	SYSTEM	WAD could not initialize.[error code]
	Initializing the Web authentication program failed. [Action] Reconfigure the configuration for Web authentication. If this message appears frequently, use the "restart web-authentication" command to restart the Web authentication program.		
	Error code		
89	ERROR	SYSTEM	Connection failed ; Operation command. error=[error-code]
	Outputting the response message for the command failed. [Action] Wait a while, and then re-execute the command.		
	Error code		
90	ERROR	SYSTEM	Connection failed ; L2MacManager.
	An attempt to communicate with the L2MAC manager program was made, but failed. [Action] If this message appears frequently, execute the "restart vlan mac-manager" command.		
	—		
98	NOTICE	LOGOUT	Logout failed ; User is not authenticating.
	Logout failed because the user is not being authenticated by Web authentication. [Action] Use the "show web-authentication login" command to check the authentication status.		
	MAC address		
99	ERROR	SYSTEM	Accounting failed ; RADIUS accounting.
	A response to an accounting request was not received from the RADIUS server. [Action] Check whether communication is possible between the Switch and the RADIUS server.		
	MAC address, user name		
100	NORMAL	SYSTEM	Accepted clear logging command.
	A request to delete the action log by the "clear web-authentication logging" command was received. [Action] None.		
	—		
103	NORMAL	SYSTEM	Synchronized ; Wad -> L2MacManager.
	The authentication status was registered in the hardware because a difference with the hardware was found. [Action] No action is required because the authentication status and the hardware status can be synchronized by Web authentication.		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
	MAC address, user name		
105	NOTICE	LOGIN	Login failed ; VLAN suspended.
	An authentication error occurred because the VLAN used by the login user to be switched after authentication was in disable status. [Action] Enable the post-authentication VLAN, and then log in again.		
	MAC address, user name, VLAN ID		
106	NORMAL	LOGOUT	Force logout ; VLAN suspended.
	Authentication was canceled because the status of the VLAN for the login user changed to disable. [Action] Enable the VLAN, and then log in again.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
107	NOTICE	LOGIN	Login failed ; Multi-step failed.
	Authentication failed because MAC-based authentication failed in multistep authentication. [Action] Log in again.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
108	NORMAL	LOGOUT	Force logout ; Authentic method changed.
	Multistep authentication settings for the target port were changed. [Action] None.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
109	NOTICE	LOGIN	Login failed ; Multi-step failed. (Terminal Auth Info get fail).
	An authentication status query for the terminal failed in multistep authentication. [Action] Log in again.		
	MAC address, user name, IP address, VLAN ID, port number or channel group number		
110	NORMAL	SYSTEM	Accepted clear dead-interval-timer command.
	A request issued by the "clear web-authentication dead-interval-timer" command for recovering the dead interval function was received. [Action] None.		
	—		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
111	NOTICE	SYSTEM	Invalid user class. [class]
	An invalid user class was set on the RADIUS server. [Action] Check the RADIUS server setting.		
	—		
112	NOTICE	LOGOUT	Force logout ; User replacement.
	Authentication of the user ID of the currently logged-in user was canceled because a different user ID was used to log in on the same client PC. [Action] None.		
	—		
255	ERROR	SYSTEM	The other error. [error-code]
	An internal Web authentication error occurred. Communication failed with an internal function indicated by the error code in [] after The other error. [Action] An internal error occurred in the Web authentication program. Use the "dump protocols web-authentication" command to collect information, and then use the "restart web-authentication" command to restart the Web authentication program.		
	Error code		

Legend: —: Not applicable

#: Displayed if logout failed during logout processing because the port is down, or due to VLAN suspend or the specification by a user using an operation command.

Impact on communication

None

Notes

Web authentication action log messages are displayed from the newest message to the oldest.

show web-authentication

Shows the configuration for Web authentication.

Syntax

```
show web-authentication
```

Input mode

Administrator mode

Parameters

None

Example

```
# show web-authentication
Date 20XX/06/10 05:31:14 UTC
web-authentication Information:
   Authentic-method : Local         Accounting-state : disable
   Dead-interval    : 10
   Syslog-send      : enable
   URL-redirect     : enable    Protocol : https
   Jump-URL         : http://www.example.com/
   Web-IP-address   : 1.1.1.1
   FQDN             : aaa.example.com
   Web-port         : http  : 80,8080        https : 443,8443
   ARP-relay Port   : 1/0/1-2
   Force-Authorized : enable
   Auth-max-user    : 1024
   User replacement : enable
   HTML files       : default

   Authentic-mode   : Dynamic-VLAN
          Max-timer : 60                  Max-user  : 256
         VLAN Count : -                 Auto-logout : enable

   Authentic-mode   : Static-VLAN
          Max-timer : 60                  Max-user  : 256
         VLAN Count : -                 Auto-logout : -
    Alive-detection : enable
              timer : 300   interval-timer : 1     count : 3

Port Information:
       Port               :    1/0/1
         Dynamic-VLAN     :
            VLAN ID       :    100
            Native VLAN   :    1
            Forceauth VLAN:    1000
         Static-VLAN      :
            VLAN ID       :    15,4089
         IP access-list   :    AUTH-LIST
         MAC access-list  :    AuthMacAcl
         Max-user         :    64
         HTML fileset     :    default

       Port               :    1/0/2
         Dynamic-VLAN     :
            VLAN ID       :    100,200
            Native VLAN   :    14
            Forceauth VLAN:    1000
         IP access-list   :    AUTH-LIST
```

```
  MAC access-list  :    -
  Max-user         :    64
  HTML fileset     :    default

Port               :    CH:10
  Dynamic-VLAN     :
     VLAN ID       :
     Native VLAN   :    14
     Forceauth VLAN:    -
  IP access-list   :    AUTH-LIST
  MAC access-list  :    -
  Max-user         :    64
  HTML fileset     :    default
```

Display items

Table 33-6: Items displayed for the Web authentication configuration

Item	Meaning	Displayed detailed information
Authentic-method	Authentication method	Authentication method for the Web authentication function Local: Indicates the local authentication method. RADIUS: Indicates the RADIUS authentication method.
Accounting-state	Whether an accounting server is available	Whether an accounting server is available for the Web authentication function enable: An accounting server is available. disable: An accounting server is not available.
Dead-interval	RADIUS connection retry interval	The interval time (in minutes) at which a RADIUS connection attempt is retried if a RADIUS connection fails
Syslog-send	Setting for sending action log messages	The setting for the "web-authentication logging enable" configuration command: enable: The command has been enabled. disable: The command has not been enabled.
URL-redirect	Usage state	Usage state of URL redirection in Web authentication enable: Used disable: Not used
Protocol	http/https type	Login page type to be displayed on a terminal. http: Login page is displayed over http. https: Login page is displayed over https.
Jump-URL	URL to jump to after authentication	URL to jump to after Web authentication is successful
Web-IP-address	IP address	Web authentication IP address
FQDN	FQDN setting	Specified FQDN (Fully Qualified Domain Name) "-" is displayed if no FQDNs have been configured.
Web-port	Communication port	The number of the communication port for the Web server
http	http port	The port number of the http communication port
https	https port	The port number of the https communication port

Item	Meaning	Displayed detailed information
ARP-relay port	ARP relay	The port number of the port, or the channel group number of the channel group, that is used as a relay port or channel group if arp-relay is specified <switch no.>/<nif no.>/<port no.>: Indicates the port number. CH:<channel group number>: Indicates the channel group number. "-" is displayed if arp-relay is not configured.
Force-Authorized	Status of forced authentication	Status of forced authentication. enable: Forced authentication is enabled. disable: Forced authentication is disabled.
Auth-max-user	Maximum number of authenticated users allowed on the device	Maximum number of authenticated users allowed on the device
User replacement	User switching option	The setting for the user switching option enable: Enabled disable: Disabled
HTML files	Page setting	The setting for the basic Web authentication screen default: Default custom: Screen replaced by the authentication page replacement function
Authentic-mode	Authentication mode	Authentication mode for the Web authentication function Dynamic-VLAN: Indicates the dynamic VLAN mode Static-VLAN: Indicates the fixed VLAN mode
Max-timer	Maximum connection time	Maximum connection time (in minutes) for a login user
Max-user	Maximum number of authenticated users	The maximum number of authenticated users who can log in to the Web authentication function
VLAN Count	Total number of VLANs	Displays "-". (The item is not used.)
Auto-logout	Whether forced logout by MAC address aging is available	Whether forced logout by MAC address aging in dynamic VLAN mode for the Web authentication is available enable: Forced logout can be used. disable: Forced logout cannot be used. "-" is displayed when the mode is in fixed VLAN mode.
Alive-detection	Usage state	The usage state of the function that cancels authentication when disconnection of a terminal authenticated in fixed VLAN mode of Web authentication is detected. enable: Used disable: Not used
timer	Monitoring packet sending interval	Sending interval of monitoring packets for detecting disconnections of terminals authenticated through Web authentication (in seconds)
interval-timer	The interval for retransmitting monitoring packets	The interval for retransmitting monitoring packets if no monitoring packets are returned from a terminal (in seconds)
count	The number of monitoring packet retransmissions	The number of monitoring packet retransmissions used for detecting disconnection of a terminal authenticated through Web authentication

Item	Meaning	Displayed detailed information
Port	Port information	Port number of a port used for Web authentication, or a channel group number <switch no.>/<nif no.>/<port no.>: Indicates the port number. CH:<channel group number>: Indicates the channel group number.
Dynamic-VLAN	Dynamic VLAN mode information	Displays the information of the VLAN in dynamic VLAN mode for the port. This item is not displayed if the VLAN is not in dynamic VLAN mode.
VLAN ID	VLAN information	VLAN ID registered in Web authentication In dynamic VLAN mode, the VLAN ID specified for the MAC VLAN is displayed.
Native VLAN	VLAN ID of a native VLAN	The VLAN ID of the native VLAN set for the port for the dynamic VLAN mode
Forceauth VLAN	VLAN setting for forced authentication	The VLAN ID switched to when forced authentication is performed in dynamic VLAN mode If this information is not set by using a configuration command, a hyphen (-) is displayed. This item is not displayed in fixed VLAN mode.
Static-VLAN	Fixed VLAN mode information	Displays the information of the VLAN in fixed VLAN mode for the port. This item is not displayed in fixed VLAN mode.
IP access-list	IP access list	access list number or access list name "-" is displayed if neither is specified.
MAC access-list	MAC access list	access list name "-" is displayed if neither is specified.
Max-user	Maximum number of authenticated users allowed on each port	Maximum number of authenticated users allowed on each port If this information is not set by using a configuration command, a hyphen (-) is displayed.
HTML fileset	Fileset name	Displays the name of the fileset configured for each port. If the configured fileset name is invalid, the name displayed is followed by "(not defined)". "default" is displayed when the name is not configured.

Impact on communication

None

Notes

None

show web-authentication statistics

Shows statistics for Web authentication.

Syntax

```
show web-authentication statistics
```

Input mode

Administrator mode

Parameters

None

Example

- The following command shows an example when the authentication method is local or forced authentication, there is no RADIUS definition, and no user information is registered in the internal Web authentication DB:

```
# show web-authentication statistics
Date 20XX/06/10 05:00:51 UTC
web-authentication Information:
  Authentication Request Total :           3
  Authentication Current Count :           1
  Authentication Error Total   :           0
  Force Authorized Count       :           0
Port Information:
  Port     User-count
   1/0/ 1     0/  64
   1/0/ 2     1/  64
   1/0/ 4     0/  64
   CH: 10     0/1024
```

- The following command shows an example when the authentication method is RADIUS authentication:

```
# show web-authentication statistics
Date 20XX/06/10 03:38:38 UTC
web-authentication Information:
  Authentication Request Total :           2
  Authentication Current Count :           1
  Authentication Error Total   :           0
  Force Authorized Count       :           0
RADIUS web-authentication Information:
[RADIUS frames]
           TxTotal   :         2  TxAccReq  :         2  TxError   :         0
           RxTotal   :         2  RxAccAccpt:         2  RxAccRejct:         0
                                  RxAccChllg:         0  RxInvalid :         0
Account web-authentication Information:
[Account frames]
           TxTotal   :         3  TxAccReq  :         3  TxError   :         0
           RxTotal   :         3  RxAccResp :         3  RxInvalid :         0
Port Information:
  Port     User-count
   1/0/ 1     0/  64
   1/0/ 2     1/  64
   1/0/ 4     0/  64
   CH: 10     0/1024
```

Display items

Table 33-7: Items displayed for the Web authentication statistics

Item	Meaning
Authentication Request Total	The total number of authentication requests
Authentication Current Count	The number of users currently authenticated
Authentication Error Total	The total number of authentication request errors
Force Authorized Count	Number of users forcibly authenticated at this time
RADIUS frames	RADIUS information
TxTotal	The total number of packets sent to the RADIUS server
TxAccReq	The total number of Access-Request packets sent to the RADIUS server
TxError	The number of errors occurring during transmission to the RADIUS server
RxTotal	The total number of received packets from the RADIUS server
RxAccAccpt	The total number of Access-Accept packets received from the RADIUS server
RxAccRejct	The total number of Access-Reject packets received from the RADIUS server
RxAccChllg	The total number of Access-Challenge packets received from the RADIUS server
RxInvalid	The total number of invalid frames received from the RADIUS server
Account frames	Accounting information
TxTotal	The total number of packets sent to the accounting server
TxAccReq	The total number of Accounting-Request packets sent to the accounting server
TxError	The number of errors occurring during transmission to the accounting server
RxTotal	The total number of received packets from the accounting server
RxAccResp	The total number of Accounting-Response packets received from the accounting server
RxInvalid	The total number of invalid frames received from the accounting server
Port Information	Port information
Port	<switch no.>/<nif no.>/<port no.>: Indicates the port number. CH:<channel group number>: Indicates the channel group number.
User-count	The number of authenticated users for each port and the maximum number of users that can be authenticated for each port. This information is displayed in "m/n" format where m is the number of authenticated users, and n is the maximum number of users that can be authenticated.

Impact on communication

None

Notes

None

clear web-authentication logging

Clears log information for Web authentication.

Syntax

```
clear web-authentication logging
```

Input mode

Administrator mode

Parameters

None

Example

The following command shows an example of clearing the log information for Web authentication:

```
# clear web-authentication logging
```

Display items

None

Impact on communication

None

Notes

None

clear web-authentication statistics

Clears Web authentication statistics.

Syntax

```
clear web-authentication statistics
```

Input mode

Administrator mode

Parameters

None

Example

The following command shows an example of clearing the Web authentication statistics:

```
# clear web-authentication statistics
```

Display items

None

Impact on communication

None

Notes

None

commit web-authentication

Stores local authentication user data for Web authentication in internal flash memory.

Syntax

```
commit web-authentication [-f]
```

Input mode

Administrator mode

Parameters

-f

Stores local authentication data for Web authentication in internal flash memory without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example

The following command shows an example of storing the local authentication data for Web authentication:

```
# commit web-authentication
Commitment web-authentication user data.  Are you sure? (y/n): y
Commit complete.
```

Display items

None

Impact on communication

None

Notes

- Information in the Web authentication DB which is being operated is not overwritten unless this command is executed after the following commands are executed to add, change, or delete users:
  - set web-authentication user
  - set web-authentication passwd
  - set web-authentication vlan
  - remove web-authentication user
- If this command is interrupted during execution before it is completed, the Web authentication DB is not updated. In such a case, re-execute the command to update the Web authentication DB.

store web-authentication

Backs up Web authentication user information to a file.

Syntax

```
store web-authentication <file name> [-f]
```

Input mode

Administrator mode

Parameters

<file name>

Specify the name of the file to which Web authentication user information is to be backed up.

-f

Backs up Web authentication user information to a file without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example

When the "authdata" backup file for Web authentication user information is created:

```
# store web-authentication authdata
Backup web-authentication user data.  Are you sure? (y/n): y
Backup complete.
```

Display items

None

Impact on communication

None

Notes

If Web authentication user information is backed up to a file when the available space in the flash memory is insufficient, incomplete backup files might be created. When creating backup files, use the "show flash" command to make sure there is enough free capacity (20 KB or more) in the flash memory.

load web-authentication

Restores Web authentication user information from a backup file for Web authentication user information. Note that information registered or changed by using the following commands will be replaced by the information that is being restored:

- set web-authentication user
- set web-authentication passwd
- set web-authentication vlan
- remove web-authentication user
- commit web-authentication

Syntax

```
load web-authentication <file name> [-f]
```

Input mode

Administrator mode

Parameters

<file name>

Specify the name of the backup file from which Web authentication user information is restored.

-f

Restores Web authentication user information without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example

To restore the Web authentication user information from the "authdata" backup file:

```
# load web-authentication authdata
Restore web-authentication user data.  Are you sure? (y/n): y
Restore complete.
```

Display items

None

Impact on communication

None

Notes

- Note that the information registered or changed by using the following commands will be replaced by the information that is being restored:
  - set web-authentication user
  - set web-authentication passwd

  - set web-authentication vlan
  - remove web-authentication user
  - commit web-authentication
- If this command is interrupted during execution before it is completed, the Web authentication DB is not updated. In such a case, re-execute the command to update the Web authentication DB.

clear web-authentication auth-state

Forcibly logs out an authenticated, currently logged-in user.

When multiple logins are performed using the same user ID, if a user logs out by using this command, all users who have the same user ID are forcibly logged out. Alternatively, a specific login can be canceled by specifying a MAC address.

Syntax

```
clear web-authentication auth-state { user {<user name> | -all } | mac-address <mac> } [-f]
```

Input mode

Administrator mode

Parameters

user { <user name> | -all }

<user name>

Forces user to get logged out by specifying an authenticated, currently logged-in user.

Specify it with 1 to 128 characters. You can use alphanumeric characters and some symbols. However, you cannot use the following characters:

Double exclamation marks (!!), space, two-byte characters, double-quotation mark ("), ampersand (&), left curly bracket ({), right curly bracket (}), bracket (() and ()), single-quotation mark ('), semicolon (;), dollar sign ($), grave accent mark (`), backslash (\), sharp sign (#) at the beginning, and percent sign (%).

-all

Forcibly logs out all authenticated, currently logged-in users.

mac-address <mac>

<mac>

Forces user logout by specifying the MAC address that is used by the authenticated, currently logged-in user.

Specify the MAC address in the range from 0000.0000.0000 to feff.ffff.ffff. Note that you cannot specify a multicast MAC address (address in which the lowest bit of the first byte is 1).

-f

Forces user logout without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example

- To force authenticated, currently logged-in user "USER01" to log out:
```
# clear web-authentication auth-state user USER01
Logout user web-authentication.  Are you sure? (y/n): y
```
- To force all authenticated, currently logged-in users to log out:
```
# clear web-authentication auth-state user -all
Logout all user web-authentication.  Are you sure? (y/n): y
```

- To force an authenticated user that is currently logged in to log out by specifying the MAC address "0012.e200.0001":

```
# clear web-authentication auth-state mac-address 0012.e200.0001
Logout user web-authentication of specified MAC address.  Are you sure? (y/n): y
```

Display items

None

Impact on communication

Authentication for any user that is specified will be canceled.

Notes

None

set web-authentication html-files

Replaces the images for Web authentication pages (such as login and logout pages), the messages output for authentication errors, and the icons displayed in the Favorites menu of the Web browser.

When you execute this command, specify the name of the directory in which the page images, messages, or icons to be registered are stored. Page images (such as HTML or GIF files), messages, and icons to be registered must have been created and stored in any directory (such as the current directory) beforehand. Note that if you execute this command with the directory in which a new file is stored specified, all registered information will be cleared and overwritten with the new information.

Syntax

```
set web-authentication html-files <directory> [html-fileset <name>] [-f]
```

Input mode

Administrator mode

Parameters

<directory>

Specify the directory that stores page images, messages, or icons to be displayed in the Favorites menu of your Web browser that you want to register.

Page images, messages, and icons to be displayed in the Favorites menu of your Web browser that you want to register must be stored in a directory according to the following conditions:

- Specify a directory other than /config.
- There must be no subdirectories in the specified directory.
- There must be a "login.html" file in the specified directory.
- Specify the file names of the page images, messages, and icons to be registered as follows:

  Login page: "login.html"

  Login success page: "loginOK.html"

  Login failed page: "loginNG.html"

  Logout page: "logout.html"

  Logout success page: "logoutOK.html"

  Logout failed page: "logoutNG.html"

  Authentication error messages: "webauth.msg"

  Icons to be displayed in the Favorites menu of your Web browser: "favicon.ico"

  Other stored files, such as GIF files, can have any name.

html-fileset <name>

Specifies the name of the fileset used to store the files for the individual web authentication screens.

Specify it with 1 to 16 characters. Specifiable characters are uppercase alphanumeric characters.

Behavior when this parameter is omitted:

The basic Web authentication screen is replaced.

-f

Replaces pages, messages, and icons without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example

The following command shows an example of registering Web authentication page images, messages, and icons (when page images, messages, and icons to be registered are stored in the "k-html" directory):

```
# ls -l k-html
-rwxr-xr-x  operator  users  1108 Dec  6 09:59 login.html
-rwxr-xr-x  operator  users  1302 Dec  6 09:59 loginNG.html
-rwxr-xr-x  operator  users  1300 Dec  6 09:59 loginOK.html
-rwxr-xr-x  operator  users   843 Dec  6 09:59 logout.html
-rwxr-xr-x  operator  users   869 Dec  6 09:59 logoutNG.html
-rwxr-xr-x  operator  users   992 Dec  6 09:59 logoutOK.html
-rwxr-xr-x  operator  users   109 Dec  6 09:59 webauth.msg
-rwxr-xr-x  operator  users   199 Dec  6 09:59 favicon.ico
-rwxr-xr-x  operator  users 20045 Dec  6 09:59 aaa.gif
```

- Registering basic Web authentication page files:
  ```
  # set web-authentication html-files k-html
  Would you wish to install new html-files ? (y/n):y
  executing…
  Install complete.
  ```
- Registering an individual Web authentication page file:
  ```
  # set web-authentication html-files k-html html-fileset FILE01
  Would you wish to install new html-files ? (y/n):y
  executing…
  Install complete.
  ```

Display items

None

Impact on communication

None

Notes

- This command does not check the contents of the HTML files. If the contents of the specified file are incorrect, login and logout operations for Web authentication might not be possible.
- This command can be executed regardless of whether or not the configuration command for Web authentication has been set.
- Page images, messages, and icons registered by using this command are retained when Web authentication is performed, the Web server is restarted, and a device is restarted.
- The total capacity of a file that can be registered is 1024 KB. If the capacity exceeds 1024 KB, the file cannot be registered.
- A maximum of 100 files can be registered. If there are too many files, command execution might take time.
- If this command is interrupted while it is being executed, the registered page is not displayed, but the default page is displayed. In addition, the result might not be displayed correctly by using the "show web-authentication html-files" command. If this happens, re-execute this command to register page images and messages.
- In dynamic VLAN mode, if you associate the loginOK.html file with another file, the login success page might not be displayed correctly.
- A maximum of 4 fileset names can be registered.

clear web-authentication html-files

Deletes the Web authentication pages, messages, and icons registered by the "set web-authentication html-files" command, and reverts to the default settings.

Syntax

```
clear web-authentication html-files [{html-fileset <name> | -all}] [-f]
```

Input mode

Administrator mode

Parameters

{html-fileset <name> | -all}

html-fileset <name>

Deletes the specified fileset for individual Web authentication screens.

Specify it with 1 to 16 characters. Specifiable characters are uppercase alphanumeric characters.

-all

Deletes all the specified filesets for individual Web authentication screens.

The basic Web authentication screen is restored to the default.

Behavior when this parameter is omitted:

The basic Web authentication screen is restored to the default.

-f

Deletes the pages, messages, and icons without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example

- Deleting the registered basic Web authentication page files:

```
# clear web-authentication html-files
Would you wish to clear registered html-files and initialize? (y/n):y
Clear complete.
```

- Deleting a registered individual Web authentication page file:

```
# clear web-authentication html-files html-fileset FILE01
Would you wish to clear registered html-files and initialize? (y/n):y
Clear complete.
```

Display items

None

Impact on communication

None

Notes

This command can be executed regardless of whether or not the configuration command for Web authentication has been set.

show web-authentication html-files

Displays the size of the file (in bytes) registered by the "set web-authentication html-files" command and the date and time registered. If no file has been registered, that the default setting is being used is displayed.

Syntax

```
show web-authentication html-files [detail]
```

Input mode

Administrator mode

Parameters

detail

Specify this parameter if you want to display information about individual files that are not the HTML file, msg (message) file, and ico (icon) file (such as GIF files).

Behavior when this parameter is omitted:

Information about files other than the HTML file, msg file, and ico file is displayed collectively as the other files.

Example

The following commands show examples of displaying the size of the file registered by the "set web-authentication html-files" command and the date and time when the file was registered.

- When files are registered:

  If a fileset for the individual Web authentication screen is registered, the fileset name (e.g., < FILE01 >) is displayed.

```
# show web-authentication html-files
Date 20XX/04/15 10:07:04 UTC
TOTAL SIZE      :      125554
-------------------------------------------------
                        SIZE         DATE
login.html      :        2049      20XX/04/10 14:05
loginProcess.html        2002      20XX/04/10 14:05
loginOK.html    :        1046      20XX/04/10 14:05
loginNG.html    :         985      20XX/04/10 14:05
logout.html     :         843      20XX/04/10 14:05
logoutOK.html   :         856      20XX/04/10 14:05
logoutNG.html   :         892      20XX/04/10 14:05
webauth.msg     :         104      20XX/04/10 14:05
favicon.ico     :           0      default now
the other files :       54000      20XX/04/10 14:05
< FILE01 >
login.html      :        2049      20XX/12/10 14:07
loginProcess.html        2002      20XX/12/10 14:07
loginOK.html    :        1046      20XX/12/10 14:07
loginNG.html    :         985      20XX/12/10 14:07
logout.html     :         843      20XX/12/10 14:07
logoutOK.html   :         856      20XX/12/10 14:07
logoutNG.html   :         892      20XX/12/10 14:07
webauth.msg     :         104      20XX/12/10 14:07
favicon.ico     :           0      default now
the other files :       54000      20XX/12/10 14:07
```

- When no files are registered (the default information is displayed):

```
# show web-authentication html-files
```

```
Date 20XX/04/15 10:07:04 UTC
TOTAL SIZE      :        6993
-------------------------------------------------
                        SIZE         DATE
login.html      :        1108      default now
loginProcess.html        1263      default now
loginOK.html    :        1046      default now
loginNG.html    :         985      default now
logout.html     :         843      default now
logoutOK.html   :         856      default now
logoutNG.html   :         892      default now
webauth.msg     :           0      default now
favicon.ico     :           0      default now
the other files :           0      default now
```

- When files are registered（information about individual files that are not the HTML file, msg file, or ico file is displayed）:

```
# show web-authentication html-files detail
Date 20XX/04/15 10:07:04 UTC
TOTAL SIZE      :      125554
-------------------------------------------------
                        SIZE         DATE
login.html      :        2049      20XX/04/10 14:05
loginProcess.html        2002      20XX/04/10 14:05
loginOK.html    :        1046      20XX/04/10 14:05
loginNG.html    :         985      20XX/04/10 14:05
logout.html     :         843      20XX/04/10 14:05
logoutOK.html   :         856      20XX/04/10 14:05
logoutNG.html   :         892      20XX/04/10 14:05
webauth.msg     :         104      20XX/04/10 14:05
favicon.ico     :           0      default now
aaa.gif         :       20000      20XX/04/10 14:05
bbb.gif         :       15000      20XX/04/10 14:05
ccc.gif         :       10000      20XX/04/10 14:05
ddd.gif         :        9000      20XX/04/10 14:05
< FILE01 >
login.html      :        2049      20XX/12/10 14:07
loginProcess.html        2002      20XX/12/10 14:07
loginOK.html    :        1046      20XX/12/10 14:07
loginNG.html    :         985      20XX/12/10 14:07
logout.html     :         843      20XX/12/10 14:07
logoutOK.html   :         856      20XX/12/10 14:07
logoutNG.html   :         892      20XX/12/10 14:07
webauth.msg     :         104      20XX/12/10 14:07
favicon.ico     :           0      default now
aaa.gif         :       20000      20XX/12/10 14:07
bbb.gif         :       15000      20XX/12/10 14:07
ccc.gif         :       10000      20XX/12/10 14:07
ddd.gif         :        9000      20XX/12/10 14:07
```

Display items

None

Impact on communication

None

Notes

This command can be executed regardless of whether or not the configuration command for Web authentication has been set.

clear web-authentication dead-interval-timer

If the first RADIUS server becomes unresponsive and the dead interval function causes the switch to start using the second or later RADIUS server, the "clear mac-authentication dead-interval-timer" command resumes using the first RADIUS server before the time specified by the "authentication radius-server dead-interval" configuration command has elapsed.

Syntax

```
clear web-authentication dead-interval-timer
```

Input mode

Administrator mode

Parameters

None

Example

The following command shows an example of using the dead interval function to disable access to the second or later RADIUS server:

```
# clear web-authentication dead-interval-timer
```

Display items

None

Impact on communication

None

Notes

None

set web-authentication ssl-crt

Registers the server certificate and private key for SSL communication. Also, an intermediate CA certificate can be registered along with the server certificate and private key.

To enable the server certificate, private key, and intermediate CA certificate registered with this command, you need to use the "restart web-authentication" command to restart the Web authentication program, or use the "restart web-authentication web-server" command to restart the Web server.

Syntax

```
set web-authentication ssl-crt
```

Input mode

Administrator mode

Parameters

None

Example

The following command shows an example of registering the server certificate, private key, and intermediate CA certificate for SSL communication:

```
# set web-authentication ssl-crt
Set path to the key: serverinstall.key
Set path to the certificate: server.crt
Set path to the intermediate CA certificate: ca.crt
Would you wish to install SSL key and certificate? (y/n):y
Install complete.
Please restart web-authentication daemon or web-server daemon.
#
```

Display items

None

Impact on communication

None

Notes

- If the Web authentication program is restarted using the "restart web-authentication" command, all authentications are canceled.
- If the Web server is restarted using the "restart web-authentication web-server" command, authenticated states are retained. However, users who are in the process of being authenticated need to perform login authentication again.
- This command does not check the content and validity of the server certificate, private key, and intermediate CA certificate. Therefore, you might not be able to log in over HTTPS, or the Web server restarted by using the "restart web-authentication" command might be restarted repeatedly in the following cases:
  - A file with incorrect contents was specified.

- A wrong combination of the certificate, private key, and intermediate CA certificate was specified.

  In such a case, use the "clear web-authentication ssl-crt" command to delete the registered server certificate, private key, and intermediate CA certificate. Then, use this command again to register the correct server certificate, private key, and intermediate CA certificate.

- This command can be executed regardless of whether or not the configuration command for Web authentication has been set.
- Executing this command overwrites all server certificates, private keys, and intermediate CA certificate that have been used up to that point. Also, if the intermediate CA certificate is not specified, the previously registered intermediate CA certificate is deleted.
- The server certificate, private key, and intermediate CA certificate specified for the path when this command is executed remain without being deleted even after registration is complete. These files are no longer used after the registration.

clear web-authentication ssl-crt

Deletes the server certificate, private key, and intermediate CA certificate for SSL communication registered by the "set web-authentication ssl-crt" command, and restores the certificate to the default one.

To enable the default certificate, you need to use the "restart web-authentication" command to restart the Web authentication program, or use the "restart web-authentication web-server" command to restart the Web server.

Syntax

```
clear web-authentication ssl-crt
```

Input mode

Administrator mode

Parameters

None

Example

The following command shows an example of deleting the server certificate, private key, and intermediate CA certificate registered for SSL communication:

```
# clear web-authentication ssl-crt
Would you wish to clear SSL key and certificate? (y/n):y
Please restart web-authentication daemon or web-server daemon.
#
```

Display items

None

Impact on communication

None

Notes

- If the Web authentication program is restarted using the "restart web-authentication" command, all authentications are canceled.
- If the Web server is restarted using the "restart web-authentication web-server" command, authenticated states are retained. However, users who are in the process of being authenticated need to perform login authentication again.
- This command can be executed regardless of whether or not the configuration command for Web authentication has been set.

show web-authentication ssl-crt

Displays the registration date and time of the server certificate, private key, and intermediate CA certificate for SSL communication registered by the "set web-authentication ssl-crt" command. If nothing has been registered, the command shows that the default setting is being used.

Syntax

```
show web-authentication ssl-crt
```

Input mode

Administrator mode

Parameters

None

Example

The following commands show examples of displaying the registration date and time of the server certificate, private key, and intermediate CA certificate registered for SSL communication, and of displaying the default values:

- To display the registered server certificate, private key, and intermediate CA certificate:

```
# show web-authentication ssl-crt
Date 20XX/04/15 10:07:04 UTC
                              DATE
SSL key              :  20XX/03/30 14:05
SSL certificate      :  20XX/03/30 14:05
SSL intermediate cert:  20XX/03/30 14:05
```

- To display the defaults when no server certificate, private key, or intermediate CA certificate is registered:

```
# show web-authentication ssl-crt
Date 20XX/04/15 10:07:04 UTC
                              DATE
SSL key              :  default now
SSL certificate      :  default now
SSL intermediate cert:  -
```

Display items

Table 33-8: Information displayed by the show web-authentication ssl-crt command

Item	Meaning	Displayed detailed information
SSL key	Key for SSL communication	Displays the date and time when the private key for SSL communication was registered. default now: Default
SSL certificate	Certificate for SSL communication	Displays the date and time when the server certificate for SSL communication was registered. default now: Default

Item	Meaning	Displayed detailed information
SSL intermediate cert	Intermediate CA certificate for SSL communication	Displays the date and time when the intermediate CA certificate for SSL communication was registered. -: Indicates that the intermediate CA certificate is not registered.

Impact on communication

None

Notes

- This command can be executed regardless of whether or not the configuration command for Web authentication has been set.

restart web-authentication

Restarts the Web authentication program and the Web server.

Syntax

```
restart web-authentication [-f] [{core-file | web-server}]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the program and the server without displaying a restart confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

{core-file | web-server}

core-file

Outputs a core file for Web authentication when the program or server is restarted.

web-server

Restart the Web server only.

Behavior when this parameter is omitted:

The Web authentication program and the Web server are restarted. The core files are not output.

Example

The following command shows an example of restarting the Web authentication program:

```
> restart web-authentication
 WA restart OK? (y/n): y
```

Display items

None

Impact on communication

If web-server is specified for a parameter, only the Web server is restarted and authentication is not canceled. There is no impact on communication.

Note that if web-server is not specified, communication with the post-authentication VLAN is no longer possible because the Web authentication program is restarted, all authentications are canceled, and the MAC address is deleted from the post-authentication VLAN (MAC-VLAN).

Notes

The storage directory and the name of the core file are as follows:

Storage directory: /usr/var/core/

Web authentication core file: wad.core

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

dump protocols web-authentication

Outputs to a file detailed event trace information and control table information collected by the Web authentication program.

Syntax

```
dump protocols web-authentication
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following command shows an example of collecting Web authentication dump information:

```
> dump protocols web-authentication
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of an output file are as follows:

Storage directory: /usr/var/wa/

File: wad_dump.gz

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

34 MAC-based Authentication

show mac-authentication login

Displays the currently logged-in (already authenticated) terminals, in ascending order by login date and time.

Syntax

```
show mac-authentication login
```

Input mode

Administrator mode

Parameters

None

Example

The following command shows an example of displaying authenticated MAC addresses:

```
# show mac-authentication login
Date 20XX/06/10 12:56:45 UTC
Total client counts:2
F MAC address      Port     VLAN   Class  Login time                Limit time  Mode    Reauth
* 0012.e200.0001   1/0/1    39     0      20XX/06/10 12:55:40 UTC   00:08:55    Static    3165
* 0012.e200.0002   1/0/2    50     0      20XX/06/10 12:56:37 UTC   00:09:52    Dynamic   3222
```

Display items

The following table describes the items displayed for authenticated MAC addresses.

Table 34-1: Items displayed for authenticated MAC addresses

Item	Meaning	Displayed detailed information
Total client counts	Total number of terminals	The number of authenticated, currently logged-in terminals
F	Forced authentication indication	Forcibly authenticated terminals *: Indicates that the terminal was forcibly authenticated.
MAC address	MAC address	The MAC addresses of the authenticated, currently logged-in terminals
Port	Port number or channel group number	The port number of the port accommodating the authenticated, currently logged-in terminal, or the channel group number <switch no.>/<nif no.>/<port no.>: Indicates the port number. CH:<channel group number>: Indicates the channel group number.
VLAN	VLAN	The VLANs set for the authenticated, currently logged-in terminals. The VLANs that were switched after authentication in dynamic VLAN mode.
Class	User class	Displays the user class. "-" is displayed in the first step of multistep authentication.
Login time	Login date and time	The time when the authenticated, currently logged-in terminal is successfully authenticated for the first time

Item	Meaning	Displayed detailed information
Limit time	Remaining login time	The remaining login times of the authenticated, currently logged-in terminals. When a user is logged in, the remaining time might be displayed as 00:00:00 immediately before the user is logged out due to a timeout. When the maximum connection time is from 10 to 1440 (minutes): hh:mm:ss hour:minute:second When the maximum connection time is set to infinity: infinity
Mode	Running mode	Authenticated mode. Static: Authenticated in fixed VLAN mode Dynamic: Authenticated in dynamic VLAN mode
Reauth	Time to re-authentication	Remaining time until the terminal is re-authenticated (in seconds) "-" is displayed if re-authentication is disabled.

Impact on communication

None

Notes

The number of displayed terminals may exceed 1024 because it includes terminals that are in pending state (terminal authentication has been successful but user authentication has not been completed) during multi-step authentication.

show mac-authentication logging

Displays action log messages collected by the MAC-based authentication program.

Syntax

```
show mac-authentication logging [client]
```

Input mode

Administrator mode

Parameters

client

Specify the type of action log message to be displayed.

If this parameter is specified, terminal authentication information is displayed.

Behavior when this parameter is omitted:

The action log of the MAC-based authentication program and the terminal authentication information are displayed in chronological order.

Example

The following examples show action log messages displayed for MAC-based authentication.

- When the parameter is omitted:

```
# show mac-authentication logging
Date 20XX/06/09 14:57:33 JST
No=82:Jun 09 14:57:30:NORMAL:SYSTEM: Accepted clear auth-state command.
No=2:Jun 09 14:57:09:NORMAL:LOGOUT: MAC=0012.e212.0001 PORT=1/0/1 VLAN=39 Force logout ; Po
rt link down.
No=1:Jun 09 14:56:47:NORMAL:LOGIN: MAC=0012.e212.0001 PORT=1/0/1 VLAN=39 Login succeeded.
```

- When "client" is specified for the parameter:

```
# show mac-authentication logging client
Date 20XX/06/09 14:57:37 UTC
No=2:Jun 09 14:57:09:NORMAL:LOGOUT: MAC=0012.e212.0001 PORT=1/0/1 VLAN=39 Force logout ; Po
rt link down.
No=1:Jun 09 14:56:47:NORMAL:LOGIN: MAC=0012.e212.0001 PORT=1/0/1 VLAN=39 Login succeeded.
```

Display items

The following shows the display format of a message:

```
No=1:Dec  1 10:09:50:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=0/1 VLAN=3 Login succeeded.
(1)   (2)     (3)     (4)    (5)              (6)                              (7)
```

(1) Message number: Indicates the number assigned to each message shown in "Table 34-4: List of action log messages".

(2) Date: Indicates the date recorded in the MAC-based authentication program.

(3) Time: Indicates the time recorded in the MAC-based authentication program.

(4) Log ID: Indicates the level of the action log message.

(5) Log type: Indicates the type of operation that outputs the log message.

(6) Additional information: Indicates supplementary information provided in the message.

(7) Message body

Action log messages show the following information:

- Log ID: "Table 34-2: Log ID and type of action log messages"
- Log type: "Table 34-2: Log ID and type of action log messages"
- Additional information: "Table 34-3: Additional information"
- List of messages: "Table 34-4: List of action log messages"

Table 34-2: Log ID and type of action log messages

Log ID	Log type	Meaning
NORMAL	LOGIN	Indicates that authentication was successful.
	LOGOUT	Indicates that authentication was canceled.
	SYSTEM	Indicates a runtime notification.
NOTICE	LOGIN	Indicates that authentication failed.
	LOGOUT	Indicates that cancellation of authentication was failed.
	SYSTEM	Indicates alternative behavior in case of communication failure.
ERROR	SYSTEM	Indicates a communication failure or a failure while the MAC-based authentication program is running.

Table 34-3: Additional information

Display format	Meaning
MAC=xxxx.xxxx.xxxx	Indicates the MAC address.
VLAN=xxxx	Indicates the VLAN ID. Note, however, that this is not displayed if VLAN ID information could not be acquired.
PORT=xx/xx/xx CHGR=xx	Indicates the port number or channel group number. Note, however, that this information is not displayed if port information could not be acquired.

Table 34-4: List of action log messages

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
1	NORMAL	LOGIN	Login succeeded.
	The terminal was successfully authenticated. [Action] None.		
	MAC address, VLAN ID, port number or channel group number		
2	NORMAL	LOGOUT	Force logout ; Port link down.
	Authentication was canceled because the link for the relevant port went down. [Action] Make sure the status of relevant port is link-up.		
	MAC address, VLAN ID, port number or channel group number		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
3	NORMAL	LOGOUT	Force logout ; Authentic method changed (RADIUS <-> Local).
	Authentication was canceled because of a switch between the RADIUS authentication and local authentication methods. [Action] None.		
	MAC address, VLAN ID, port number or channel group number		
4	NORMAL	LOGOUT	Force logout ; Clear mac-authentication command succeeded.
	Authentication was canceled by an operation command. [Action] None.		
	MAC address, VLAN ID, port number or channel group number		
5	NORMAL	LOGOUT	Force logout ; Connection time was beyond a limit.
	Authentication was canceled because the maximum connection time was exceeded. [Action] None. If the terminal is connected, authentication is attempted again.		
	MAC address, VLAN ID, port number or channel group number		
6	NOTICE	LOGIN	Login failed ; Port link down.
	An authentication error occurred because the port was down. [Action] Make sure the status of relevant port is link-up.		
	MAC address, VLAN ID, port number or channel group number		
7	NOTICE	LOGIN	Login failed ; Port not specified.
	An authentication error occurred because the authentication request was sent from a port that was not set as a MAC-based authentication port. [Action] Make sure the terminal is connected to the correct port. If there are no problems with the connection, check the configuration.		
	MAC address, VLAN ID, port number or channel group number		
8	NOTICE	LOGIN	Login failed ; VLAN not specified.
	An authentication error occurred because the authentication request was sent from a VLAN that does not exist on the port. [Action] Make sure the terminal is connected to the correct port. If there are no problems with the connection, check the configuration.		
	MAC address, VLAN ID, port number or channel group number		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
9	NORMAL	LOGOUT	Force logout ; Program stopped.
	Authentication of all users was canceled because the MAC-based authentication program stopped. [Action] If you still want to use MAC-based authentication, set the configuration.		
	MAC address, VLAN ID, port number or channel group number		
10	NORMAL	LOGOUT	Force logout ; Other authentication program.
	Authentication was canceled because it was overwritten by another authentication operation. [Action] Check whether another authentication operation was performed on the same terminal.		
	MAC address, VLAN ID, port number or channel group number		
11	NORMAL	LOGOUT	Force logout ; VLAN deleted.
	Authentication was canceled because the VLAN for the authentication port was changed. Alternatively, authentication was canceled because dynamically registered VLANs were deleted by executing the "switchport mac" configuration command with the vlan parameter specified for the authentication port. [Action] Check the VLAN configuration.		
	MAC address, VLAN ID, port number or channel group number		
12	NORMAL	LOGOUT	Force logout ; Client moved.
	The old authenticated state was canceled because the authenticated terminal was connected to another port. [Action] None. Authentication is performed again.		
	MAC address, VLAN ID, port number or channel group number		
13	NOTICE	LOGIN	Login failed ; Double login. (L2MacManager)
	The L2MAC manager program reported that authentication was not possible (because duplicate MAC addresses were registered). [Action] Check whether the MAC address has already been authenticated. If necessary, cancel the existing authentication for the relevant MAC address from the authentication function that is currently authenticating the MAC address.		
	MAC address, VLAN ID, port number or channel group number		
14	NOTICE	LOGIN	Login failed ; Double login.
	Authentication could not be performed because of duplicate registration. [Action] Check whether the MAC address has already been authenticated. If necessary, cancel the existing authentication for the relevant MAC address from the authentication function that is currently authenticating the MAC address.		
	MAC address		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
15	NOTICE	LOGIN	Login failed ; Number of login was beyond limit.
	Authentication could not be performed because the maximum login limit was exceeded. The cause is either of the following: • The capacity limit for MAC-based authentication has already been exceeded. • The total number of IEEE 802.1X authentications, Web authentications, and MAC-based authentications exceeded the capacity limit. [Action] Attempt authentication again when the number of authentications drops low enough.		
	MAC address		
17	NOTICE	LOGOUT	Logout failed ; L2MacManager failed.
	Deletion failed because the user was not being authenticated by MAC-based authentication. [Action] Check whether the MAC address has already been authenticated.		
	MAC address, VLAN ID, port number or channel group number		
18	NOTICE	LOGIN	Login failed ; MAC address could not register. [error-code]
	Authentication could not be performed because registration of the MAC address failed. [Action] Attempt authentication again. If error-code is "HARDWARE_RESTRICTION", log in from another PC.		
	MAC address, error code		
19	NOTICE	LOGOUT	Logout failed ; MAC address could not delete. [error-code]
	An attempt to delete a MAC address failed. [Action] Attempt authentication cancellation again.		
	MAC address[#1], VLAN ID[#1], port number or channel group number[#1], error code		
20	NOTICE	LOGIN	Login failed ; RADIUS authentication failed.
	Authentication could not be performed because RADIUS authentication failed. [Action] Make sure the terminal to be authenticated is correct. Also make sure the RADIUS definition is correct.		
	MAC address, VLAN ID, port number or channel group number		
21	NOTICE	LOGIN	Login failed ; Failed to connection to RADIUS server.
	Authentication failed because an attempt to communicate with the RADIUS server failed. [Action] Check whether communication is possible between the Switch and the RADIUS server. After the Switch can communicate with the RADIUS server, make an authentication attempt again.		
	MAC address, VLAN ID, port number or channel group number		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
22	NOTICE	LOGIN	Login failed ; Connection failed L2MacManager.
	Authentication failed because an attempt to communicate with the L2MAC manager program failed. [Action] Attempt authentication again. If this message appears frequently, execute the "restart vlan mac-manager" command.		
	MAC address		
28	NORMAL	LOGOUT	Force logout ; Port not specified.
	Authentication was canceled because the setting was deleted from the port. [Action] Check the configuration.		
	MAC address, VLAN ID, port number or channel group number		
29	NOTICE	LOGIN	Login failed ; Port number failed.
	Authentication is impossible because port number acquisition failed. [Action] Attempt authentication again.		
	MAC address, port number or channel group number		
30	NORMAL	LOGOUT	Force logout ; mac-address-table aging.
	Authentication was canceled because a MAC address was deleted due to MAC address table aging. [Action] The terminal is not in use. Check the terminal.		
	MAC address, VLAN ID, port number or channel group number		
31	NORMAL	LOGOUT	Force logout ; Authentic mode had changed (dynamic vlan -> static vlan).
	All authentications were canceled because the authentication mode changed from the dynamic VLAN mode to the fixed VLAN mode. [Action] None.		
	MAC address, VLAN ID, port number or channel group number		
32	NORMAL	LOGOUT	Force logout ; Authentic mode had changed (static vlan -> dynamic vlan).
	All authentications were canceled because the authentication mode changed from the fixed VLAN mode to the dynamic VLAN mode. [Action] None.		
	MAC address, VLAN ID, port number or channel group number		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
33	NORMAL	LOGIN	Force login succeeded.
	Forced authentication for the terminal was successful. [Action] None.		
	MAC address, VLAN ID, port number or channel group number		
34	NORMAL	LOGIN	Un-authorized Port Accepted.
	Communication with an authentication exemption terminal was detected. [Action] None.		
	MAC address, VLAN ID, port number or channel group number		
35	NORMAL	LOGOUT	Force logout ; Interface mode had changed.
	Authentication was canceled because the interface mode of the MAC port for which dot1q is set was changed. [Action] None.		
	MAC address, VLAN ID, port number or channel group number		
36	NOTICE	LOGIN	Login failed ; Number of login was beyond limit of port.
	Authentication cannot be performed because the maximum login limit for a port was exceeded. [Action] Reduce the number of terminals to be authenticated.		
	MAC address, VLAN ID, port number or channel group number		
37	NORMAL	LOGOUT	Force logout ; Number of login was beyond limit of port.
	Authentication was canceled because the number of ports after moving terminals exceeded the maximum allowable number. [Action] Reduce the number of terminals to be authenticated.		
	MAC address, VLAN ID, port number or channel group number		
48	NORMAL	LOGOUT	Force logout ; Multi-step finished.
	MAC-based authentication was canceled in response to the completion of multistep authentication. [Action] None.		
	MAC address, VLAN ID, port number or channel group number		
49	NOTICE	LOGOUT	Force logout ; Authentic method changed.
	Multistep authentication settings for the target port were changed. [Action] None.		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
	MAC address, VLAN ID, port number or channel group number		
64	NORMAL	LOGIN	Reauthentication succeeded.
	Re-authentication was successful. [Action] None.		
	MAC address, VLAN ID, port number or channel group number		
65	NORMAL	LOGIN	Force reauthentication succeeded.
	Re-authentication was successful through forced authentication. [Action] None.		
	MAC address, VLAN ID, port number or channel group number		
66	NOTICE	LOGOUT	Force logout ; Reauthentication failed. [Error code]
	Authentication was canceled because re-authentication failed. [Action] See the action with the same number as the message number indicated by the error code.		
	MAC address, VLAN ID, port number or channel group number		
82	NORMAL	SYSTEM	Accepted clear auth-state command.
	A notification issued by the "clear mac-authentication auth-state" command for forced logout was received. [Action] None.		
	—		
83	NORMAL	SYSTEM	Accepted clear statistics command.
	A request issued by the "clear mac-authentication statistics" command for deleting statistics was received. [Action] None.		
	—		
84	NORMAL	SYSTEM	Accepted commit command.
	A notification issued by the "commit mac-authentication" command for re-configuring the authentication information was received. [Action] None.		
	—		
85	NORMAL	SYSTEM	Accepted dump command.
	A dump output request issued by the "dump protocols mac-authentication" command was received.		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
	[Action] None.		
	—		
86	NORMAL	LOGOUT	Force logout ; MAC address not found L2MacManager.
	A MAC address is available for MAC-based authentication, but it is not available for the L2MAC manager program. Therefore, an attempt was made to register a MAC address in the L2MAC manager program, but it failed and authentication is canceled. [Action] Attempt authentication again.		
	MAC address, VLAN ID, port number or channel group number		
88	ERROR	SYSTEM	Macauthd could not initialize.[error-code]
	Initializing the MAC-based authentication program failed. [Action] Check the configurations of MAC-based authentication. If this message appears frequently, use the "restart mac-authentication" command to restart the MAC-based authentication program.		
	Error code		
89	ERROR	SYSTEM	Connection failed ; Operation command. error=[error-code]
	Outputting the response message for the command failed. [Action] Wait a while, and then re-execute the command.		
	Error code		
90	ERROR	SYSTEM	Connection failed ; L2MacManager.
	An attempt to communicate with the L2MAC manager program was made, but failed. [Action] If this message appears frequently, execute the "restart vlan mac-manager" command.		
	—		
92	ERROR	SYSTEM	Disconnection failed ; L2MacManager.
	Communication with the L2MAC manager program was interrupted. [Action] If this message appears frequently, execute the "restart vlan mac-manager" command.		
	—		
93	ERROR	SYSTEM	Program failed ; Configuration command. [error-code]
	An attempt to read the configuration failed. [Action] Use the "restart mac-authentication" command to restart the MAC-based authentication program.		
	Error code		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
94	ERROR	SYSTEM	Program failed ; Internal data update. [error-code]
	An attempt to update the internal table for the configuration failed. [Action] Use the "restart mac-authentication" command to restart the MAC-based authentication program.		
	Error code		
95	ERROR	SYSTEM	Program failed ; Login information could not create. [error-code]
	Creation of login information failed. [Action] Use the "restart mac-authentication" command to restart the MAC-based authentication program.		
	Error code		
96	ERROR	SYSTEM	Program failed ; Login information could not delete.
	An attempt to delete the login information failed. [Action] Use the "restart mac-authentication" command to restart the MAC-based authentication program.		
	—		
99	ERROR	SYSTEM	Accounting failed ; RADIUS accounting.
	A response to an accounting request was not received from the RADIUS server. [Action] Check whether communication is possible between the Switch and the RADIUS server. After the Switch can communicate with the RADIUS server, make an authentication attempt again.		
	MAC address		
100	NORMAL	SYSTEM	Accepted clear logging command.
	A request to delete the action log by the "clear mac-authentication logging" command was received. [Action] None.		
	—		
103	NORMAL	SYSTEM	Synchronized ; Macauthd -> L2MacManager.
	The authentication status was registered in the hardware because a difference with the hardware was found. [Action] No action is required because the authentication status and the hardware status can be synchronized by MAC-based authentication.		
	MAC address		
105	NOTICE	LOGIN	Login failed ; VLAN suspended.
	An authentication error occurred because the VLAN was in disable status.		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
	[Action] Enable the VLAN, and then attempt authentication again.		
	MAC address, VLAN ID, port number or channel group number		
106	NORMAL	LOGOUT	Force logout ; VLAN suspended.
	Authentication was canceled because the status of the VLAN changed to disable. [Action] Enable the VLAN, and then attempt authentication again.		
	MAC address, VLAN ID, port number or channel group number		
107	NOTICE	LOGIN	Login failed ; MAC address not found to MAC authentication DB.
	Authentication failed because the MAC address to be authenticated was not registered in the internal MAC-based authentication DB. [Action] Make sure the MAC address registered in the internal MAC-based authentication DB is correct.		
	MAC address, VLAN ID[#2]		
108	NOTICE	LOGIN	Login failed ; VLAN ID not found to MAC authentication DB.
	Authentication failed because the VLAN ID to be authenticated was not registered in the internal MAC-based authentication DB. [Action] Make sure the VLAN ID registered in the internal MAC-based authentication DB is correct.		
	MAC address, VLAN ID		
110	NORMAL	SYSTEM	Accepted clear dead-interval-timer command.
	A request issued by the "clear mac-authentication dead-interval-timer" command for recovering the dead interval function was received. [Action] None.		
	—		
111	NOTICE	SYSTEM	Invalid user class. [class]
	An invalid user class was set on the RADIUS server. [Action] Check the RADIUS server setting.		
	—		
255	ERROR	SYSTEM	The other error. [error-code]
	An internal MAC-based authentication error occurred. Communication failed with an internal function indicated by the error code in [] after The other error. [Action]		

No.	Log ID	Log type	Message text
	Description and action		
	Additional information		
	An internal error of the MAC-based authentication program occurred. Use the "dump protocols mac-authentication" command to collect information, and then use the "restart mac-authentication" command to restart the MAC-based authentication program.		
	Error code		

Legend: —: Not applicable

#1: Displayed if logout failed during logout processing because the port is down, or due to VLAN suspend or the specification by a user using an operation command.

#2: Displayed for the fixed VLAN mode only.

Impact on communication

None

Notes

Action log messages for MAC-based authentication are displayed from the newest message to the oldest.

show mac-authentication

Shows the configuration for MAC-based authentication.

Syntax

```
show mac-authentication
```

Input mode

Administrator mode

Parameters

None

Example

The following examples show configuration information displayed for MAC-based authentication.

- When no port for MAC-based authentication is registered:

```
# show mac-authentication
Date 20XX/06/10 13:58:58 UTC
mac-authentication Information:
   Authentic-method : RADIUS        Accounting-state    : disable
   Dead-interval    : 10
   Syslog-send      : enable
   Force-Authorized : disable
   Auth-max-user    : 1024
   Reauth-period    : 3600

   Authentic-mode   : Static-VLAN
         Max-timer  : 60                  Max-terminal : 256
         Port Count : 0                    Auto-logout : enable
   VLAN-check       : enable
         Vid-key    : %VLAN

   Authentic-mode   : Dynamic-VLAN
         Max-timer  : 60                  Max-terminal : 256
         Port Count : 0                    Auto-logout : enable
```

- When ports for MAC-based authentication are registered:

```
# show mac-authentication
Date 20XX/06/07 15:35:06 UTC
mac-authentication Information:
   Authentic-method : RADIUS        Accounting-state    : disable
   Dead-interval    : 10
   Syslog-send      : enable
   Force-Authorized : enable
   Auth-max-user    : 1024
   Reauth-period    : 3600

   Authentic-mode   : Static-VLAN
         Max-timer  : 60                  Max-terminal : 256
         Port Count : 2                    Auto-logout : enable
   VLAN-check       : disable
         Vid-key    : %VLAN

   Authentic-mode   : Dynamic-VLAN
         Max-timer  : 60                  Max-terminal : 256
         Port Count : 1                    Auto-logout : enable

Port Information:
       Port               :    1/0/1
         Static-VLAN      :
            VLAN ID       :    5,10,15
         IP access-list   :    100
         MAC access-list  :    -
         Max-user         :    64

       Port               :    1/0/2
         Dynamic-VLAN     :
```

```
    VLAN ID       :    1300-1310
    Native VLAN   :    20
    Forceauth VLAN:    1300
  IP access-list  :    100
  MAC access-list :    AuthMacAcl
  Max-user        :    64

Port              :    1/0/10
  Static-VLAN     :
    VLAN ID       :    300,305
  IP access-list  :    100
  MAC access-list :    -
  Max-user        :    64
```

Display items

Table 34-5: Items displayed for the configuration of MAC-based authentication

Item	Meaning	Displayed detailed information
Authentic-method	Authentication method	Authentication method for the MAC-based authentication function. Local: Indicates the local authentication method. RADIUS: Indicates the RADIUS authentication method.
Accounting-state	Whether an accounting server is available	Whether the accounting server is available for the MAC-based authentication function. enable: An accounting server is available. disable: An accounting server is not available.
Dead-interval	RADIUS connection retry interval	The interval time (in minutes) at which a RADIUS connection attempt is retried if a RADIUS connection fails
Syslog-send	Setting for sending action log messages	The setting for the "mac-authentication logging enable" configuration command: enable: The command has been enabled. disable: The command has not been enabled.
Force-Authorized	Status of forced authentication	Status of forced authentication. enable: Forced authentication is enabled. disable: Forced authentication is disabled.
Auth-max-user	Maximum number of authenticated users allowed on the device	Maximum number of authenticated users allowed on the device
Reauth-period	Re-authentication interval	Period for re-authenticating the terminal after it is successfully authenticated (in seconds)
Authentic-mode	Authentication mode	Authentication mode for MAC-based authentication. Static-VLAN: Indicates the fixed VLAN mode Dynamic-VLAN: Indicates the dynamic VLAN mode
Max-timer	Maximum connection time	Maximum connection time (in minutes) for a login terminal
Max-terminal	Maximum number of authenticated terminals	Maximum number of authentication terminals that can simultaneously login to the MAC-based authentication function.
Port Count	Total number of ports	Total number of ports registered for MAC-based authentication
Auto-logout	Automatic authentication cancellation time	The time before the auto-logout function works when continuing no-access status is detected for the relevant MAC address (in seconds) "disable" is displayed if the function is disabled.

Item	Meaning	Displayed detailed information
VLAN-check	Whether VLAN ID matching is required for authentication.	Whether VLAN ID matching is required when authentication is performed by MAC-based authentication in fixed VLAN mode. enable: The VLAN ID is checked. disable: The VLAN ID is not checked.
Vid-key	Character string to be added to the account name when RADIUS authentication is performed.	Character strings to be added to the account name when authentication request is sent to the RADIUS server.
Port	Port information	Port number registered for MAC-based authentication, or a channel group number <switch no.>/<nif no.>/<port no.>: Indicates the port number. CH:<channel group number>: Indicates the channel group number.
VLAN ID	VLAN information	The ID of the VLAN to which a port, which is registered for MAC-based authentication, belongs. In dynamic VLAN mode, the VLAN ID specified for the MAC VLAN is displayed.
Auth type	Setting that determines whether authentication is required for tagged frames	Whether to permit communication without authentication for terminals that use tagged frames to communicate over a MAC port. force-authorized: Permits communication without authentication. mac auth: Authentication is required.
Native VLAN	VLAN ID of a native VLAN	The VLAN ID of the native VLAN set for the port for the dynamic VLAN mode
Forceauth VLAN	VLAN setting for forced authentication	The VLAN ID switched to when forced authentication is performed in dynamic VLAN mode If this information is not set by using a configuration command, a hyphen (-) is displayed. This item is not displayed in fixed VLAN mode.
IP access-list	IP access list	access list number or access list name "-" is displayed if neither is specified.
MAC access-list	MAC access list	access list name "-" is displayed if neither is specified.
Max-user	Maximum number of authenticated users allowed on each port	Maximum number of authenticated users allowed on each port If this information is not set by using a configuration command, a hyphen (-) is displayed.

Impact on communication

None

Notes

None

show mac-authentication statistics

Displays MAC-based authentication statistics.

Syntax

```
show mac-authentication statistics
```

Input mode

Administrator mode

Parameters

None

Example

The following command shows an example of displaying the MAC-based authentication statistics:

```
# show mac-authentication statistics
Date 20XX/06/10 13:01:18 UTC
mac-authentication Information:
  Authentication Request Total :          12
  Authentication Current Count :           2
  Authentication Error Total   :           0
  Force Authorized Count       :           2
Unauthorized Information:
  Unauthorized Client Count    :           0
RADIUS mac-authentication Information:
[RADIUS frames]
           TxTotal   :        14  TxAccReq  :        10  TxError   :         4
           RxTotal   :        10  RxAccAccpt:        10  RxAccRejct:         0
                                  RxAccChllg:         0  RxInvalid :         0
Port Information:
  Port     User-count
   1/0/ 1     1/ 256
   1/0/ 2     1/1024
```

Display items

Table 34-6: Items displayed for the MAC-based authentication statistics

Item	Meaning
Authentication Request Total	The total number of authentication requests
Authentication Current Count	The number of currently authenticated terminals
Authentication Error Total	The total number of authentication request errors
Force Authorized Count	Number of users forcibly authenticated at this time
Unauthorized Information	Information about authentication exemption terminals
Unauthorized Client Count	Number of current authentication exemption terminals
RADIUS frames	RADIUS information
TxTotal	The total number of packets sent to the RADIUS server

Item	Meaning
TxAccReq	The total number of Access-Request packets sent to the RADIUS server
TxError	The number of errors occurring during transmission to the RADIUS server
RxTotal	The total number of received packets from the RADIUS server
RxAccAccpt	The total number of Access-Accept packets received from the RADIUS server
RxAccRejct	The total number of Access-Reject packets received from the RADIUS server
RxAccChllg	The total number of Access-Challenge packets received from the RADIUS server
RxInvalid	The total number of invalid frames received from the RADIUS server
Account frames	Accounting information
TxTotal	The total number of packets sent to the accounting server
TxAccReq	The total number of Accounting-Request packets sent to the accounting server
TxError	The number of errors occurring during transmission to the accounting server
RxTotal	The total number of received packets from the accounting server
RxAccResp	The total number of Accounting-Response packets received from the accounting server
RxInvalid	The total number of invalid frames received from the accounting server
Port Information	Port information
Port	<switch no.>/<nif no.>/<port no.>: Indicates the port number. CH:<channel group number>: Indicates the channel group number.
User-count	Total number of authenticated terminals and authentication exemption terminals for the port/maximum number of terminals that can be authenticated set for the port. This information is displayed in "m/n" format where m is the number of authenticated users, and n is the maximum number of users that can be authenticated.

Impact on communication

None

Notes

None

clear mac-authentication auth-state

Forces a specific authenticated terminal to get logged out by specifying the MAC address of the terminal.

In addition, you can force all the authenticated, currently logged-in terminals to get logged out.

Syntax

```
clear mac-authentication auth-state mac-address {<mac> | -all} [-f]
```

Input mode

Administrator mode

Parameters

mac-address {<mac> | -all}

<mac>

Forces an authenticated terminal that has the MAC address specified by <mac> to get logged out.

Specify the MAC address in the range from 0000.0000.0000 to feff.ffff.ffff. Note that you cannot specify a multicast MAC address (address in which the lowest bit of the first byte is 1).

-all

Forces all the authenticated, currently logged-in terminals to get logged out.

-f

Forces terminals to get logged out without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example

The following commands show examples of forcing all the authenticated, currently logged-in terminals to get logged out.

- To force an authenticated, currently logged-in terminal to get logged out by specifying its MAC address (0012.e200.0001):
```
# clear mac-authentication auth-state mac-address 0012.e200.0001
Logout client mac-authentication of specified MAC address.  Are you sure? (y/n): y
```
- To force all the authenticated, currently logged-in terminals to get logged out:
```
# clear mac-authentication auth-state mac-address -all
Logout all client mac-authentication.  Are you sure? (y/n): y
```

Display items

None

Impact on communication

Authentication for the specified terminal will be canceled.

Notes

None

clear mac-authentication logging

Clears log information for MAC-based authentication.

Syntax

```
clear mac-authentication logging
```

Input mode

Administrator mode

Parameters

None

Example

The following command shows an example of clearing the log information for MAC-based authentication:

```
# clear mac-authentication logging
```

Display items

None

Impact on communication

None

Notes

None

clear mac-authentication statistics

Clears MAC-based authentication statistics.

Syntax

```
clear mac-authentication statistics
```

Input mode

Administrator mode

Parameters

None

Example

The following command shows an example of clearing the MAC-based authentication statistics:

```
# clear mac-authentication statistics
```

Display items

None

Impact on communication

None

Notes

None

set mac-authentication mac-address

Adds a MAC address for MAC-based authentication to the internal MAC-based authentication DB. Specify the VLAN ID of the VLAN to which the user belongs. You can add a MAC address that has already been registered if the VLAN ID is different from that already registered.

At least one VLAN ID must be specified if you use this command in dynamic VLAN mode because a VLAN ID is changed to the specified VLAN ID by using this command after authentication in dynamic VLAN mode.

To apply the setting to the internal MAC-based authentication DB, execute the "commit mac-authentication" command.

Syntax

```
set mac-authentication mac-address <mac> [<vlan id>]
```

Input mode

Administrator mode

Parameters

<mac>

Specify the MAC address to be registered.

Specify the MAC address in the range from 0000.0000.0000 to feff.ffff.ffff. Note that you cannot specify a multicast MAC address (address in which the lowest bit of the first byte is 1).

<vlan id>

Specify the VLAN ID of the VLAN over which the user will communicate after authentication.

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

In dynamic VLAN mode, you must specify at least one VLAN ID for each MAC address. Also, in dynamic VLAN mode, if you specify 1 as the VLAN ID, an authentication error occurs because that VLAN cannot be used as the post-authentication VLAN.

Behavior when this parameter is omitted:

In fixed VLAN mode, the VLAN ID is not checked at authentication time.

In dynamic VLAN mode, an authentication error occurs during authentication for the specified MAC address.

Example

To add "0012.e200.1234" as the MAC address and "10" as the VLAN ID:

```
# set mac-authentication mac-address 0012.e200.1234 10
```

Display items

None

Impact on communication

None

Notes

- This command cannot be used concurrently by multiple users.
- The setting is applied to the internal MAC-based authentication DB only when the "commit mac-authentication" command is executed.
- When using the command in dynamic VLAN mode, note the following and specify <vlan id>:
  - When one MAC address is registered and associated with multiple VLAN IDs, the VLAN ID that has the smallest number is used for matching.
  - When the VLAN ID is omitted, an authentication error occurs at terminal authentication time because the VLAN ID after switching cannot be determined.
  - For a given MAC address, if it is registered both with no associated VLAN ID and with an associated VLAN ID, then this is taken to be no VLAN ID specified, and an authentication error occurs at terminal authentication time.
  - When 1 is specified as the VLAN ID, an authentication error occurs at terminal authentication time.

remove mac-authentication mac-address

Deletes a MAC address or MAC addresses for MAC-based authentication from the internal MAC-based authentication DB. Regardless of any associated VLAN ID, as long as the MAC address is the same as the specified MAC address, the MAC address is deleted.

To apply the setting to the authentication information, execute the "commit mac-authentication" command.

Syntax

```
remove mac-authentication mac-address {<mac> | -all} [-f]
```

Input mode

Administrator mode

Parameters

<mac>

Deletes the specified MAC address.

Specify the MAC address in the range from 0000.0000.0000 to feff.ffff.ffff. Note that you cannot specify a multicast MAC address (address in which the lowest bit of the first byte is 1).

-all

Deletes all MAC addresses.

-f

Deletes a MAC address or MAC addresses without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example

- To delete the MAC address "0012.e200.1234":

```
# remove mac-authentication mac-address 0012.e200.1234
Remove mac-authentication mac-address.  Are you sure? (y/n): y
```

- To delete all the MAC addresses registered in the local authentication data:

```
# remove mac-authentication mac-address -all
Remove all mac-authentication mac-address.  Are you sure? (y/n): y
```

Display items

None

Impact on communication

None

Notes

The setting is applied to the internal MAC-based authentication DB only when the "commit mac-authentication" command is executed.

commit mac-authentication

Saves the internal MAC-based authentication DB for MAC-based authentication in the internal flash memory.

The contents of the internal MAC-based authentication DB which is being used is not overwritten unless this command is executed after the following commands are executed to add or delete MAC addresses:

- set mac-authentication mac-address
- remove mac-authentication mac-address

Syntax

```
commit mac-authentication [-f]
```

Input mode

Administrator mode

Parameters

-f

Stores the internal MAC-based authentication DB for MAC-based authentication in internal flash memory without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example

The following command shows an example of saving the internal MAC-based authentication DB for MAC-based authentication:

```
# commit mac-authentication
Commitment mac-authentication mac-address data.  Are you sure? (y/n): y
Commit complete.
```

Display items

None

Impact on communication

None

Notes

- The information in the internal MAC-based authentication DB which is being used is modified only when this command is executed.
- If execution of this command is interrupted before completion, the MAC-based authentication DB is not updated. In such a case, re-execute the command to update the MAC-based authentication DB.

show mac-authentication mac-address

Displays information about the MAC addresses for MAC-based authentication that are registered in a device. MAC address information which is either being entered or being edited by using the following commands can also be displayed:

- set mac-authentication mac-address
- remove mac-authentication mac-address

Information is displayed in ascending order of MAC addresses.

Syntax

```
show mac-authentication mac-address {edit | commit}
```

Input mode

Administrator mode

Parameters

{edit | commit}

edit

Displays information that is being edited.

commit

Displays information about the current internal MAC-based authentication DB.

Example

- To display the information that is being edited:

```
# show mac-authentication mac-address edit
 Date 20XX/12/01 10:52:49 UTC
 Total mac-address counts:2
 mac-address         VLAN
 0012.e200.1234         3
 0012.e201.abcd      4094
```

- To display the information in the current internal MAC-based authentication DB:

```
# show mac-authentication mac-address commit
 Date 20XX/12/01 10:52:49 UTC
 Total mac-address counts:3
 mac-address         VLAN
 0012.e200.1234         4
 0012.e201.abcd      4094
 0012.e202.6789         2
```

Display items

Table 34-7: Items displayed for the MAC-based authentication registration information

Item	Meaning	Displayed detailed information
Total mac-address counts	The total number of registered MAC addresses	The number of registered MAC addresses
mac-address	MAC address	Registered MAC address
VLAN	VLAN	The VLAN set for a registered MAC address. A hyphen (-) is displayed if no VLANs are set.

Impact on communication

None

Notes

None

store mac-authentication

Backs up the internal MAC-based authentication DB to a file.

Syntax

```
store mac-authentication <file name> [-f]
```

Input mode

Administrator mode

Parameters

<file name>

Specify the name of a file to which the internal MAC-based authentication DB is to be backed up.

-f

Backs up the internal MAC-based authentication DB to a file without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example

To create the "authdata" backup file for the internal MAC-based authentication DB:

```
# store mac-authentication authdata
Backup mac-authentication MAC address data.  Are you sure? (y/n): y
Backup complete.
```

Display items

None

Impact on communication

None

Notes

If the internal MAC-based authentication DB is backed up when the flash memory capacity is insufficient, an incomplete backup file might be created. When creating backup files, use the "show flash" command to make sure there is enough free capacity (100 KB or more) in the flash memory.

load mac-authentication

Restores the internal MAC-based authentication DB from a backup file to the internal MAC-based authentication DB. Note that the contents registered or changed by the following commands will be replaced by the contents of the restored backup:

- set mac-authentication mac-address
- remove mac-authentication mac-address
- commit mac-authentication

Syntax

```
load mac-authentication <file name> [-f]
```

Input mode

Administrator mode

Parameters

<file name>

Specify the name of the backup file from which the internal MAC-based authentication DB is to be restored.

-f

Restores the internal MAC-based authentication DB without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example

To restore the internal MAC-based authentication DB from the "authdata" backup file:

```
# load mac-authentication authdata
Restore mac-authentication MAC address data.  Are you sure? (y/n): y
Restore complete.
```

Display items

None

Impact on communication

None

Notes

- Note that the contents registered or changed by the following commands will be replaced by the contents of the restored backup:
  - set mac-authentication mac-address
  - remove mac-authentication mac-address
  - commit mac-authentication
- If execution of this command is interrupted before completion, the MAC-based authentication DB is not updated. In such a case, re-execute the command to update the MAC-based authentication DB.

restart mac-authentication

Restarts the MAC-based authentication program.

Syntax

```
restart mac-authentication [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the program and the server without displaying a restart confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs a core file for MAC-based authentication when the MAC-based authentication program is re-started.

Behavior when this parameter is omitted:

A core file is not output.

Example

The following command shows an example of restarting the MAC-based authentication program:

```
> restart mac-authentication
 macauth restart OK? (y/n): y
```

Display items

None

Impact on communication

All authentications for authenticated, currently logged-in terminals are canceled and the terminals are unable to communicate.

After the MAC-based authentication program is restarted, you must perform authentication again.

Notes

The storage directory and the name of the core file are as follows:

- Storage directory: /usr/var/core/
- Core file for MAC-based authentication: macauthd.core

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

dump protocols mac-authentication

Outputs to a file detailed event trace information and control table information collected by the MAC-based authentication program.

Syntax

```
dump protocols mac-authentication
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following command shows an example of taking a dump of the MAC-based authentication information:

```
> dump protocols mac-authentication
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of an output file are as follows:

- Storage directory: /usr/var/macauth/
- File: macauthd_dump.gz

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

clear mac-authentication dead-interval-timer

If the first RADIUS server becomes unresponsive and the dead interval function causes the switch to start using the second or later RADIUS server, the "clear mac-authentication dead-interval-timer" command resumes using the first RADIUS server before the time specified by the "authentication radius-server dead-interval" configuration command has elapsed.

Syntax

```
clear mac-authentication dead-interval-timer
```

Input mode

Administrator mode

Parameters

None

Example

The following command shows an example of using the dead interval function to disable access to the second or later RADIUS server:

```
# clear mac-authentication dead-interval-timer
```

Display items

None

Impact on communication

None

Notes

None

35 Multistep Authentication

show authentication multi-step

Displays information about terminals authenticated through multistep authentication for each interface.

Syntax

```
show authentication multi-step [{port <port list> | channel-group-number <channel group list>}]
[mac-address <mac>]
```

Input mode

Administrator mode

Parameters

{port <port list> | channel-group-number <channel group list>}

port <port list>

Displays the information about terminals authenticated through multistep authentication for the ports specified in list format. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters".

channel-group-number <channel group list>

Displays the information about terminals authenticated through multistep authentication for the specified channel group in list format. For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

Displays the information about terminals authenticated through multistep authentication for all ports and channel groups.

mac-address <mac>

Displays the information about terminals authenticated through multistep authentication, for which the specified MAC address is registered.

Behavior when this parameter is omitted:

The information about authenticated terminals for all the registered MAC addresses is displayed.

Behavior when all parameters are omitted:

The information about all the terminals authenticated through multistep authentication is displayed.

Example

The following command is an example of displaying the information about terminals authenticated through multistep authentication:

```
# show authentication multi-step

Date 20XX/01/21 22:01:23 UTC
Port 1/0/6  : multi-step dot1x
     Supplicant information                    Authentic method
  No MAC address   State VLAN F Type    Class  Last  (first step)
   1 0012.e2fd.4971 pass   200   multi     24  web   (dot1x)

Port 1/0/7  : multi-step
     Supplicant information                    Authentic method
  No MAC address    State VLAN F Type   Class  Last  (first step)
   1 0012.e2fb.2612 pass   200   single     0  mac   (-)
```

```
Port 1/0/13 : multi-step permissive
     Supplicant information                    Authentic method
  No MAC address    State VLAN F Type   Class  Last  (first step)
   1 0012.e2a5.3e1a pass   100   single     0  dot1x (-)

#
```

Display items

Table 35-1: Items displayed for the information about terminals authenticated through multistep authentication

Item	Meaning	Displayed detailed information
Port/ChGr	Port <switch no.>/<nif no.>/<port no.>: Port ChGr <channel group number>: Channel group number	This item is displayed only when the multistep authentication port (including a channel group) has any authentication entry.
<port status>	Port status	multi-step: User authentication is not permitted when MAC-based authentication fails. multi-step permissive: The permissive parameter is specified, and user authentication is permitted even if MAC-based authentication fails. multi-step dot1x: Web authentication is not permitted when the dot1x parameter is specified and MAC-based authentication or IEEE 802.1X authentication fails.
No	Displayed terminal number	Number assigned to the displayed terminal for each port
Supplicant information	Information about the authenticated terminals	—
MAC address	MAC address	MAC address of the terminal undergoing the authentication process
State	Authentication status	wait: A new terminal is being authenticated. pass: Single authentication or multistep authentication has been completed. This status is displayed while re-authentication is in progress or the authentication time is being updated.
VLAN	VLAN ID of the VLAN which the terminal belongs to	In multistep authentication, the VLAN ID of the VLAN which the terminal will belong to is determined preferentially by the result of user authentication If the post-authentication VLAN is unknown because authentication is not completed, "-" is displayed.
F	Forced authentication indication	*: Terminal that logged in using the forced authentication function If a re-authentication request is sent to a RADIUS server that then authenticates the terminal, the asterisk (*) will disappear.
Type	Type of step authentication	single: Indicates that the device was authenticated via single authentication. multi: Indicates that the terminal was authenticated via multistep authentication. If the authenticate type is unknown because authentication is not completed yet, "-" is displayed.

Item	Meaning	Displayed detailed information
Class	User class	Displays the user class. However, "-" is displayed in the following cases: • The user class is unknown because authentication is not completed yet. • First step of authentication
Authentic method	Information about the authentication function	—
Last	Last authentication function	Authentication function that authenticated the device last mac: MAC-based authentication web: Web authentication dot1x: IEEE 802.1X If the last authentication is not completed yet, "-" is displayed.
(first step)	First step of the authentication function	First-step authentication function for multistep authentication terminals (mac): MAC-based authentication (dot1x): IEEE 802.1X If there is no first-step authentication, "-" is displayed.

Impact on communication

None

Notes

None

36 DHCP snooping

show ip dhcp snooping binding

Displays the DHCP snooping binding database.

Syntax

```
show ip dhcp snooping binding [[ip] <ip address>] [mac <mac address>]
                              [vlan <vlan id>]
                              [interface <interface type> <interface number>]
                              [{ static | dynamic }]
```

Input mode

User mode and administrator mode

Parameters

[ip] <ip address>

Displays the binding database entry for the specified IP address.

mac <mac address>

Displays the binding database entry for the specified MAC address.

vlan <vlan id>

Displays the binding database entry for the specified VLAN interface.

For <vlan id>, specify the VLAN ID set by the "ip dhcp snooping vlan" configuration command.

interface <interface type> <interface number>

Displays the binding database entry for the specified interface.

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below. For details, see "■How to specify an interface" in "Specifiable values for parameters".

- Ethernet interface
- Port channel interface

{ static | dynamic }

static

Displays statically registered entries in the binding database.

dynamic

Displays dynamically registered entries in the binding database.

Behavior when each parameter is omitted:

This command can display only the entries that meet the conditions specified by the parameter. If no parameters are set, entries are displayed with no condition applied. If multiple parameters are specified, the entries conforming to the conditions will be displayed.

Behavior when all parameters are omitted:

All entries are displayed.

Example

The following figure shows an example of displaying all DHCP snooping entries.

Figure 36-1: Result of executing the command to display the DHCP snooping binding database

```
> show ip dhcp snooping binding
Date 20XX/04/20 12:00:00 UTC
Agent URL: flash
Last succeeded time: 20XX/04/20 11:50:00 UTC
Total Bindings Used/Max    :       5/   3070
Total Source guard Used/Max:       5/    200

Bindings: 5
MAC Address     IP Address       Expire(min)  Type      VLAN  Port
0012.e287.0001  192.168.0.201    -            static*   1     1/0/1
0012.e287.0002  192.168.0.204    1439         dynamic   2     1/0/4
0012.e287.0003  192.168.0.203    -            static    3     1/0/3
0012.e287.0004  192.168.0.202    3666         dynamic   4     ChGr:2
0012.e2be.b0fb  192.168.100.11   59           dynamic*  12    1/0/11
>

> show ip dhcp snooping binding 192.168.0.202
Date 20XX/04/20 12:00:00 UTC
Agent URL: flash
Last succeeded time: 20XX/04/20 11:50:00 UTC
Total Bindings Used/Max    :       5/   3070
Total Source guard Used/Max:       5/    200

Bindings: 1
MAC Address     IP Address       Expire(min)  Type      VLAN  Port
0012.e287.0004  192.168.0.202    3666         dynamic   4     ChGr:2
>
```

Display items

Table 36-1: Information displayed by the show ip dhcp snooping binding command

Item	Meaning	Displayed detailed information
Agent URL	Save location for the binding database	Displays setting information in the configuration. flash: Indicates internal flash memory. mc: Indicates a memory card. -: Not specified
Last succeeded time	Date and time the device last saved# (year/month/day hour:minute:second time-zone)	Displays the date and time when information was saved to the save location. "-" is displayed for the following cases: • The Agent URL is not specified. • The database has never been saved. • The number of entries to be restored is zero.
Total Bindings Used/Max: <Used>/<Max>	Number of entries registered in the binding database and maximum number of entries that can be registered	<Used>: Number of registered entries <Max>: Maximum number of entries that can be registered
Total Source guard Used/Max: <Used>/<Max>	Number of entries which are applied to an interface and for which terminal filter is enabled, and maximum number of applicable entries	<Used>: Number of applied entries <Max>: Maximum number of entries that can be applied
Bindings	Number of displayed binding databases	—
MAC Address	Terminal MAC address.	—
IP Address	Terminal IP address.	—

Item	Meaning	Displayed detailed information
Expire(min)	Aging time (in minutes)	If there is no limit in the number of static entries or the aging time, "-" is displayed.
Type	Entry type	static: Indicates a static entry. static*: Indicates a static entry (for a terminal filter). dynamic: Indicates a dynamic entry. dynamic*: Indicates a dynamic entry (for a terminal filter).
VLAN	VLAN ID of the VLAN to which a terminal is connected	—
Port	Port or channel group (ChGr) to which the terminal is connected	Displays the switch number, NIF number, and port number if the target interface is an Ethernet interface. For a port channel interface, the channel group number is displayed.

Legend: —: Not applicable

#: If the binding database has been restored due to device restart or for another reason, the time that the restore information was saved is displayed.

Impact on communication

None

Notes

None

clear ip dhcp snooping binding

Clears the DHCP snooping binding database. This command clears only the entries that have been registered dynamically.

Syntax

```
clear ip dhcp snooping binding [[ip] <ip address>] [mac <mac address>]
                               [vlan <vlan id>]
                               [interface <interface type> <interface number>]
```

Input mode

User mode and administrator mode

Parameters

[ip] <ip address>

Clears the binding database for the specified IP address.

mac <mac address>

Clears the binding database for the specified MAC address.

vlan <vlan id>

Clears the binding database for the specified VLAN interface.

For <vlan id>, specify the VLAN ID set by the "ip dhcp snooping vlan" configuration command.

interface <interface type> <interface number>

Clears the binding database for the specified interface.

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the interface type groups shown below. For details, see "■How to specify an interface" in "Specifiable values for parameters".

- Ethernet interface
- Port channel interface

Behavior when each parameter is omitted:

This command can clear only the entries that meet the conditions specified by the parameter. If no parameters are specified, the entries are cleared without being limited by any conditions. If multiple parameters are specified, the entries conforming to the conditions will be cleared.

Behavior when all parameters are omitted:

The following figure shows an example of clearing all the dynamically registered entries.

Example

The following figure shows an example of clearing all the dynamically registered entries.

Figure 36-2: Result of executing the command to clear the binding database for DHCP snooping

```
> clear ip dhcp snooping binding
>
```

Display items

None

Impact on communication

The access from the terminal corresponding to a cleared entry is strictly restricted until learning is completed again.

Notes

None

show ip dhcp snooping statistics

Shows DHCP snooping statistics.

Syntax

```
show ip dhcp snooping statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure shows an example of displaying statistics for DHCP snooping.

Figure 36-3: Result of executing the command to display the statistics for DHCP snooping

```
> show ip dhcp snooping statistics
Date 20XX/04/20 12:00:00 UTC
Database Exceeded: 0
Total DHCP Packets: 8995
Port            Recv      Filter
1/0/1            170         170
1/0/3           1789          10
              :
1/0/20             0           0
ChGr:1          3646        2457
>
```

Display items

Table 36-2: Items displayed for the DHCP snooping statistics

Item	Meaning	Displayed detailed information
Database Exceeded	Number of times that binding database entries exceeded the maximum allowed number	—
Total DHCP Packets	Total number of DHCP packets processed on untrusted ports in DHCP snooping	—
Port	An untrusted port for which DHCP snooping is enabled	Displays the switch number, NIF number, and port number if the target interface is an Ethernet interface. For a port channel interface, the channel group number is displayed.
Recv	Number of DHCP packets received on untrusted ports for DHCP snooping	The number of packets discarded by Filter is included.
Filter	Of the DHCP packets received (Recv) on the untrusted port for DHCP snooping, the number of DHCP packets discarded as invalid packets	—

Legend: —: Not applicable

Impact on communication

None

Notes

1. If VLAN tunneling is used on the device and DHCP snooping is enabled for the default VLAN, access ports with no VLAN specified are also displayed using this command.
2. When port mirroring is used, if DHCP snooping is enabled for the default VLAN, the mirror port is also displayed using this command.

clear ip dhcp snooping statistics

Clears DHCP snooping statistics.

Syntax

```
clear ip dhcp snooping statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure shows an example of clearing the DHCP snooping statistics.

Figure 36-4: Result of executing the command to clear the DHCP snooping statistics

```
> clear ip dhcp snooping statistics
>
```

Display items

None

Impact on communication

None

Notes

None

show ip arp inspection statistics

Shows statistics for dynamic ARP inspection.

Syntax

```
show ip arp inspection statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure shows an example of displaying the statistics for dynamic ARP inspection.

Figure 36-5: Result of executing the command to display the statistics for dynamic ARP inspection

```
> show ip arp inspection statistics
Date 20XX/04/20 12:00:00 UTC
Port       Forwarded     Dropped  ( DB mismatch     Invalid  )
1/0/1              0          15  (           15           0  )
1/0/2            584         883  (          883           0  )
1/0/3              0           0  (            0           0  )
                                :
ChGr:2           170          53  (           53           0  )
>
```

Display items

Table 36-3: Items displayed for the dynamic ARP inspection statistics

Item	Meaning	Displayed detailed information
Port	Port number	Displays the switch number, NIF number, and port number if the target interface is an Ethernet interface. For a port channel interface, the channel group number is displayed.
Forwarded	Number of forwarded ARP packets	—
Dropped	Total number of discarded ARP packets	Total number of packets listed in the DB mismatch and Invalid items.
DB mismatch	The number of ARP packets discarded because a mismatch of the binding database was found through a basic check	—
Invalid	The number of ARP packets discarded because a mismatch of the binding database was found through an optional inspection	—

Legend: —: Not applicable

Impact on communication

None

Notes

1. If VLAN tunneling is used on the device and dynamic ARP inspection is enabled for the default VLAN, access ports with no VLAN specified are also displayed using this command.
2. When port mirroring is used, if dynamic ARP inspection is enabled in the default VLAN, the mirror port is also displayed using this command.

clear ip arp inspection statistics

Clears dynamic ARP inspection statistics.

Syntax

```
clear ip arp inspection statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure shows an example of clearing the statistics for dynamic ARP inspection.

Figure 36-6: Result of executing the command to clear the statistics for dynamic ARP inspection

```
> clear ip arp inspection statistics
>
```

Display items

None

Impact on communication

None

Notes

None

show ip dhcp snooping logging

Displays action log messages collected by the DHCP snooping program.

Syntax

```
show ip dhcp snooping logging [{ error | warning | notice | info }]
```

Input mode

User mode and administrator mode

Parameters

{ error | warning | notice | info }

Specify the level of action log message to be displayed. Of the output messages at the level specified by the "ip dhcp snooping loglevel" configuration command, log entries whose severity level is equal to or greater than that specified by using this "show ip dhcp snooping logging" command are displayed.

Behavior when this parameter is omitted:

The same action log messages as those displayed when notice is specified is displayed.

Example

The following figure shows an example of displaying an action log message for DHCP snooping.

Figure 36-7: Result of executing the command to display an action log message of DHCP snooping

```
> show ip dhcp snooping logging
Date 20XX/04/20 12:00:00 UTC
Apr 20 11:00:00 ID=2201 NOTICE DHCP server packets were received at an untrust
port(1/0/2/1/0012.e2ff.fe01/192.168.100.254).
>
```

Display items

The following shows the display format of a message:

```
Apr 13 08:44:26 ID=2204 NOTICE ARP packet was received from the client who isn't
  (1)    (2)     (3)    (4)                        (5)
in binding(1/0/3/1/0012.e286.1300).
```

(1) Date: Displays the date (month and day) when the event indicated in the action log message occurred.

(2) Time: Displays the time when the event indicated in the action log message occurred.

(3) Message ID

(4) Level: The following table shows the levels and their description.

Table 36-4: Levels and their description

Level	Type	Description
ERROR	Problem	Interruption of communication is detected or configurations of events were inconsistent.
WARN	Warning	Malicious packets were detected or events that occurred when configurations were inconsistent.

Level	Type	Description
NOTICE	Notification	Errors that occur during normal operation or events that occurred when configurations were inconsistent.
INFO	Regular	A normal event that occurs during normal operation

(5) Message text

The following table lists action log messages.

Table 36-5: List of action log messages

Message ID	Level	Message text
	Description and action	
1109	INFO	The binding entry was deleted all.
	All binding database entries were deleted. [Action] None.	
1110	INFO	The source guard entry was deleted all.
	All terminal filter entries were deleted. [Action] None.	
1201	INFO	The binding entry was created(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).
	An entry was added to the binding database. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] None.	
1202	INFO	The binding entry timed out(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).
	An entry was deleted from the binding database because an aging time expired. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] None.	
1203	INFO	The binding entry was deleted by received DHCPRELEASE(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).
	An entry was deleted from the binding database because DHCPRELEASE was received. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal	

Message ID	Level	Message text
	Description and action	
	[Action] None.	
1204	INFO	The binding entry was deleted by received DHCPDECLINE(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).
	An entry was deleted from the binding database because DHCPDECLINE was received. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] None.	
1205	INFO	The binding entry was renewed(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).
	A binding database entry was updated because lease renewal was detected. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] None.	
1206	INFO	The binding entry was deleted(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).
	An entry was deleted from the binding database. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] None.	
1207	INFO	The source guard entry was added(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).
	A terminal filter entry was added. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] None.	
1208	INFO	The source guard entry was deleted(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).
	A terminal filter entry was deleted. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID	

Message ID	Level	Message text
	Description and action	
	<mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] None.	
1301	INFO	The binding entry was created(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).
	An entry was added to the binding database. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] None.	
1302	INFO	The binding entry timed out(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).
	An entry was deleted from the binding database because an aging time expired. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] None.	
1303	INFO	The binding entry was deleted by received DHCPRELEASE(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).
	An entry was deleted from the binding database because DHCPRELEASE was received. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] None.	
1304	INFO	The binding entry was deleted by received DHCPDECLINE(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).
	An entry was deleted from the binding database because DHCPDECLINE was received. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] None.	

Message ID	Level	Message text
	Description and action	
1305	INFO	The binding entry was renewed(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).
	A binding database entry was updated because lease renewal was detected. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] None.	
1306	INFO	The binding entry was deleted(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).
	An entry was deleted from the binding database. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] None.	
1307	INFO	The source guard entry was added(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).
	A terminal filter entry was added. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] None.	
1308	INFO	The source guard entry was deleted(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).
	A terminal filter entry was deleted. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] None.	
2105	NOTICE	Discard of packets occurred by a reception rate limit of DHCP packets and ARP packets.
	Packets were discarded due to the reception rate limit for DHCP packets and ARP packets. [Action] Revise the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.	

Message ID	Level	Message text
	Description and action	
2201	NOTICE	DHCP server packets were received at an untrust port(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).
	An invalid DHCP server was detected. This message is output once every five minutes on a port-by-port basis. The MAC address and IP address of the detected DHCP server are displayed. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] Check the connected device.	
2202	NOTICE	Lease release was received from the client who isn't in binding(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).
	Invalid lease release was detected. This message is output once every five minutes on a port-by-port basis. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] If this occurs frequently, it might have been caused by an attack. Check the connected devices.	
2204	NOTICE	ARP packet was received from the client who isn't in binding(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>).
	An ARP packet that does not match the binding database was detected. This message is output once every five minutes on a port-by-port basis. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal [Action] Revise the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.	
2301	NOTICE	DHCP server packets were received at an untrust port(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).
	An invalid DHCP server was detected. This message is output once every five minutes on a port-by-port basis. The MAC address and IP address of the detected DHCP server are displayed. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] Check the connected device.	

Message ID	Level	Message text
	Description and action	
2302	NOTICE	Lease release was received from the client who isn't in binding(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).
	Invalid lease release was detected. This message is output once every five minutes on a port-by-port basis. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] If this occurs frequently, it might have been caused by an attack. Check the connected devices.	
2304	NOTICE	ARP packet was received from the client who isn't in binding(ChGr:<channel group number>/<vlan id>/<mac address>).
	An ARP packet that does not match the binding database was detected. This message is output once every five minutes on a port-by-port basis. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal [Action] Revise the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.	
3201	WARN	DHCP packet discard with Option82(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).
	An Option 82 packet was discarded. This message is output once every five minutes on a port-by-port basis. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] Revise the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.	
3202	WARN	Discard of the DHCP packet which SMAC and chaddr isn't identical(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).
	A DHCP packet whose source MAC address and client hardware address do not match was discarded. This message is output once every five minutes on a port-by-port basis. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] Revise the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.	

Message ID	Level	Message text
	Description and action	
3203	WARN	ARP packet was discarded for src-mac inspection(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>).
	An ARP packet whose source MAC address contained in the Layer 2 header and source MAC address contained in the ARP header do not match was discarded. This message is output once every five minutes on a port-by-port basis. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal [Action] Check the connected devices because this might be caused by an attack.	
3204	WARN	ARP packet was discarded for dst-mac inspection(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>).
	An ARP packet whose destination MAC address contained in the Layer 2 header and destination MAC address contained in the ARP header do not match was discarded. This message is output once every five minutes on a port-by-port basis. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal [Action] Check the connected devices because this might be caused by an attack.	
3205	WARN	ARP packet was discarded for ip inspection(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>).
	An ARP packet that has an invalid IP address was discarded. This message is output once every five minutes on a port-by-port basis. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal [Action] Check the connected devices because this might be caused by an attack.	
3301	WARN	DHCP packet discard with Option82(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).
	An Option 82 packet was discarded. This message is output once every five minutes on a port-by-port basis. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] Revise the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.	

Message ID	Level	Message text
	Description and action	
3302	WARN	Discard of the DHCP packet which SMAC and chaddr isn't identica(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).
	A DHCP packet whose source MAC address and client hardware address do not match was discarded. This message is output once every five minutes on a port-by-port basis. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] Revise the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.	
3303	WARN	ARP packet was discarded for src-mac inspection(ChGr:<channel group number>/<vlan id>/<mac address>).
	An ARP packet whose source MAC address contained in the Layer 2 header and source MAC address contained in the ARP header do not match was discarded. This message is output once every five minutes on a port-by-port basis. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal [Action] Check the connected devices because this might be caused by an attack.	
3304	WARN	ARP packet was discarded for dst-mac inspection(ChGr:<channel group number>/<vlan id>/<mac address>).
	An ARP packet whose destination MAC address contained in the Layer 2 header and destination MAC address contained in the ARP header do not match was discarded. This message is output once every five minutes on a port-by-port basis. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal [Action] Check the connected devices because this might be caused by an attack.	
3305	WARN	ARP packet was discarded for ip inspection(ChGr:<channel group number>/<vlan id>/<mac address>).
	An ARP packet that has an invalid IP address was discarded. This message is output once every five minutes on a port-by-port basis. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal [Action] Check the connected devices because this might be caused by an attack.	

Message ID	Level	Message text
	Description and action	
4201	ERROR	The number of the binding entry exceeded the capacity of this system(<switch no.>/<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).
	The number of entries in the binding database exceeds the capacity limit of the device. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] Review the system configuration. If this message is displayed because a static entry has been added, delete the relevant static entry, and then review the system configuration.	
4203	ERROR	The number of the source guard entry exceeded the capacity of this system(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).
	The number of entries for the terminal filter exceeds the capacity limit of the device. <nif no.>/<port no.>: NIF number/port number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] Review the system configuration. If this message is displayed because a static entry has been added, delete the relevant static entry, and then review the system configuration.	
4301	ERROR	The number of the binding entry exceeded the capacity of this system(Ch-Gr:<channel group number>/<vlan id>/<mac address>/<ip address>).
	The number of entries in the binding database exceeds the capacity limit of the device. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] Review the system configuration. If this message is displayed because a static entry has been added, delete the relevant static entry, and then review the system configuration.	
4303	ERROR	The number of the source guard entry exceeded the capacity of this system(Ch-Gr:<channel group number>/<vlan id>/<mac address>/<ip address>).
	The number of entries for the terminal filter exceeds the capacity limit of the device. ChGr <channel group number>: Channel group number <vlan id>: VLAN ID <mac address>: MAC address of the terminal <ip address>: IP address of the terminal [Action] Review the system configuration. If this message is displayed because a static entry has been added, delete the relevant static entry, and then review the system configuration.	

Impact on communication

None

Notes

None

clear ip dhcp snooping logging

Clears log messages collected by the DHCP snooping program.

Syntax

```
clear ip dhcp snooping logging
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure shows an example of clearing log messages for DHCP snooping.

Figure 36-8: Result of executing the command to clear the log messages for DHCP snooping

```
> clear ip dhcp snooping logging
>
```

Display items

None

Impact on communication

None

Notes

None

restart dhcp snooping

Restarts the DHCP snooping program.

Syntax

```
restart dhcp snooping [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the DHCP snooping program without displaying a restart confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

When the DHCP snooping program is restarted, the core file of the program (dhcp_snoopingd.core) is output.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

After the restart confirmation message is output, the DHCP snooping program is restarted.

Example

Figure 36-9: Result of executing the command to restart the DHCP snooping program

```
> restart dhcp snooping
DHCP snooping program restart OK? (y/n):y
>
```

Display items

None

Impact on communication

Because the binding database is temporarily deleted, DHCP or ARP packets received from terminals permitted on untrusted ports for DHCP snooping or dynamic ARP inspection may be discarded.

Notes

1. Core output file: /usr/var/core/dhcp_snoopingd.core
2. Do not add or delete the configuration related to DHCP snooping while the DHCP snooping program is being restarted. The binding database might become invalid.

dump protocols dhcp snooping

Outputs to a file logs or internal information collected by the DHCP snooping program.

Syntax

```
dump protocols dhcp snooping
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure shows an example of outputting logs or internal information for DHCP snooping to a file.

Figure 36-10: Result of executing the DHCP snooping dump command

```
> dump protocols dhcp snooping
>
```

Display items

None

Impact on communication

None

Notes

Output file: /usr/var/dhsn/dhcp_snoopingd.dmp

37 GSRP aware

show gsrp aware

Shows GSRP aware information.

Syntax

```
show gsrp aware
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 37-1: Example of messages displayed by the show gsrp aware command

```
> show gsrp aware
Date 20XX/07/14 12:00:00 UTC

Last MAC Address Table Flush Time : 20XX/07/14 11:00:00
GSRP Flush Request Parameters :
 GSRP ID : 10      VLAN Group ID : 1   Port : 1/0/8
 Source MAC Address : 0012.e2a8.2527

>
```

Display items

Table 37-1: Items displayed for the GSRP aware information

Item	Meaning	Displayed detailed information
Last MAC Address Table Flush Time	Time when MAC Address Table Flush was last performed	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second
GSRP Flush Request Parameters	Information about the GSRP Flush request frame for which MAC Address Table Flush was last performed	—
GSRP ID	GSRP group ID	1 to 65535
VLAN Group ID	VLAN group ID for the received GSRP Flush request frame	1 to 64 (It indicates the VLAN group ID of the VLAN group for which the master and backup were switched.)
Port	Port on which a GSRP Flush request frame was received	—
Source MAC Address	MAC address from which the received GSRP Flush request frame was sent	—

Impact on communication

None

Notes

Receiving a GSRP Flush request frame clears all the MAC Address Table for every VLAN group ID.

restart gsrp

Restarts the GSRP program.

Syntax

```
restart gsrp [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the GSRP program without displaying a restart confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file when the program is restarted.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

After the restart confirmation message is output, the GSRP program is restarted.

Example

Figure 37-2: Example of restarting GSRP

```
> restart gsrp

gsrp program restart OK? (y/n):y
>

> restart gsrp -f
>
```

Display items

None

Impact on communication

Frames cannot be received in VLANs belonging to a VLAN group of GSRP.

Notes

The storage directory and the name of the core file are as follows:

Storage directory: /usr/var/core/

Core file: gsrpd.core

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

dump protocols gsrp

Dumps detailed event trace information and control table information collected by the GSRP program to a file.

Syntax

```
dump protocols gsrp
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 37-3: Example of taking a GSRP dump

```
> dump protocols gsrp

>
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of the output dump file are as follows.

Storage directory: /usr/var/gsrp/

File: gsrp_dump.gz

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance if necessary.

38 Uplink Redundancy

show switchport-backup

Displays information about the uplink redundancy function.

Syntax

```
show switchport-backup [port <port list>] [channel-group-number <channel group list>] [detail]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Specify the port for which you want to display the information about the uplink redundancy function. Uplink port information is displayed for whichever you specify, the primary port or secondary port.

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

channel-group-number <channel group list>

Specify the channel group number for which you want to display the information about the uplink redundancy function. Uplink port information is displayed for whichever you specify, the primary port or secondary port.

For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when each parameter is omitted:

This command can display only the information relevant to the condition applied by a parameter that has been set. If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information conforming to the conditions will be displayed.

detail

Displays detailed information about the uplink redundancy function.

Behavior when this parameter is omitted:

Information about the uplink redundancy function is displayed.

Behavior when all parameters are omitted:

All information about the uplink redundancy function is displayed.

Example

Displays detailed information about the uplink redundancy function.

Figure 38-1: Example of displaying the detailed information about the uplink redundancy function

```
> show switchport-backup detail
Date 20XX/04/04 16:49:07 UTC
startup active port selection: primary only
Switchport Backup pair                          Preemption   Flush
 Primary     Status     Secondary   Status      Delay  Rest   VLAN  Update  Reset
 Port 1/0/1  Forwarding Port 1/0/24 Blocking       -     -   4093       -      -
  VLAN                            : 4051-4094
  MAC Address update Exclude-VLAN : -
  Last change factor              : primary down
  Last change time                : 20XX/04/03 16:52:21
  Last Flush Tx time              : 20XX/04/03 16:52:22
  Last MAC Address update Tx time : -
```

```
  Last port reset time            : -
Switchport Backup pair                          Preemption   Flush
 Primary     Status     Secondary   Status      Delay  Rest   VLAN  Update  Reset
 Port 1/0/10 Down       ChGr 4      Forwarding      -     -      -       1      -
  VLAN                           : 4000-4049
  MAC Address update Exclude-VLAN : 4000-4010
  Last change factor              : command
  Last change time                : 20XX/04/03 09:52:21
  Last Flush Tx time              : -
  Last MAC Address update Tx time : 20XX/04/03 09:52:22
  Last port reset time            : -
Switchport Backup pair                          Preemption   Flush
 Primary     Status     Secondary   Status      Delay  Rest   VLAN  Update  Reset
*Port 1/0/11 Down       Port 1/0/15 Blocking        -     -     10       -      -
  VLAN                           : 10-19,21-30
  MAC Address update Exclude-VLAN : -
  Last change factor              : -
  Last change time                : -
  Last Flush Tx time              : -
  Last MAC Address update Tx time : -
  Last port reset time            : -
Switchport Backup pair                          Preemption   Flush
 Primary     Status     Secondary   Status      Delay  Rest   VLAN  Update  Reset
*Port 1/0/20 Down       Port 1/0/21 Down            -     -      -       -     3s
  VLAN                           : 200-204
  MAC Address update Exclude-VLAN : -
  Last change factor              : -
  Last change time                : -
  Last Flush Tx time              : -
  Last MAC Address update Tx time : -
  Last port reset time            : 20XX/12/03 09:52:22
>
```

Display items

Table 38-1: Items displayed for the detailed uplink redundancy information

Item		Meaning	Displayed detailed information
startup active port selection		Setting of the active port locking function at device startup	primary only: The active port locking function at device startup is enabled. This item is displayed only when this function is enabled.
Switchport Backup pair	Primary	Port number of the primary port, or the channel group number	If an asterisk (*) is displayed, the port is an uplink port and the secondary port cannot be used for communication because the active port locking function at device startup is enabled.
	Status	Status of the primary port	Forwarding: Forwarding status Blocking: Blocking status Down: The port or channel group is in Down status.
	Secondary	Port number of the secondary port, or the channel group number	—
	Status	Status of the secondary port	Forwarding: Forwarding status Blocking: Blocking status Down: The port or channel group is in Down status.
Preemption	Delay	Period for automatic switchbacks (in seconds)	The time that must pass before the active port is automatically switched back. "-" is displayed when this item is not set.

Item		Meaning	Displayed detailed information
	Rest	Remaining time for automatic switchbacks (in seconds)	The time remaining before the active port is switched back. If this setting has not been specified or no switchback conditions apply, a hyphen (-) is displayed.
Flush	VLAN	VLAN ID of the VLAN sending flush control frames	If the VLAN specified in configuration mode does not exist for the access port, protocol port, or MAC port, a VLAN ID different from the specified ID might be displayed. If any of the following conditions applies and flush control frames are not sent, a hyphen (-) is displayed: • Sending of flush control frames is not set in configuration mode. • The VLAN specified in configuration mode does not exist for the trunk port. • The native VLAN does not exist when no VLAN is specified in configuration mode for the trunk port.
	Update	Number of MAC address update frames sent	If the MAC address update function is disabled, a hyphen (-) is displayed.
	Reset	Port resetting	1 to 10s: Port-down time to be applied when port resetting is used. "-" is displayed when this item is not set.
VLAN		VLAN ID of the VLAN set for the primary port	If no VLAN exists in the primary port, a hyphen (-) is displayed.
MAC Address update Exclude-VLAN		VLAN not subject to the MAC address update function	"-" is displayed when this item is not set.
Last change factor		Last factor that determined the active port	command: An operation command was entered. config: A configuration command was entered.[#] primary down: The primary port went down. primary up: The primary port was activated. secondary down: The secondary port went down. secondary up: The secondary port was activated. preemption delay: An automatic switchback was performed. A hyphen (-) is displayed if an active port has never been defined.
Last change time		The date and time when the active port was last determined.	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second A hyphen (-) is displayed if an active port has never been defined.
Last Flush Tx time		Date and time when the flush control frame was last sent	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second This item displays the last time when the flush control frame was sent on the relevant uplink port. "-" is displayed if the frame has never been sent. This information is not cleared even if the flush control frame function is disabled by using a configuration command.

Item	Meaning	Displayed detailed information
Last MAC Address update Tx time	The date and time when the MAC address update frame was last sent.	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second This item displays the last time when the MAC address update frame was sent on the relevant uplink port. "-" is displayed if the frame has never been sent. This information is not cleared even if the MAC address update function is disabled by using a configuration command.
Last port reset time	Date and time when port resetting was last executed	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second The time when the port resetting was last executed on the relevant uplink port is displayed. "-" is displayed if the port resetting has never been executed. This information is not cleared even if the port resetting is disabled by using a configuration command.

#: This item is displayed if the secondary port operating as the active port is changed by using a configuration command before the active port is switched back to the primary port by the automatic switchback function.

Impact on communication

None

Notes

None

set switchport-backup active

Switches the standby port to the active port. You can use this command when you want to manually switch the active port from the secondary port back to the primary port. This could occur, for example, if the primary port is placed in standby state due to a failure.

Syntax

```
set switchport-backup active { port <switch no.>/<nif no.>/<port no.>
                             | channel-group-number <channel group number> } [-f]
```

Input mode

User mode and administrator mode

Parameters

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

Specify the port that you want to activate. For details about the specifiable range of values, see "Specifiable values for parameters".

channel-group-number <channel group number>

Specifies the channel group number which becomes the active port. For details about how to specify <channel group number>, see "Specifiable values for parameters".

-f

Switches to the active port without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Example

The following figure shows an example of switching the standby port to the active port.

Figure 38-2: Example of executing the command that switches the active port

```
> set switchport-backup active port 1/0/1
Are you sure to change the forwarding port to specified port? (y/n): y
>
```

Display items

None

Impact on communication

When the port used for communication is switched, communication might temporarily be interrupted.

Notes

Make sure that the port that you want to activate is in link-up state before you execute the command.

restart uplink-redundant

Restarts the uplink redundancy program.

Syntax

```
restart uplink-redundant [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the uplink redundancy program without outputting any restart confirmation messages.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file when the program is restarted.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

After a restart confirmation message is output, the uplink redundancy program is restarted.

Example

Figure 38-3: Example of restarting uplink redundancy

```
> restart uplink-redundant
Uplink Redundant restart OK? (y/n): y
>
```

Display items

None

Impact on communication

All VLANs become unable to send or receive data temporarily.

Notes

- The storage directory and the name of the core file are as follows:

  Storage directory: /usr/var/core/

  Core file: stpd.core

  If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.
- When this command is executed, the Spanning Tree program is also restarted.
- When the program is restarted, "stpd restarted." is displayed as an operation message.

dump protocols uplink-redundant

Outputs to a file containing detailed event trace information and control table information collected for an uplink redundancy program.

Syntax

```
dump protocols uplink-redundant
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure is an example of outputting detailed event trace information and control table information to a file.

Figure 38-4: Outputting the detailed event trace information and control table information

```
> dump protocols uplink-redundant
>
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of the output dump file are as follows.

Storage directory: /usr/var/ulr/

Output file: ulrd_dump.gz

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

show switchport-backup statistics

Displays statistics pertaining to uplink redundancy.

Syntax

```
show switchport-backup statistics [port <port list>]
                                  [channel-group-number <channel group list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Specify the port for which you want to display the statistics about the uplink redundancy function. Uplink port statistics are displayed for whichever you specify, the primary port or secondary port.

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

channel-group-number <channel group list>

Specify the channel group number for which you want to display the uplink redundancy statistics. Uplink port statistics are displayed for whichever you specify, the primary port or secondary port.

For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when each parameter is omitted:

This command can display only the information relevant to the condition applied by a parameter that has been set. If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information conforming to the conditions will be displayed.

Behavior when all parameters are omitted:

All uplink redundancy statistics are displayed.

Example

Figure 38-5: Example of displaying the uplink redundancy statistics

```
> show switchport-backup statistics port 1/0/1,10
Date 20XX/04/04 17:34:51 UTC
Switchport Backup pair                    Became active count :       201
Primary                                 Secondary
Port 1/0/1                              Port 1/0/24
  Flush Transmit        :           0       Flush Transmit        :           0
  MAC Address update                        MAC Address update
    Transmit            :         101         Transmit            :         100
    Over flow count     :           0         Over flow count     :           0
Switchport Backup pair                    Became active count :           5
Primary                                 Secondary
Port 1/0/10                               ChGr 4
  Flush Transmit        :           6       Flush Transmit        :           5
  MAC Address update                        MAC Address update
    Transmit            :           0         Transmit            :           0
    Over flow count     :           0         Over flow count     :           0
>
```

Display items

Table 38-2: Items displayed for the uplink redundancy statistics

Item		Meaning	Displayed detailed information
Switchport Backup pair	Primary	Primary port number	—
	Secondary	Secondary port number	—
Became active count		Number of times the port became the active port	Number of times the active port was determined by uplink redundancy
Flush Transmit		Number of times a flush control frame was sent	—
MAC Address Update	Transmit	Number of MAC address update frames that have been sent	—
	Over flow count	Number of overflows of MAC address update frames	This value is incremented if the maximum number of entries allowed on the device is exceeded when a MAC address update frame is sent at the time of a switchover or switchback.

Impact on communication

None

Notes

None

clear switchport-backup statistics

Clears uplink redundancy statistics. All uplink redundancy statistics are cleared.

Syntax

```
clear switchport-backup statistics [port <port list>]
                                   [channel-group-number <channel group list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Specify the port for which you want to clear the uplink redundancy statistics. Uplink port statistics are cleared for whichever you specify, the primary port or secondary port.

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

channel-group-number <channel group list>

Specify the channel group number for which you want to clear the uplink redundancy statistics. Uplink port statistics are cleared for whichever you specify, the primary port or secondary port.

For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when each parameter is omitted:

This command can clear only the uplink redundancy statistics relevant to the condition applied by a parameter that has been set. If no parameter is specified, the uplink redundancy statistics is cleared without being limited by any conditions. If multiple parameters are specified, the uplink redundancy statistics that meets the conditions will be cleared.

Behavior when all parameters are omitted:

All uplink redundancy statistics are cleared.

Example

Figure 38-6: Example of clearing the uplink redundancy statistics

```
> clear switchport-backup statistics
>
```

Display items

None

Impact on communication

None

Notes

If a port or channel group is specified, the uplink redundancy statistics on the paired port or channel group are also cleared.

39 L2 Loop Detection

show loop-detection

Shows L2 loop detection information.

Syntax

```
show loop-detection [port <port list>] [channel-group-number <channel group list>]
```

Input mode

User mode and administrator mode

Parameters

[port <port list>] [channel-group-number <channel group list>]

Displays L2 loop detection information for the specified ports and channel groups. Ports and channel groups can be specified at the same time. In this case, L2 loop detection information about either the specified ports or the specified channel groups is displayed.

port <port list>

Displays L2 loop detection information for the specified port numbers. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters".

channel-group-number <channel group list>

Displays L2 loop detection information for the channel groups specified in list format in the specified link aggregation. For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

L2 loop detection information, not limiting it to specific ports or specific channel groups, is displayed.

Example

The following figure shows an example of displaying L2 loop detection information.

Figure 39-1: Displaying the L2 loop detection information

```
> show loop-detection
Date 20XX/04/21 12:10:10 UTC
Interval Time           :10
Output Rate             :30pps
Threshold               :1000
Hold Time               :300
Auto Restore Time       :3600
VLAN Port Counts
    Configuration       :103         Capacity       :300
Port Information
  Port    Status     Type         DetectCnt RestoringTimer  SourcePort  Vlan
  1/0/1   Up         send-inact         100              -  1/0/3       4090
  1/0/2   Down       send-inact           0              -  -
  1/0/3   Up         send               100              -  1/0/1       4090
  1/0/4   Up         exception            0              -  -
  1/0/5   Down(loop) send-inact        1000           1510  CH:8(U)      100
  CH:1    Up         trap                 0              -  -
  CH:8    Up         uplink               -              -  1/0/5        100
>
```

Display items

Table 39-1: Items displayed for the L2 loop detection information

Item	Meaning	Displayed detailed information
Interval Time	Interval for sending L2 loop detection frames (in seconds)	—
Output Rate	L2 loop detection frame transmission rate (packets/s)	The current transmission rate for L2 loop detection frames is displayed.
Threshold	Number of detections before the port changes to the inactive status	The number of times that L2 loop detection frames for inactivating a port were received is displayed.
Hold Time	Retention time for the number of detections (in seconds)	The period of time to retain the number of times that L2 loop detection frames for inactivating a port were received is displayed. When the number is to be retained indefinitely, "infinity" is displayed.
Auto Restore Time	Automatic-restoration time (in seconds)	The period of time before an inactive port is automatically switched to an active port is displayed. "-" is displayed if the port is not automatically restored.
Configuration	Number of ports set to send L2 loop detection frames	The number of VLAN ports# that are set to send L2 loop detection frames is displayed. If this value is greater than the value displayed for the number of ports allowed to send L2 loop detection frames, the excess L2 loop detection frames cannot be sent.
Capacity	Number of ports allowed to send L2 loop detection frames	The number of VLAN ports# where L2 loop detection frames can be sent at the defined transmission rate is displayed.
Port	Port number or channel group number	<switch no.>/<nif no.>/<port no.>: Indicates the port number. CH:<channel group number>: Indicates the channel group number.
Status	Port status	Up: Indicates that the port status is Up. Down: Indicates that the port status is Down. Down(loop): Indicates that the port status is Down due to the L2 loop detection function.
Type	Port type	send-inact: Indicates a detecting and blocking port. send: Indicates a detecting and sending port. trap: Indicates a detecting port. exception: Indicates a port exempted from detection. uplink: Indicates an uplink port.
DetectCnt	Current number of detections	The number of times that L2 loop detection frames were received within the retention time for the number of detections is displayed. For an uplink port, "-" is displayed. The number of receptions on the uplink port is counted on the sending port. The number of receptions is updated until it reaches 10000.

Item	Meaning	Displayed detailed information
RestoringTimer	Time remaining until automatic restoration (in seconds)	The time before the port is activated automatically is displayed. "-" is displayed if the port is not automatically restored.
SourcePort	Port for sending L2 loop detection frames	The sending port used when an L2 loop detection frame was last received. <switch no.>/<nif no.>/<port no.>: Indicates the port number. CH:<channel group number>: Indicates the channel group number. For the receive uplink port, "(U)" is displayed. "-" is displayed if no L2 loop detection frames have been received.
Vlan	Source VLAN ID of the L2 loop detection frame	Displays the source VLAN ID when an L2 loop detection frame was last received.

#: Total number of VLANs set for the applicable physical ports or channel groups.

Impact on communication

None

Notes

None

show loop-detection statistics

Shows L2 loop detection statistics.

Syntax

```
show loop-detection statistics [port <port list>] [channel-group-number <channel group list>]
```

Input mode

User mode and administrator mode

Parameters

[port <port list>] [channel-group-number <channel group list>]

Displays L2 loop detection statistics for the specified ports and channel groups. Ports and channel groups can be specified at the same time. In this case, L2 loop detection statistics related to either the specified ports or the specified channel groups are displayed.

port <port list>

Displays L2 loop detection statistics for the specified port number. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters".

channel-group-number <channel group list>

Displays L2 loop detection statistics for the channel groups specified in list format in the specified link aggregation. For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

L2 loop detection statistics, not limiting it to specific ports or specific channel groups, are displayed.

Example

The following figure shows an example of displaying L2 loop detection statistics.

Figure 39-2: Displaying the L2 loop detection statistics

```
> show loop-detection statistics
Date 20XX/04/21 12:10:10 UTC
Port:1/0/1   Up          Type :send-inact
  TxFrame       :            10000000  RxFrame       :                1200
  Inactive Count:                   3  RxDiscard     :                  30
  Last Inactive : 20XX/04/10 19:20:20  Last RxFrame  : 20XX/04/21 12:02:10
Port:1/0/2   Down        Type :send-inact
  TxFrame       :                   0  RxFrame       :                   0
  Inactive Count:                   0  RxDiscard     :                   0
  Last Inactive :                   -  Last RxFrame  :                   -
Port:1/0/3   Up          Type :send
  TxFrame       :            10000000  RxFrame       :                 600
  Inactive Count:                   0  RxDiscard     :                   0
  Last Inactive :                   -  Last RxFrame  : 20XX/04/10 19:20:20
Port:1/0/4   Up          Type :exception
  TxFrame       :                   0  RxFrame       :                   0
  Inactive Count:                   0  RxDiscard     :                   0
  Last Inactive :                   -  Last RxFrame  :                   -
Port:1/0/5   Down(loop)  Type :send-inact
  TxFrame       :               12000  RxFrame       :                   1
  Inactive Count:                   1  RxDiscard     :                   0
  Last Inactive : 20XX/04/21 09:30:50  Last RxFrame  : 20XX/04/21 09:30:50
CH:1         Up          Type :trap
  TxFrame       :                   0  RxFrame       :                   0
  Inactive Count:                   0  RxDiscard     :                   0
  Last Inactive :                   -  Last RxFrame  :                   -
```

```
CH:8         Up          Type :uplink
  TxFrame       :                  0  RxFrame       :                  100
  Inactive Count:                  0  RxDiscard     :                    0
  Last Inactive :                  -  Last RxFrame  : 20XX/04/21 09:30:50
>
```

Display items

Table 39-2: Items displayed for the L2 loop detection statistics

Item	Meaning	Displayed detailed information
Port	Port number	<switch no.>/<nif no.>/<port no.>: Indicates the port number.
CH	Channel group number	<channel group number>: Indicates the channel group number.
Up	The port is in Up status.	—
Down	The port is in Down status.	—
Down(loop)	The port status is Down due to the L2 loop detection function.	—
Type	Port type	send-inact: Indicates a detecting and blocking port. send: Indicates a detecting and sending port. trap: Indicates a detecting port. exception: Indicates a port exempted from detection. uplink: Indicates an uplink port.
TxFrame	Number of sent L2 loop detection frames	—
RxFrame	Number of received L2 loop detection frames	—
Inactive Count	Number of times that the port or channel group was inactivated	—
RxDiscard	Number of L2 loop detection frames that have been received and discarded	—
Last Inactive	Time when the port or channel group was last inactivated	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second "-" is displayed if the port or channel group has never been in inactive status.
Last RxFrame	Time when the L2 loop detection frame was last received	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second "-" is displayed if no L2 loop detection frames have been received. The time an L2 loop detection frame was received and discarded is not displayed.

Impact on communication

None

Notes

None

show loop-detection logging

Displays log information about received L2 loop detection frames.

With this command, you can check the port from which an L2 loop detection frame was sent and the port on which it was received. Log entries for the latest 1000 received frames are displayed in reverse chronological order. Note that the discarded frames are not displayed.

Syntax

```
show loop-detection logging
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure shows an example of displaying log information about the received L2 loop detection frames.

Figure 39-3: Displaying the log information about received L2 loop detection frames

```
> show loop-detection logging
Date 20XX/04/21 12:10:10 UTC
20XX/04/21 12:10:10  1/0/1    Source: 1/0/3    Vlan: 4090  Inactive
20XX/04/21 12:10:09  1/0/1    Source: 1/0/3    Vlan: 1
20XX/04/21 12:10:08  1/0/1    Source: 1/0/3    Vlan: 4090
20XX/04/21 12:10:07  1/0/3    Source: 1/0/1    Vlan: 4090
20XX/04/21 12:10:06  1/0/3    Source: 1/0/1    Vlan: 4090
20XX/04/10 04:10:10  1/0/20   Source: CH:8     Vlan: 4090
20XX/03/21 03:10:10  1/0/20   Source: 1/0/12   Vlan: 4093
20XX/03/21 02:12:50  1/0/20   Source: 1/0/12   Vlan: 4093
20XX/03/21 02:12:10  1/0/20   Source: 1/0/12   Vlan: 4093
20XX/03/21 02:12:09  1/0/20   Source: 1/0/12   Vlan: 12
20XX/09/05 20:00:00  CH:8     Source: 1/0/12   Vlan: 12    Uplink
20XX/09/05 00:00:00  CH:8     Source: 1/0/12   Vlan: 12    Uplink
>
```

Display items

Table 39-3: Items displayed for the log information about received L2 loop detection frames

Item	Meaning	Displayed detailed information
yyyy/mm/dd hh:mm:ss	Time when an L2 loop detection frame was received	year/month/day hour:minute:second
<switch no.>/<nif no.>/<port no.>	Port number	Displays the port number of the port on which the L2 loop detection frame was received.
CH:<channel group number>	Channel group number	Displays the channel group number of the channel group on which the L2 loop detection frame was received.

Item	Meaning	Displayed detailed information
Source	Port number of the port from which the L2 loop detection frame was sent	Displays the port number of the port from which the L2 loop detection frame was sent. <switch no.>/<nif no.>/<port no.>: Indicates the port number. CH:<channel group number>: Indicates the channel group number.
Vlan	VLAN ID	Displays the VLAN ID when an L2 loop detection frame was sent.
Uplink	Uplink port	Indicates that an L2 loop detection frame was received on an uplink port.
Inactive	Status transition to the inactive status	Indicates that the status is changed to the inactive status.

Impact on communication

None

Notes

None

clear loop-detection statistics

Clears L2 loop detection statistics.

Syntax

```
clear loop-detection statistics [port <port list>] [channel-group-number <channel group list>]
```

Input mode

User mode and administrator mode

Parameters

[port <port list>] [channel-group-number <channel group list>]

Clears the L2 loop detection statistics for the specified ports and channel groups. Ports and channel groups can be specified at the same time. In this case, L2 loop detection statistics related to either the specified ports or the specified channel groups are cleared.

port <port list>

Clears the L2 loop detection statistics for the specified port number. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters".

channel-group-number <channel group list>

Clears the L2 loop detection statistics for the channel groups specified in list format in the specified link aggregation. For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

L2 loop detection statistics, not limiting them to specific ports or specific channel groups, are cleared.

Example

The following figure shows an example of clearing L2 loop detection statistics.

Figure 39-4: Clearing the L2 loop detection statistics

```
> clear loop-detection statistics
>
```

Display items

None

Impact on communication

None

Notes

- Disabling the L2 loop detection function clears the statistics.
- Using this command to clear the statistics also clears the MIB information acquired by SNMP.

clear loop-detection logging

Clears log information for received L2 loop detection frames.

Syntax

```
clear loop-detection logging
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure show an example of clearing the log information for received L2 loop detection frames.

Figure 39-5: Clearing the log information for received L2 loop detection frames

```
> clear loop-detection logging
>
```

Display items

None

Impact on communication

None

Notes

None

restart loop-detection

Restarts the L2 loop detection program.

Syntax

```
restart loop-detection [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the L2 loop detection program without displaying a restart confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file when the program is restarted.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

After the restart confirmation message is output, the L2 loop detection program is restarted.

Example

The following figure shows an example of restarting the L2 loop detection program.

Figure 39-6: Restarting the L2 loop detection program

```
> restart loop-detection
L2 Loop Detection program restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of the core file are as follows:

Storage directory: /usr/var/core/

Core file: l2ldd.core

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

dump protocols loop-detection

Outputs detailed event trace information and control table information collected by the L2 loop detection program to a file.

Syntax

```
dump protocols loop-detection
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure is an example of outputting detailed event trace information and control table information to a file.

Figure 39-7: Outputting the detailed event trace information and control table information

```
> dump protocols loop-detection
>
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of the output dump file are as follows:

Storage directory: /usr/var/l2ld/

Output file: l2ld_dump.gz

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

40 Storm Control

show storm-control

Displays storm control information.

Syntax

```
show storm-control [port <port list>] [broadcast] [multicast] [unicast] [detail]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Displays storm control information for the specified port numbers in list format.

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

broadcast

Displays broadcast storm control information.

multicast

Displays multicast storm control information.

unicast

Displays unicast storm control information.

detail

Displays detailed information on storm control.

Behavior when this parameter is omitted:

The detailed information is not displayed.

Behavior when each parameter is omitted:

This command can display only the information relevant to the condition applied by a parameter that has been set. If multiple parameters are specified, information conforming to the conditions together will be displayed.

Behavior when all parameters are omitted:

If no parameter is specified, the information for all ports is displayed with no condition applied.

Example 1

Figure 40-1: Displaying the storm control information

```
> show storm-control
Date 20XX/01/16 10:46:41 UTC
Broadcast
  Port     Detect Recovery   Filter State           Count Last detect
  1/0/1      1000      500      500 Filtering           1 20XX/01/16 10:43:29
  1/0/2      1000      500        - Forwarding          0 ----/--/-- --:--:--

Unicast
  Port     Detect Recovery   Filter State           Count Last detect
  1/0/1       200      100      100 Filtering           1 20XX/01/16 10:42:46
  1/0/2       200      100        - Forwarding          0 ----/--/-- --:--:--
>
```

Display items in Example 1

Table 40-1: Display items for the storm control information

Item	Meaning	Displayed detailed information
Broadcast	Storm control information on broadcast frames	—
Multicast	Storm control information on multicast frames	—
Unicast	Storm control information on unicast frames	—
Port	Port number	—
Detect	Storm detection threshold	Displays the upper threshold.
Recovery	Storm recovery threshold	—
Filter	Flow rate restriction value	Displays the lower threshold. If the applicable configuration has not been set, "-" is displayed.
State	Storm detection status	Forwarding: Frames are forwarded normally. Filtering: Flow rate restriction is in effect. Inactive: Port inactive status due to storm detection and the "inactive" command Detecting: Storm is being detected (displayed in inactive status of the port or when flow rate restriction is not in effect).
Count	Number of storm detections	—
Last detect	Date and time when the storm was last detected	year/month/day hour:minute:second "-" is displayed when no storm is detected.

Example 2

Figure 40-2: Displaying the detailed storm control information

```
> show storm-control port 1/0/1 broadcast detail
Date 20XX/01/16 10:46:45 UTC
Broadcast
  Port 1/0/1
    Detect rate: 1000          Recover rate: 500          Filter rate: 500
    Action: Inactive,Trap,Log
    Filter recovery time: 30              Auto restore time: 30
    Recovery time: 60
    State: Inactive
    Filter recovery remaining time: -     Auto restore remaining time: 29
    Recovery remaining time: -
    Current rate: 1251519                 Current filter rate: 500
    Detect count: 1                       Last detect: 20XX/01/16 10:43:29
    Discard packet: 1251019
```

Display items in Example 2

Table 40-2: Display items for the detailed storm control information

Item	Meaning	Displayed detailed information
Broadcast	Storm control information on broadcast frames	—
Multicast	Storm control information on multicast frames	—
Unicast	Storm control information on unicast frames	—
Port	Port number	—
Detect rate	Storm detection threshold	Displays the upper threshold.
Recovery rate	Storm recovery threshold	—
Filter rate	Flow rate restriction value	Displays the lower threshold. If the applicable configuration has not been set, "-" is displayed.
Action	Post-storm action setting configured	inactive: Put the target port in inactive status. Filter: Restrict the flow rate of frames to be received Trap: Send an SNMP notification. Log: Output an operation message.
Filter recovery time	Monitoring time before the flow rate restriction is removed	If the applicable configuration has not been set, "-" is displayed.
Auto restore time	Time before the port automatically recovers from the inactive status	If the applicable configuration has not been set, "-" is displayed.
Recovery time	Monitoring time of recovery from storm	—
State	Storm detection status	Forwarding: Frames are forwarded normally. Filtering: Flow rate restriction is in effect. Inactive: Port inactive status due to storm detection and the "inactivate" command Detecting: Storm is being detected (displayed in inactive status of the port or when flow rate restriction is not in effect).
Filter recovery remaining time	Monitoring time remaining before the flow rate restriction is removed	Displays the remaining time until the flow rate restriction is removed. If the storm detection status is other than Filtering, "-" is displayed.
Auto restore remaining time	Time remaining before automatic recovery from the inactive status of the port	Displays the time remaining before the port automatically recovers from the inactive status. "-" is displayed when: • The applicable configuration is not set. • Neither storm detection nor the port is put in inactive status.
Recovery remaining time	Remaining monitoring time of storm recovery	Displays the time remaining before recovery from storm. "-" is displayed when: • Storm detection is in Forwarding status. • Storm detection is in Inactive status.

Item	Meaning	Displayed detailed information
Current rate	Current flow rate	—
Current filter rate	Current state of flow rate restriction	On Filtering in effect: Flow rate restriction value Other than the above: Storm detection threshold
Detect count	Number of storm detections	—
Discard packet	Number of discarded packets	Displays the number of packets discarded by storm control.
Last detect	Date and time when the storm was last detected	year/month/day hour:minute:second "-" is displayed when no storm is detected.

Impact on communication

None

Notes

None

clear storm-control

Clears the statistics counters for storm control information to zero.

Syntax

```
clear storm-control
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 40-3: Clearing the statistics counters for the storm control information to zero

```
> clear storm-control

>
```

Impact on communication

None

Notes

None

41 sFlow Statistics

show sflow

Displays the configuration setting status and behavior status of sFlow statistics.

Syntax

```
show sflow [detail]
```

Input mode

User mode and administrator mode

Parameters

detail

Displays detailed information about the setting status and the behavior status of sFlow statistics.

Example

Figure 41-1: Displaying detailed information about the setting status and behavior status of sFlow statistics

```
> show sflow detail
Date 20XX/01/26 20:04:01 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared:  8:00:05
sFlow agent data :
  sFlow service version  : 4
  CounterSample interval rate: 60 seconds
  Default configured rate: 1 per 2048 packets
  Default actual rate    : 1 per 2048 packets
  Configured sFlow ingress ports :  1/0/2-4
  Configured sFlow egress ports  :  ----
  Received sFlow samples : 37269  Dropped sFlow samples              :    2093
  Exported sFlow samples : 37269  Couldn't export sFlow samples      :       0
  Overflow time of sFlow queue   :  0 seconds
sFlow collector data :
  Collector IP address: 192.168.4.199  UDP:6343  Source IP address: 130.130.130
.1
   Send FlowSample UDP packets   : 12077  Send failed packets:     0
   Send CounterSample UDP packets:   621  Send failed packets:     0
  Collector IP address: 192.168.4.203  UDP:65535  Source IP address: 130.130.13
0.1
   Send FlowSample UDP packets   : 12077  Send failed packets:     0
   Send CounterSample UDP packets:   621  Send failed packets:     0
Detail data :
  Max packet size: 1400 bytes
  Packet information type: header
  Max header size: 128 bytes
  Extended information type: switch,router,gateway,user,url
  Url port number: 80,8080
  Sampling mode: random-number
  Sampling rate to collector: 1 per 2163 packets
  Target ports for CounterSample: 1/0/2-4
```

Display items

Table 41-1: Items displayed for the sFlow statistics

Item	Displayed information
sFlow service status	Indicates the current behavior status of sFlow statistics. (disable is displayed if the target port is not specified.)
Progress time from sFlow statistics cleared	Indicates the time elapsed after sFlow statistics has started or the time elapsed after the "clear sflow statistics" command was last executed. hh:mm:ss: (when the elapsed time is within 24 hours: hh = hours, mm = minutes, ss = seconds) D day: (when the elapsed time is over 24 hours: D = number of days)
sFlow service version	Version of the sFlow packet.
CounterSample interval rate	Sending interval (in seconds) between counter samples
Default configured rate	Sampling interval for the entire device set in the configuration.
Default actual rate	Actual sampling interval for the entire device
Configured sFlow ingress ports	Ports for which "sflow forward ingress" is set in the configuration and on which sFlow statistics are collected#
Configured sFlow egress ports	Ports for which "sflow forward egress" is set in the configuration and on which sFlow statistics are collected#
Received sFlow samples	Total number of packets which were sampled correctly
Dropped sFlow samples	Total number of packets discarded without being accumulated in the sFlow statistics queue for the software if a higher-priority processing was processed on a device or notification over the device's performance was received. (The number of packets discarded because they could not be accumulated in the sFlow statistics queue for the hardware is not included.)
Exported sFlow samples	Total number of sample packets contained in UDP packets sent to the collector
Couldn't export sFlow samples	Total number of sample packets contained in UDP packets that could not be sent
Overflow time of sFlow queue	Length of time (in seconds) during which the sFlow statistics queue was full after the "clear sflow statistics" command was executed. If this value has increased, adjust the sampling interval.
Collector IP address	IP address of the collector set in the configuration
UDP	UDP port number
Source IP address	Address used as an agent IP when packets are sent to the collector
Send FlowSample UDP packets	Number of UDP packets for flow samples sent to the collector
Send failed packets	Number of UDP packets that could not be sent to the collector
Send CounterSample UDP packets	Number of UDP packets for counter samples sent to the collector
Max packet size	Maximum sFlow packet size
Packet information type	Basic data format for flow samples

Item	Displayed information
Max header size	The maximum size of the sample packet when the header type is used as the basic data format
Extended information type	Extended data format for flow samples
Url port number	Port number used to determine if a packet is an HTTP packet when URL information is used for the extended data format
Sampling mode	Sampling method
random-number	Collection at a rate (random numbers) according to the sampling interval
Sampling rate to collector	Recommended sampling interval at which no packets are discarded. If there are problems at the current sampling interval, an applicable value is displayed. The value cannot be smaller than the value set in the configuration. If the sampling interval is changed, execute the "clear sflow statistics" command. The correct value might not be displayed until the command is executed.
Target ports for CounterSample	Target port for counter samples

#

If no configured port exists, ---- is displayed.

Impact on communication

None

Notes

If the number of packets or the statistics counter exceeds the maximum value (32-bit counter), the value is reset to 0.

If no IP addresses or ports are set in the configuration, "----" is displayed.

clear sflow statistics

Clears statistics managed by sFlow statistics.

Syntax

```
clear sflow statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

```
>clear sflow statistics
>
```

Display items

None

Impact on communication

None

Notes

None

restart sflow

Restarts the flow statistics program.

Syntax

```
restart sflow [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the flow statistics program without displaying a restart confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file of the flow statistics program (flowd.core) when the program is restarted.

Behavior when this parameter is omitted:

A core file is not output.

Example

```
>restart sflow
sflow program restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Notes

- The counter value for statistics is cleared when the flow statistics program is restarted.
- The storage directory and the name of the core file are as follows:

  Storage directory: /usr/var/core/

  Core file: flowd.core

  If a file with this name already exists, the file is overwritten unconditionally. Back up the file in advance, if necessary.

dump sflow

Dumps debug information collected in the flow statistics program to a file.

Syntax

```
dump sflow
```

Input mode

User mode and administrator mode

Parameters

None

Example

```
>dump sflow
>
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of the output dump file are as follows:

Storage directory: /usr/var/flowd/

File: sflow.trc

If a file with this name already exists, the file is overwritten unconditionally. Back up the file in advance, if necessary.

42 IEEE 802.3ah/UDLD

show efmoam

Displays the IEEE 802.3ah/OAM configuration information and the status of ports.

Syntax

```
show efmoam [port <port list>] [detail]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Displays the IEEE 802.3ah/OAM configuration information for the specified port.

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

Behavior when this parameter is omitted:

The IEEE 802.3ah/OAM configuration information for all ports is displayed.

detail

Displays configuration information for all modes that send and receive OAMPDU frames.

Note, however, that this parameter is not displayed if a port in passive mode does not recognize the remote device.

Behavior when this parameter is omitted:

No information about ports in passive mode is displayed.

Behavior when all parameters are omitted:

The IEEE 802.3ah/OAM configuration information for all ports that are not in passive mode is displayed.

Example

The following figure shows an example of displaying detailed information related to the IEEE 802.3ah/OAM configuration by specifying the detail parameter.

Figure 42-1: Displaying the detailed IEEE 802.3ah/OAM configuration information

```
> show efmoam detail
Date 20XX/10/02 23:59:59 UTC
Status: Enabled
udld-detection-count: 30
Port     Link status     UDLD status    Dest MAC
1/0/1    Up              detection    * 0012.e298.dc20
1/0/2    Down            active         unknown
1/0/3    Up              passive        0012.e298.7478
1/0/4    Down(uni-link)  detection      unknown
>
```

Display items

Table 42-1: Items displayed for the detailed IEEE 802.3ah/OAM configuration information

Item	Meaning	Displayed detailed information
Status	Status of the IEEE 802.3ah/OAM function of the Switch	Enabled: Indicates that the IEEE 802.3ah/OAM function is enabled.

Item	Meaning	Displayed detailed information
		Disabled: Indicates that the IEEE 802.3ah/OAM function is disabled.
udld-detection-count	Number of response timeouts for detecting failures	3 to 300 (times)
Port	Port information	Switch number/NIF number/port number of the port whose information is to be displayed
Link status	Link status of the applicable port	Up: Indicates that the port status is Up. Down: Indicates that the port status is Down. Down(uni-link): Indicates that the port status is Down (with a unidirectional link failure detected). Down(loop): Indicates that the port status is Down (with a loop detected).
UDLD status	UDLD behavior status by the IEEE 802.3ah/UDLD function for each port	detection: Indicates that a failure is detected. active: Indicates that OAMPDU frames are being sent and responses are received. passive: Only OAMPDU frames are responded to.
Dest MAC	MAC address of the port on the partner device	"unknown" is displayed if no information has been received from the partner device. Note, however, that no unknown ports are displayed in passive mode. If a bidirectional link is confirmed in active mode, "*" is displayed on the left of the MAC address.

Impact on communication

None

Notes

None

show efmoam statistics

Displays IEEE 802.3ah/OAM statistics.

Syntax

```
show efmoam statistics [port <port list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Displays the IEEE 802.3ah/OAM statistics for the specified port in list format.

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

Behavior when this parameter is omitted:

Statistics for all IEEE 802.3ah/OAM frames (OAMPDUs) are displayed by port.

Example

The following figure shows an example of displaying statistics for all configured IEEE 802.3ah/OAM ports.

Figure 42-2: Displaying the IEEE 802.3ah/OAM statistics

```
>show efmoam statistics
Date 20XX/10/02 23:59:59 UTC
Port 1/0/1 [detection]
  OAMPDUs   :Tx       =       295  Rx       =       295
             Invalid  =         0  Unrecogn.=         0
  TLVs      :Invalid  =         0  Unrecogn.=         0
  Info TLV  :Tx_Local =       190  Tx_Remote=       105  Rx_Remote=       187
             Timeout  =         3  Invalid  =         0  Unstable =         0
  Inactivate:TLV      =         0  Timeout  =         0
Port 1/0/2 [active]
  OAMPDUs   :Tx       =       100  Rx       =       100
             Invalid  =         0  Unrecogn.=         0
  TLVs      :Invalid  =         0  Unrecogn.=         0
  Info TLV  :Tx_Local =       100  Tx_Remote=       100  Rx_Remote=       100
             Timeout  =         0  Invalid  =         0  Unstable =         0
  Inactivate:TLV      =         0  Timeout  =         0
Port 1/0/3 [passive]
  OAMPDUs   :Tx       =       100  Rx       =       100
             Invalid  =         0  Unrecogn.=         0
  TLVs      :Invalid  =         0  Unrecogn.=         0
  Info TLV  :Tx_Local =         0  Tx_Remote=       100  Rx_Remote=       100
             Timeout  =         0  Invalid  =         0  Unstable =         0
  Inactivate:TLV      =         0  Timeout  =         0
>
```

Display items

Table 42-2: Items displayed for the IEEE 802.3ah/OAM statistics

Item	Meaning	Displayed detailed information
Port	Port information	Switch number/NIF number/port number of the port whose information is to be displayed
UDLD status	UDLD behavior status by the IEEE 802.3ah/ UDLD function for each port	detection: Indicates that a failure is detected.

Item	Meaning	Displayed detailed information
		active: Indicates that Information OAMPDU frames are sent and responded to. passive: Only OAMPDU frames are responded to.
OAMPDUs	Statistics for frames	—
Tx	Number of OAMPDUs that have been sent for each port	0 to 4294967295
Rx	Number of OAMPDUs that have been received for each port	0 to 4294967295
Invalid	Number of OAMPDUs that have been received but were discarded because they were invalid	0 to 4294967295
Unrecogn.	Number of unsupported OAMPDUs that have been received	0 to 4294967295
TLVs	TLV statistics	—
Invalid	Number of TLVs that were determined as having format errors and discarded	0 to 4294967295
Unrecogn.	Number of TLVs that conform to standards but cannot be recognized by the current version	0 to 4294967295
Info TLV	TLV statistics for Information OAMPDU frames	—
Tx_Local	Number of times that Local Information TLV was sent	0 to 4294967295
Tx_Remote	Number of times that Local Information TLV from the partner device was received and Remote Information TLV was edited and then sent	0 to 4294967295
Rx_Remote	Number of received Local Information TLVs for responses from the partner device	0 to 4294967295
Timeout	Number of times that response timeout occurred on a port	0 to 4294967295
Invalid	Number of TLVs that were determined as having format errors and discarded	0 to 4294967295
Unstable	Number of times that control frames were received from a different device on a currently connected port	0 to 4294967295 If this number is updated, multiple devices might be connected via a hub.
Inactivate	Statistics for failure detections	—
TLV	Number of times that failures showing the received TLV contents were detected	0 to 4294967295
Timeout	Number of times that failures were detected through consecutive response timeouts	0 to 4294967295

Impact on communication

None

Notes

Ports on which no OAMPDUs have been sent or received in passive mode are not displayed.

clear efmoam statistics

Clears IEEE 802.3ah/OAM statistics.

Syntax

```
clear efmoam statistics [port <port list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Clears the IEEE 802.3ah/OAM statistics for the specified port.

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

Behavior when this parameter is omitted:

All IEEE 802.3ah/OAM statistics for the Switch are cleared.

Example

Figure 42-3: Clearing the IEEE 802.3ah/OAM statistics

```
> clear efmoam statistics
>
```

Display items

None

Impact on communication

None

Notes

None

restart efmoam

Restarts IEEE 802.3ah/OAM.

Syntax

```
restart efmoam [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts IEEE 802.3ah/OAM without displaying a restart confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file when the program is restarted.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

After the restart confirmation message is output, IEEE 802.3ah/OAM is restarted.

Example

Figure 42-4: Restarting the IEEE 802.3ah/OAM program

```
> restart efmoam
IEEE802.3ah/OAM program restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Notes

1. The storage directory and the name of the core file are as follows:

   Storage directory: /usr/var/core/

   Core file: efmoamd.core

   If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

2. While the device is operating with the udld parameter specified by the "efmoam active" configuration command in the partner device, when the status of multiple VLANs is being changed concurrently, a unidirectional link failure might be incorrectly detected in the partner device.

dump protocols efmoam

Outputs to a file detailed event trace information and control table information collected for IEEE 802.3ah/OAM.

Syntax

```
dump protocols efmoam
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 42-5: Taking a dump for IEEE 802.3ah/OAM

```
> dump protocols efmoam
>
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of the output dump file are as follows.

Storage directory: /usr/var/efmoam/

File: efmoamd_dump.gz

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

43 CFM

l2ping

This command can be used to determine whether the MEP of the Switch can communicate with a remote MEP or MIP.

Syntax

```
l2ping {remote-mac <mac address> | remote-mep <mepid>} domain-level <level> ma <no.> mep <mepid
> [count <count>] [timeout <seconds>] [framesize <size>]
```

Input mode

User mode and administrator mode

Parameters

{remote-mac <mac address> | remote-mep <mepid>}

remote-mac <mac address>

Specify the MAC address of the remote MEP or MIP whose connectivity you want to verify.

remote-mep <mepid>

Specify the MEP ID of the remote MEP whose connectivity you want to verify. For this parameter, you can specify a remote MEP that can be checked by a CC.

domain-level <level>

Specify the domain level whose connectivity you want to verify. For this parameter, you can specify a domain level that was set by a configuration command.

ma <no.>

Specify the MA ID number whose connectivity you want to verify. For this parameter, you can specify an MA ID number that was set by using a configuration command.

mep <mepid>

Specify the MEP ID of the Switch's MEP from which you want to verify connectivity. For this parameter, you can specify an MEP ID that was set by a configuration command.

count <count>

Sends loopback messages for the number of times specified. The specifiable values are from 1 to 5.

Behavior when this parameter is omitted:

Loopback messages are sent only five times.

timeout <seconds>

Specify the wait time for a response in seconds. The specifiable values are from 1 to 60.

Behavior when this parameter is omitted:

The wait time for a response is 5 seconds.

framesize <size>

Specify the number of bytes of data to be added to the CFM PDU to be sent. The specifiable values are from 1 to 9192.

Behavior when this parameter is omitted:

The number of bytes of data to be added is 40 bytes, and the CFM PDU that is sent is 64 bytes.

Example

The following figure shows an example of executing the "l2ping" command.

Figure 43-1: Example of executing the l2ping command

```
>l2ping remote-mep 1010 domain-level 7 ma 1000 mep 1020 count 3
L2ping to MP:1010(0012.e220.00a3) on Level:7  MA:1000  MEP:1020  VLAN:20
Time:20XX/03/10 19:10:24
1: L2ping Reply from 0012.e220.00a3  64bytes  Time=  751 ms
2: L2ping Reply from 0012.e220.00a3  64bytes  Time=  752 ms
3: L2ping Reply from 0012.e220.00a3  64bytes  Time=  753 ms

--- L2ping Statistics ---
  Tx L2ping Request :    3  Rx L2ping Reply :    3  Lost Frame  :   0%
  Round-trip Min/Avg/Max : 751/752/753 ms
>
```

Display items

Table 43-1: Items displayed for the l2ping command

Item	Meaning	Displayed detailed information
L2ping to MP:<remote mp>	The MAC address of the destination remote MEP or MIP.	The MAC address of the destination remote MEP or MIP. <remote mac address>: When the MAC address of the destination remote MEP or MIP is specified. <remote mep id>(<remote mac address>): When the destination remote MEP ID is specified.
Level	Domain level	0 to 7
MA	MA ID number	MA ID number configured in the configuration
MEP	MEP ID	MEP ID for the Switch
VLAN	VLAN ID	Source VLAN ID
Time	Send time	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second
<count>	Test number	Test number
L2ping Reply from <mac address>	MAC address of the replying MP	The MAC address of the remote MEP or MIP that replied.
bytes	Number of received bytes	Number of bytes starting from the common CFM header and ending with End TLV of the CFM PDU
Time	Response time	The time from the transmission of a loopback message until a loopback reply is received
Request Timed Out.	Reply wait timeout	Indicates that no reply was received within the reply wait time.
Transmission failure.	Transmission failure	Indicates that a message could not be sent from the source VLAN.
Tx L2ping Request	Number of loopback messages that were sent	—
Rx L2ping Reply	Number of loopback replies that were received	Number of replies that were received normally from the remote MEP or MIP

Item	Meaning	Displayed detailed information
Lost Frame	Percentage of lost frames (%)	—
Round-trip Min/Avg/Max	Minimum, average, and maximum response times	—

Impact on communication

None

Notes

- To halt execution of this command, press Ctrl + C.
- This command cannot be used concurrently by multiple users.
- If you want to specify 1477 bytes or more for the framesize parameter, use the "mtu" or "system mtu" configuration command to set the MTU value for jumbo frames to 1500 bytes or more.
- To verify connectivity, use the MAC address for the remote MP. Even when remote-mep is specified, the connectivity is verified by using the MAC address that corresponds to the MEP ID. Therefore, even when the specified MEP ID does not exist, due to a configuration change or another reason, a reply is sent if an MEP or MIP has that MAC address.

l2traceroute

Verifies the route from the Switch's MEP to a remote MEP or MIP.

Syntax

```
l2traceroute {remote-mac <mac address> | remote-mep <mepid>} domain-level <level> ma <no.> mep
<mepid> [timeout <seconds>] [ttl <ttl>]
```

Input mode

User mode and administrator mode

Parameters

{remote-mac <mac address> | remote-mep <mepid>}

remote-mac <mac address>

Specify the MAC address of the destination remote MEP or MIP whose route you want to verify.

remote-mep <mepid>

Specify the destination remote MEP ID of the destination remote MEP that you want to verify the route to. For this parameter, you can specify a remote MEP ID that can be checked by a CC.

domain-level <level>

Specify the domain level for which you want to verify there is a route. For this parameter, you can specify a domain level that was set by a configuration command.

ma <no.>

Specify the MA ID number of the MA that you want to verify the route to. For this parameter, you can specify an MA ID number that was set by using a configuration command.

mep <mepid>

Specify the MEP ID of the Switch from which you want to verify the route. For this parameter, you can specify an MEP ID that was set by a configuration command.

timeout <seconds>

Specify the wait time for a response in seconds. The specifiable values are from 1 to 60.

Behavior when this parameter is omitted:

The wait time for a response is 5 seconds.

ttl <ttl>

Specify the maximum time-to-live (the maximum number of hops) for the linktrace message. The specifiable values are from 1 to 255.

Behavior when this parameter is omitted:

The maximum number of hops is 64.

Example

The following figure shows an example of executing the "l2traceroute" command.

Figure 43-2: Example of executing the l2traceroute command

```
>l2traceroute remote-mep 1010 domain-level 7 ma 1000 mep 1020 ttl 255
L2traceroute to MP:1010(0012.e220.00a3) on Level:7  MA:1000  MEP:1020  VLAN:20
Time:20XX/03/17 10:42:20
```

```
254  0012.e220.00c2  Forwarded
253  0012.e210.000d  Forwarded
252  0012.e220.00a3  NotForwarded  Hit
>
```

Display items

Table 43-2: Items displayed for the l2traceroute command

Item	Meaning	Displayed detailed information
L2traceroute to MP:<remote mp>	The MAC address of the destination remote MEP or MIP.	The MAC address of the destination remote MEP or MIP. <remote mac address>: When the MAC address of the destination remote MEP or MIP is specified. <remote mep id>(<remote mac address>): When the destination remote MEP ID is specified.
Level	Domain level	0 to 7
MA	MA ID number	MA ID number configured in the configuration
MEP	MEP ID	MEP ID for the Switch
VLAN	VLAN ID	Source VLAN ID
Time	Send time	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second
<ttl>	Time to Live	0 to 255
<remote mac address>	MAC address of the replying MP	The MAC address of the MEP or MIP that replied during route verification
Forwarded	Linktrace message forwarded	Indicates that the replying MP forwarded the linktrace message.
NotForwarded	Linktrace message not forwarded	Indicates that the replying MP did not forward the linktrace message.
Hit	Reply from the destination remote MEP or MIP	Indicates that the reply was from the destination remote MEP or MIP.
Transmission failure.	Transmission failure	Indicates that a message could not be sent from the source VLAN.

Impact on communication

None

Notes

- To halt execution of this command, press Ctrl + C.
- This command cannot be used concurrently by multiple users.
- If you execute this command multiple times for the same remote MP, only the last execution result is retained in the linktrace database.
- Information about some replies is not displayed if those replies are received after being forwarded by a number of devices that exceeds the number of devices on the routes that can be registered in the linktrace database.

- The MAC address of the remote MP is used to verify the route. Even when remote-mep is specified, the route is verified by using the MAC address that corresponds to the MEP ID. Therefore, even when the specified MEP ID does not exist, due to a configuration change or another reason, a reply is sent if an MEP or MIP has that MAC address.

show cfm

Displays the configuration information for domains and MPs, and the CFM information related to detected failures.

Syntax

```
show cfm [{[domain-level <level>] [ma <no.>] [mep <mepid>] | summary}]
```

Input mode

User mode and administrator mode

Parameters

{[domain-level <level>] [ma <no.>] [mep <mepid>] | summary}

domain-level <level>

Displays CFM information for the specified domain level.

ma <no.>

Displays CFM information for the specified MA ID number.

mep <mepid>

Displays CFM information for the specified MEP ID.

Behavior when each parameter is omitted:

Only the CFM information conforming to the specified parameter condition can be displayed. If the parameter is not specified, the CFM information is displayed with no condition applied. If multiple parameters are specified, the CFM information conforming to the conditions will be displayed.

summary

Displays the number of MPs and CFM ports that can be accommodated.

Behavior when this parameter is omitted:

All CFM information is displayed.

Example 1

The following figure shows an example of displaying the CFM configuration information.

Figure 43-3: Example of displaying the CFM configuration information

```
>show cfm
Date 20XX/03/15 18:32:10 UTC
Domain Level 3 Name(str): ProviderDomain_3
  MA 300   Name(str) : Tokyo_to_Osaka
    Primary VLAN:300   VLAN:10-20,300
    CC:Enable   Interval:1min
    Alarm Priority:2  Start Time: 2500ms  Reset Time:10000ms
    MEP Information
      ID:8012  UpMEP    CH1 (Up)    Enable   MAC:0012.e200.00b2  Status:Timeout
  MA 400   Name(str) : Tokyo_to_Nagoya
    Primary VLAN:400   VLAN:30-40,400
    CC:Enable   Interval:1min
    Alarm Priority:2  Start Time: 2500ms  Reset Time:10000ms
    MEP Information
      ID:8014  DownMEP  0/21(Up)    Disable  MAC:0012.e220.0040  Status:-
  MIP Information
      0/12(Up)    Enable   MAC:0012.e200.0012
```

```
      0/22(Down)  Disable  MAC:-
Domain Level 4 Name(str): ProviderDomain_4
  MIP Information
      CH8(Up)     Enable   MAC:0012.e220.00b2
>
```

Display items in Example 1

Table 43-3: Items displayed for the CFM configuration information

Item	Meaning	Displayed detailed information
Domain Level <level>	Domain level and domain name	<level>: Indicates the domain level. Name:-: Indicates that the domain name is not used. Name(str):<name>: Indicates that a character string is used for the domain name. Name(dns):<name>: Indicates that the domain name server name is used for the domain name. Name(mac):<mac>(<id>): Indicates that the MAC address and ID are used for the domain name.
MA <no.>	MA ID number and MA name	<no.>: Indicates the MA ID number when the configuration was set. Name(str):<name>: Indicates that a character string is used for the MA name. Name(id):<id>: Indicates that a numeric value is used for the MA name. Name(vlan):<vlan id>: Indicates that the VLAN ID is used for the MA name.
Primary VLAN	Primary VLAN ID	The primary VLAN in the VLANs belonging to the MA. "-" is displayed if the primary VLAN has not been configured.
VLAN	VLAN ID	VLAN ID of the VLAN belonging to the MA. "-" is displayed if no VLANs have been configured.
CC	Behavior status of the CC	Enable: CC is enabled. Disable: CC is disabled.
Interval	CCM sending interval	1s: The CCM sending interval is 1 second. 10s: The CCM sending interval is 10 seconds. 1min: The CCM sending interval is 1 minute. 10min: The CCM sending interval is 10 minutes. "-" is displayed if CC is disabled.
Alarm Priority	Failure detection priority	Priority of failures for which alarms are generated. If a failure whose level is equal to or higher than the priority that has been set is detected, an alarm is reported. • 0: Indicates that no alarms are reported. • 1: Indicates that a failure was detected on the remote MEP. • 2: Indicates a port failure on the remote MEP. • 3: Indicates a CCM timeout. • 4: Indicates that an invalid CCM was received from the remote MEP in the MA. • 5: Indicates that a CCM was received from another MA. "-" is displayed if CC is disabled.

Item	Meaning	Displayed detailed information
Start Time	Time from the detection of a failure until an alarm is generated	2500-10000ms: The time elapsed from the detection of a failure until an alarm is generated. "-" is displayed if CC is disabled.
Reset Time	Time from the detection of a failure until an alarm is canceled	2500-10000ms: The time elapsed from the detection of a failure until an alarm is canceled. "-" is displayed if CC is disabled.
MEP Information	MEP information	—
ID	MEP ID	MEP ID for the Switch
UpMEP	Up MEP	MEP facing the relay side
DownMEP	Down MEP	MEP facing the line
<nif no.>/<port no.>	Port number	MEP port number
CH<channel group number>	Channel group number	MEP channel group number
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
Enable	CFM on a port is enabled.	—
Disable	CFM on a port is disabled.	—
MAC	MEP MAC address	"-" is displayed if the status of the port to which the MEP belongs is Down.
Status	Status of failure detection on the MEP	The highest-level failure of the failures detected by MEP is displayed. • OtherCCM: Indicates that a CCM was received from another MA. • ErrorCCM: Indicates that a CCM that contains an invalid MEP ID, or a CCM with an invalid CCM sending interval, was received. • Timeout: Indicates a CCM timeout. • PortState: Indicates that a CCM reporting a port failure was received. • RDI: Indicates a CCM reporting failure detection was received. "-" is displayed if no failure has been detected.
MIP Information	MIP information	—
<nif no.>/<port no.>	Port number	MIP port number
CH<channel group number>	Channel group number	MIP channel group number
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.

Item	Meaning	Displayed detailed information
Enable	CFM on a port is enabled.	—
Disable	CFM on a port is disabled.	—
MAC	MIP MAC address	"-" is displayed if the status of the port to which the MIP belongs is Down.

Example 2

The following figure shows an example of displaying the number of entities accommodated in the CFM configuration.

Figure 43-4: Example of displaying the number of entities accommodated in the CFM configuration

```
>show cfm summary
Date 20XX/03/14 18:32:20 UTC
DownMEP Counts    :       2
UpMEP Counts      :       2
MIP Counts        :       5
CFM Port Counts   :       9
>
```

Display items in Example 2

Table 43-4: Items displayed for the number of entities accommodated in the CFM configuration

Item	Meaning	Displayed detailed information
DownMEP Counts	Number of Down MEPs	Number of Down MEPs set in the configuration
UpMEP Counts	Number of Up MEPs	Number of Up MEPs set in the configuration
MIP Counts	Number of MIPs	Number of MIPs set in the configuration
CFM Port Counts	Total number of CFM ports	Total number of VLAN ports to which CFM frames are sent out of primary VLANs for MA (For MA for which only Down MEP is configured, total number of Down MEP's VLAN ports. For MA that contains Up MEPs, total number of all VLAN ports of the primary VLAN).

Impact on communication

None

Notes

None

show cfm remote-mep

Displays the configuration of a remote MEP that has been detected by the CC function of CFM, and the monitoring status of connection between the Switch's MEP and the remote MEP.

Syntax

```
show cfm remote-mep [domain-level <level>] [ma <no.>] [mep <mepid>] [remote-mep <mepid>] [detai
l]
```

Input mode

User mode and administrator mode

Parameters

domain-level <level>

Displays the remote MEP information for the specified domain level.

ma <no.>

Displays the remote MEP information for the specified MA ID number.

mep <mepid>

Displays the remote MEP information for the specified MEP ID.

remote-mep <mepid>

Displays information for the specified remote MEP ID.

Behavior when each parameter is omitted:

This command can display only the information relevant to the condition applied by a parameter that has been set. If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information conforming to the conditions will be displayed.

detail

Displays detailed remote MEP information.

Behavior when this parameter is omitted:

Summary information about the remote MEP is displayed.

Behavior when all parameters are omitted:

Summary information about all remote MEPs is displayed.

Example

The following figure shows an example of displaying detailed remote MEP information.

Figure 43-5: Example of displaying the detailed remote MEP information

```
> show cfm remote-mep detail
Date 20XX/03/20 18:19:03 UTC
Total RMEP Counts:      4
Domain Level 3 Name(str): ProviderDomain_3
  MA 100   Name(str) : Tokyo_to_Osaka
    MEP ID:101   0/20(Up)    Enable   Status:Timeout
      RMEP Information  Counts:  2
      ID:3     Status:Timeout     MAC:0012.e220.1224  Time:20XX/03/20 17:55:20
        Interface:Up               Port:Forwarding    RDI:On
        Chassis ID Type:MAC        Info: 0012.e220.1220
      ID:15    Status:-           MAC:0012.e200.005a  Time:20XX/03/20 18:04:54
```

```
        Interface:Up              Port:Forwarding    RDI:-
        Chassis ID Type:MAC       Info: 0012.e200.0050
>
```

Display items

Table 43-5: Items displayed for the detailed remote MEP information

Item	Meaning	Displayed detailed information
Total RMEP Counts	Total number of remote MEPs	—
Domain Level <level>	Domain level and domain name	<level>: Indicates the domain level. Name:-: Indicates that the domain name is not used. Name(str):<name>: Indicates that a character string is used for the domain name. Name(dns):<name>: Indicates that the domain name server name is used for the domain name. Name(mac):<mac>(<id>): Indicates that the MAC address and ID are used for the domain name.
MA <no.>	MA ID number and MA name	<no.>: Indicates the MA ID number when the configuration was set. Name(str):<name>: Indicates that a character string is used for the MA name. Name(id):<id>: Indicates that a numeric value is used for the MA name. Name(vlan):<vlan id>: Indicates that the VLAN ID is used for the MA name.
MEP ID	MEP ID for the Switch	—
<nif no.>/<port no.>	Port number	MEP port number
CH<channel group number>	Channel group number	MEP channel group number
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
Enable	CFM on a port is enabled.	—
Status	The status of failure detection on the Switch's MEP	Displays a failure with the highest priority detected by the Switch's MEP. • OtherCCM: Indicates that a CCM was received from another MA. • ErrorCCM: Indicates that a CCM that contains an invalid MEP ID, or a CCM with an invalid CCM sending interval, was received. • Timeout: Indicates a CCM timeout. • PortState: Indicates that a CCM reporting a port failure was received. • RDI: Indicates a CCM reporting failure detection was received. "-" is displayed if no failure has been detected.

Item	Meaning	Displayed detailed information
RMEP Information	Remote MEP information	—
Counts	Number of remote MEPs	—
ID	Remote MEP ID	—
Status	The status of failure detection in the remote MEP	Displays a remote MEP failure with the highest priority. • OtherCCM: Indicates that a CCM was received from another MA. • ErrorCCM: Indicates that a CCM that contains an invalid MEP ID, or a CCM with an invalid CCM sending interval, was received. • Timeout: Indicates a CCM timeout. • PortState: Indicates that a CCM reporting a port failure was received. • RDI: Indicates a CCM reporting failure detection was received. "-" is displayed if no failure has been detected.
MAC	MAC address of the remote MEP	—
Time	The time when a CCM was last received	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second
Interface	The status of the remote MEP interface	The status of InterfaceStatus in the CCM that was last received. • Up: Indicates that the VLAN is in Up status. • Down: Indicates that the VLAN is in Down status. • Testing: Indicates that the test is being performed. • Unknown: The status is unknown. • Dormant: Waiting for an external event • NotPresent: There is no component for the interface. • LowerLayerDown: Indicates that the status of the lower-layer interface is Down. "-" is displayed if this information is not found in the received CCM.
Port	The status of the remote MEP port	The status of PortStatus in the CCM that was last received. • Forwarding: Forwarding status • Blocked: Blocking status "-" is displayed if this information is not found in the received CCM.
RDI	The status of failure detection in the remote MEP	Indicates that a failure has been detected by the remote MEP. This is the status of the RDI field in the CCM that was last received. • On: Indicates that a failure is being detected. "-" is displayed if no failure has been detected.
Chassis ID	Chassis ID of the remote MEP	Displays the chassis ID information in the CCM that was last received.
Type	Subtype of the chassis ID	Type of the information displayed for Info. • CHAS-COMP: Indicates that entPhysicalAlias of the Entity MIB is displayed for Info. • CHAS-IF: Indicates that ifAlias of the interface MIB is displayed for Info.

Item	Meaning	Displayed detailed information
		• PORT: Indicates that portEntPhysicalAlias of the Entity MIB is displayed for Info. • MAC: Indicates that macAddress of the CFM MIB is displayed for Info. • NET: Indicates that networkAddress of the CFM MIB is displayed for Info. • NAME: Indicates that ifName of the interface MIB is displayed for Info. • LOCAL: Indicates that local of the CFM MIB is displayed for Info. "-" is displayed if this information is not found in the received CCM. For this information sent from the Switch, MAC is displayed for Type and the device MAC address is displayed for Info.
Info	Information about the chassis ID	Information displayed for Type. "-" is displayed if this information is not found in the received CCM.

Impact on communication

None

Notes

None

show cfm fault

Displays the type of failure that has been detected by the CC function of CFM, and the information in the CCM that triggered the failure.

Syntax

```
show cfm fault [domain-level <level>] [ma <no.>] [mep <mepid>] [{fault | cleared}] [detail]
```

Input mode

User mode and administrator mode

Parameters

domain-level <level>

Displays the failure information for the specified domain level.

ma <no.>

Displays the failure information for the specified MA ID number.

mep <mepid>

Displays the failure information for the specified MEP ID.

{fault | cleared}

fault

Displays only the failure information being detected.

cleared

Displays only the failure information that has been cleared.

Behavior when each parameter is omitted:

This command can display only the information relevant to the condition applied by a parameter that has been set. If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information conforming to the conditions will be displayed.

detail

Displays detailed information about a failure.

Behavior when this parameter is omitted:

Summary information about a failure is displayed.

Behavior when all parameters are omitted:

Summary information about all failures is displayed.

Example 1

The following figure shows an example of displaying summary information about CFM failures.

Figure 43-6: Example of displaying the failure information

```
>show cfm fault
Date 20XX/03/21 10:24:12 UTC
MD:7  MA:1000  MEP:1000  Fault    Time:20XX/03/21 10:15:21
MD:7  MA:1010  MEP:1011  Cleared  Time:-
MD:6  MA:100   MEP:600   Cleared  Time:-
>
```

Display items in Example 1

Table 43-6: Items displayed for the failure information

Item	Meaning	Displayed detailed information
MD	Domain level	0 to 7
MA	MA ID number	MA ID number configured in the configuration
MEP	MEP ID	MEP ID for the Switch
Fault	A failure is being detected.	—
Cleared	A failure has been cleared.	—
Time	Time when a failure was detected	The time when a failure was detected by the MEP. If multiple failures have been detected, the time each failure was detected is displayed. yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second "-" is displayed if the failure has been cleared.

Example 2

The following figure shows an example of displaying detailed information about CFM failures.

Figure 43-7: Example of displaying the detailed failure information

```
>show cfm fault domain-level 7 detail
Date 20XX/03/21 12:00:15 UTC
MD:7  MA:1000  MEP:1000  Fault
  OtherCCM : -  RMEP:1001 MAC:0012.e220.11a1 VLAN:1000 Time:20XX/03/21 11:22:17
  ErrorCCM : -
  Timeout  : On RMEP:1001 MAC:0012.e220.11a1 VLAN:1000 Time:20XX/03/21 11:42:10
  PortState: -
  RDI      : -
MD:7  MA:1010  MEP:1011  Cleared
  OtherCCM : -
  ErrorCCM : -
  Timeout  : -  RMEP:1001 MAC:0012.e220.22a1 VLAN:200  Time:20XX/03/21 10:22:17
  PortState: -
  RDI      : -
>
```

Display items in Example 2

Table 43-7: Items displayed for the detailed failure information

Item	Meaning	Displayed detailed information
MD	Domain level	0 to 7
MA	MA ID number	MA ID number configured in the configuration
MEP	MEP ID	MEP ID for the Switch
Fault	A failure is being detected.	—
Cleared	A failure has been cleared.	—
OtherCCM	Failure level 5 A CCM was received from another MA.	Indicates that a CCM was received from the remote MEP belonging to another MA. On: A failure was found.

Item	Meaning	Displayed detailed information
		-: No failures were found.
ErrorCCM	Failure level 4 An invalid CCM was received.	Indicates that an invalid CCM was received from the remote MEP belonging to the same MA. The MEP ID or CCM sending interval is incorrect. On: A failure was found. -: No failures were found.
Timeout	Failure level 3 CCM timeout	Indicates that no CCMs were received from the remote MEP. On: A failure was found. -: No failures were found.
PortState	Failure level 2 Failure on the remote MEP port	Indicates that a CCM reporting a port failure was received from the remote MEP. On: A failure was found. -: No failures were found.
RDI	Failure level 1 A failure was detected on the remote MEP.	Indicates that a CCM reporting detection of a failure was received from the remote MEP. On: A failure was found. -: No failures were found.
RMEP	Remote MEP ID	Indicates the remote MEP ID of the CCM that triggered failure detection.
MAC	MAC address of the remote MEP	—
VLAN	VLAN that received a CCM	—
Time	Time when a failure was detected	The time when a failure was detected. yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second

Impact on communication

None

Notes

If the interface for which Down MEP is configured goes Down, failure information of the corresponding MEP is deleted.

show cfm l2traceroute-db

Displays route information acquired by the "l2traceroute" command and information about the MP on the route. The information registered in the linktrace database is displayed.

Syntax

```
show cfm l2traceroute-db [{remote-mac <mac address> | remote-mep <mepid>} domain-level <level>
ma <no.>] [detail]
```

Input mode

User mode and administrator mode

Parameters

{remote-mac <mac address> | remote-mep <mepid>}

remote-mac <mac address>

Specify the MAC address of the destination remote MEP or MIP on the route that will be displayed.

remote-mep <mepid>

Specify the destination remote MEP ID of the destination remote MEP on the route that will be displayed.

domain-level <level>

Specify the domain level of the domain to which the destination remote MEP or MIP belongs.

ma <no.>

Specify the MA ID number of the MA to which the destination remote MEP or MIP belongs.

detail

Displays detailed information about the route and the MP on the route.

Behavior when this parameter is omitted:

Only the route information is displayed.

Behavior when all parameters are omitted:

All route information in the linktrace database is displayed.

Example

The following figure shows an example of displaying detailed linktrace database information.

Figure 43-8: Example of displaying the detailed linktrace database information

```
> show cfm l2traceroute-db remote-mep 2010 domain-level 7  ma 2000 detail
Date 20XX/03/15 10:30:12 UTC
L2traceroute to MP:2010(0012.e220.1040) on Level:7  MA:2000  MEP:2020  VLAN:20
Time:20XX/03/14 17:37:55
63   0012.e220.10a9  Forwarded
  Last Egress : 0012.e210.2400  Next Egress : 0012.e220.10a0
  Relay Action: MacAdrTbl
  Chassis ID    Type: MAC       Info: 0012.e228.10a0
  Ingress Port  MP Address: 0012.e220.10a9 Action: OK
  Egress Port   MP Address: 0012.e220.10aa Action: OK
62   0012.e228.aa38  NotForwarded
  Last Egress : 0012.e220.10a0  Next Egress : 0012.e228.aa30
  Relay Action: MacAdrTbl
  Chassis ID    Type: MAC       Info: 0012.e228.aa30
```

```
  Ingress Port  MP Address: 0012.e228.aa38 Action: OK
  Egress Port   MP Address: 0012.e228.aa3b Action: Down
>
```

Display items

Table 43-8: Items displayed for the detailed linktrace database information

Item	Meaning	Displayed detailed information
L2traceroute to MP:<remote mp>	The MAC address of the destination remote MEP or MIP.	The MAC address of the destination remote MEP or MIP. <remote mac address>: When the MAC address of the destination remote MEP or MIP is specified. <remote mep id>(<remote mac address>): When the destination remote MEP ID is specified.
Level	Domain level	0 to 7
MA	MA ID number	MA ID number configured in the configuration
MEP	MEP ID	MEP ID for the Switch
VLAN	VLAN ID	Source VLAN ID
Time	Send time	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second
<ttl>	Time to Live	0 to 255
<remote mac address>	MAC address of the replying MP	The MAC address of the MEP or MIP that replied during route verification
Forwarded	Linktrace message forwarded	Indicates that the replying MP forwarded the linktrace message.
NotForwarded	Linktrace message not forwarded	Indicates that the replying MP did not forward the linktrace message.
Hit	Reply from the destination remote MEP or MIP	Indicates that the reply was from the destination remote MEP or MIP.
Last Egress	ID of the source device that forwarded a linktrace message	The MAC address that identifies the device that forwarded a linktrace message. "-" is displayed if this information is not found in the received linktrace reply.
Next Egress	ID of the device that received a linktrace message	The MAC address that identifies the device that received a linktrace message. "-" is displayed if this information is not found in the received linktrace reply. The device MAC address is used for sending this information from the Switch to another device.
Relay Action	The processing method for forwarding a linktrace message	The processing method for forwarding a linktrace message • RlyHit: A linktrace message was not forwarded because it had reached the destination (the destination remote MEP or MIP). • MacAdrTbl: A linktrace message was forwarded by using the MAC address table. • MPCCMDB: A linktrace message was forwarded by using the MIPCCM database. "-" is displayed if a linktrace message was not forwarded for a response from a destination other than the MP.

Item	Meaning	Displayed detailed information
Chassis ID	Chassis ID of the replying MP	The chassis ID of the MP that sent a linktrace reply.
Type	Subtype of the chassis ID	Type of the information displayed for Info. • CHAS-COMP: Indicates that entPhysicalAlias of the Entity MIB is displayed for Info. • CHAS-IF: Indicates that ifAlias of the interface MIB is displayed for Info. • PORT: Indicates that portEntPhysicalAlias of the Entity MIB is displayed for Info. • MAC: Indicates that macAddress of the CFM MIB is displayed for Info. • NET: Indicates that networkAddress of the CFM MIB is displayed for Info. • NAME: Indicates that ifName of the interface MIB is displayed for Info. • LOCAL: Indicates that local of the CFM MIB is displayed for Info. "-" is displayed if this information is not found in the received linktrace reply. For this information sent from the Switch, MAC is displayed for Type and the device MAC address is displayed for Info.
Info	Information about the chassis ID	Information displayed for Type. "-" is displayed if this information is not found in the received linktrace reply.
Ingress Port	Information about the MP port that received a linktrace message	—
MP Address	MAC address of the MP that received a linktrace message	The MAC address of the MP that received a linktrace message. "-" is displayed if this information is not found in the received linktrace reply.
Action	Status of the port that received a linktrace message	Displays the status of the MP port of each device, that received the linktrace message. • OK: Indicates the normal status. • Down: Indicates that the VLAN is in Down status. • Blcked: Indicates the Blocked status. • NoVLAN: Indicates that there is no VLAN setting for linktrace messages. "-" is displayed if this information is not found in the received linktrace reply.
Egress Port	Port information for the MP that forwarded a linktrace message	—
MP Address	MAC address of the port used to forward the linktrace message	The MAC address of the port used to send a linktrace message. "-" is displayed if this information is not found in the received linktrace reply.
Action	Status of the port used to forward a linktrace message	The status of the MP port used to forward each device's linktrace message. • OK: Indicates the normal status. • Down: Indicates that the VLAN is in Down status. • Blocked: Indicates the Blocked status. • NoVLAN: Indicates that there is no VLAN setting for linktrace messages.

Item	Meaning	Displayed detailed information
		"-" is displayed if this information is not found in the received linktrace reply.

Impact on communication

None

Notes

Information about some replies is not displayed if those replies are received after being forwarded by a number of devices that exceeds the number of devices on the routes that can be registered in the linktrace database.

show cfm statistics

Shows CFM statistics.

Syntax

```
show cfm statistics [domain-level <level>] [ma <no.>] [mep <mepid>]
```

Input mode

User mode and administrator mode

Parameters

domain-level <level>

Displays the CFM statistics for the specified domain level.

ma <no.>

Displays the CFM statistics for the specified MA ID number.

mep <mepid>

Displays the CFM statistics for the specified MEP ID.

Behavior when each parameter is omitted:

This command can display only the information relevant to the condition applied by a parameter that has been set. If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information conforming to the conditions will be displayed.

Behavior when all parameters are omitted:

All CFM statistics are displayed.

Example

The following figure shows an example of displaying CFM statistics.

Figure 43-9: Example of displaying the CFM statistics

```
>show cfm statistics domain-level 3
Date 20XX/03/15 18:32:10 UTC
Domain Level 3 Name(str): ProviderDomain_3
  MA 300   Name(str) : Tokyo_to_Osaka_300
    MEP ID:10    0/47(Up)    CFM:Disable
      CCM Tx:     80155  Rx:       784  RxDiscard:         6
      LBM Tx:         2  Rx:        11  RxDiscard:         1
      LBR Tx:        12  Rx:         2  RxDiscard:         0
      LTM Tx:         0  Rx:         0  RxDiscard:         0
      LTR Tx:         0  Rx:         0  RxDiscard:         0
                                 Other RxDiscard:         0
  MIP Information
    0/48(Up)    CFM:Enable
      CCM Tx:         -  Rx:         -  RxDiscard:         -
      LBM Tx:         -  Rx:         0  RxDiscard:         1
      LBR Tx:         0  Rx:         -  RxDiscard:         -
      LTM Tx:         -  Rx:         3  RxDiscard:         0
      LTR Tx:         3  Rx:         -  RxDiscard:         -
                                 Other RxDiscard:         0
>
```

Display items

Table 43-9: Items displayed for the CFM statistics

Item	Meaning	Displayed detailed information
Domain Level <level>	Domain level and domain name	<level>: Indicates the domain level. Name:-: Indicates that the domain name is not used. Name(str):<name>: Indicates that a character string is used for the domain name. Name(dns):<name>: Indicates that the domain name server name is used for the domain name. Name(mac):<mac>(<id>): Indicates that the MAC address and ID are used for the domain name.
MA <no.>	MA ID number and MA name	<no.>: Indicates the MA ID number when the configuration was set. Name(str):<name>: Indicates that a character string is used for the MA name. Name(id):<id>: Indicates that a numeric value is used for the MA name. Name(vlan):<vlan id>: Indicates that the VLAN ID is used for the MA name.
MEP ID	MEP ID for the Switch	—
<nif no.>/<port no.>	Port number	MEP port number
CH<channel group number>	Channel group number	MEP channel group number
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
CFM	Behavior status of CFM on the port	The behavior status of CFM on the port to which MEP belongs. Enable: Indicates that CFM on the port is enabled. Disable: Indicates that CFM on the port is disabled.
MIP Information	MIP information	—
<nif no.>/<port no.>	Port number	MIP port number
CH<channel group number>	Channel group number	MIP channel group number
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
CFM	Behavior status of CFM on the port	The behavior status of CFM on the port to which MIP belongs. Enable: Indicates that CFM on the port is enabled. Disable: Indicates that CFM on the port is disabled.

Item		Meaning	Displayed detailed information
CCM	Tx	Number of sent CCMs	"-" is displayed for MIP.
	Rx	Number of received CCMs	"-" is displayed for MIP.
	RxDiscard	Number of discarded CCMs	For an MEP, the following CCMs are discarded: • CCM in invalid format • CCM for another MA • CCM with the same MEP ID as the one set for the Switch • CCM whose sending interval is different from that of the Switch's MA "-" is displayed for MIP.
LBM	Tx	Number of loopback messages that have been sent	"-" is displayed for MIP.
	Rx	Number of loopback messages that have been received	—
	RxDiscard	Number of loopback messages that have been discarded	The following loopback messages are discarded: • A loopback message with an invalid format • A loopback message whose destination MAC address is not the MAC address for the receiving MP or the multicast address for CC • A loopback message whose source MAC address is the multicast address for a CC or a linktrace • A loopback message whose destination MAC address is not the MAC address for the receiving MIP (for an MIP)
LBR	Tx	Number of loopback replies that have been sent	—
	Rx	Number of loopback replies that have been received	"-" is displayed for MIP.
	RxDiscard	Number of loopback replies that have been discarded	For an MEP, the following loopback replies are discarded: • A loopback reply with an invalid format • A loopback reply whose destination MAC address is different from the MAC address of the MEP • A loopback reply whose source MAC address is the multicast address or broadcast address • A loopback reply whose Loopback Transaction Identifier value is different from that in the loopback message that was sent • A loopback reply that was received after the wait time for a response that was set by an operation command expired "-" is displayed for MIP.
LTM	Tx	Number of linktrace messages that have been sent	"-" is displayed for MIP.
	Rx	Number of linktrace messages that have been received	—

Item		Meaning	Displayed detailed information
	RxDiscard	Number of linktrace messages that have been discarded	The following linktrace messages are discarded: • A linktrace message with an invalid format • A linktrace message whose LTM TTL value is 0 • A linktrace message whose destination MAC address is different from the multicast address for linktrace or the MAC address of the receiving MP • A linktrace message that cannot result in a linktrace reply
LTR	Tx	Number of linktrace replies that have been sent	—
	Rx	Number of linktrace replies that have been received	"-" is displayed for MIP.
	RxDiscard	Number of linktrace replies that have been discarded	For an MEP, the following linktrace replies are discarded: • A linktrace reply with an invalid format • A linktrace reply whose destination MAC address is different from the MAC address of the receiving MEP • A linktrace reply whose LTR Transaction Identifier value is different from the value in the linktrace message • A linktrace reply that was received after the wait time for a response that was set by an operation command expired "-" is displayed for MIP.
Other RxDiscard		Number of other CFM PDUs that have been discarded	The following CFM PDUs are counted: • Unsupported CFM PDUs • Loopback replies and linktrace replies received by the MIP

Impact on communication

None

Notes

None

clear cfm remote-mep

Clears remote MEP information.

Syntax

```
clear cfm remote-mep [domain-level <level> [ma <no.> [mep <mepid> [remote-mep <mepid>]]]]
```

Input mode

User mode and administrator mode

Parameters

domain-level <level>

Clears the remote MEP information for the specified domain level.

ma <no.>

Clears the remote MEP information for the specified MA ID number.

mep <mepid>

Clears the remote MEP information for the specified MEP.

remote-mep <mepid>

Clears the information for the specified remote MEP ID.

Behavior when each parameter is omitted:

This command can clear only the information relevant to the condition applied by a parameter that has been set. If no parameter is specified, information is cleared without being limited by any conditions. If multiple parameters are specified, the information conforming to the conditions will be cleared.

Behavior when all parameters are omitted:

All remote MEP information is cleared.

Example

The following figure shows an example of clearing remote MEP information.

Figure 43-10: Example of clearing the remote MEP information

```
> clear cfm remote-mep
>
```

Display items

None

Impact on communication

None

Notes

None

clear cfm fault

Clears CFM failure information.

Syntax

```
clear cfm fault [domain-level <level> [ma <no.> [mep <mepid>]]]
```

Input mode

User mode and administrator mode

Parameters

domain-level <level>

Clears the failure information for the specified domain level.

ma <no.>

Clears the failure information for the specified MA ID number.

mep <mepid>

Clears the failure information for the specified MEP ID.

Behavior when each parameter is omitted:

This command can clear only the information relevant to the condition applied by a parameter that has been set. If no parameter is specified, information is cleared without being limited by any conditions. If multiple parameters are specified, the information conforming to the conditions will be cleared.

Behavior when all parameters are omitted:

All failure information is cleared.

Example

The following figure shows an example of clearing CFM failure information.

Figure 43-11: Example of clearing the CFM failure information

```
> clear cfm fault
>
```

Display items

None

Impact on communication

None

Notes

None

clear cfm l2traceroute-db

Clears CFM linktrace database information.

Syntax

```
clear cfm l2traceroute-db
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure shows an example of clearing CFM linktrace database information.

Figure 43-12: Example of clearing the CFM linktrace database information

```
> clear cfm l2traceroute-db
>
```

Display items

None

Impact on communication

None

Notes

None

clear cfm statistics

Clears the CFM statistics.

Syntax

```
clear cfm statistics [domain-level <level> [ma <no.> [mep <mepid>]]]
clear cfm statistics [domain-level <level> [mip] [port <port list>] [channel-group-number <chan
nel group list>]]
```

Input mode

User mode and administrator mode

Parameters

domain-level <level>

Clears the CFM statistics for the specified domain level.

ma <no.>

Clears the CFM statistics for the specified MA ID number.

mep <mepid>

Clears the CFM statistics for the specified MEP ID.

mip

Clears the CFM statistics for MIPs.

port <port list>

Clears the CFM statistics for the specified port numbers. For details about how to specify <port list> and the specifiable range of values, see "Specifiable values for parameters". Note that you specify <port list> without <switch no.>.

channel-group-number <channel group list>

Clears the CFM statistics for the channel groups specified in list format in the specified link aggregation. For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when each parameter is omitted:

This command can clear only the information relevant to the condition applied by a parameter that has been set. If no parameter is specified, information is cleared without being limited by any conditions. If multiple parameters are specified, the information conforming to the conditions will be cleared.

Behavior when all parameters are omitted:

All CFM statistics are cleared.

Example

The following figure shows an example of clearing CFM statistics.

Figure 43-13: Example of clearing the CFM statistics

```
> clear cfm statistics
>
```

Display items

None

Impact on communication

None

Notes

None

restart cfm

Restarts the CFM program.

Syntax

```
restart cfm [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the CFM program without outputting a restart confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file when the program is restarted.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

After the restart confirmation message is output, the CFM program is restarted.

Example

The following figure shows an example of restarting the CFM program.

Figure 43-14: Example of restarting the CFM program

```
> restart cfm
CFM program restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of the core file are as follows:

Storage directory: /usr/var/core/

Core file: cfmd.core

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

dump protocols cfm

Dumps detailed event trace information and control table information collected by the CFM program to a file.

Syntax

```
dump protocols cfm
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure shows an example of taking a dump of the CFM program.

Figure 43-15: Example of taking a dump of the CFM program

```
> dump protocols cfm
>
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of the output dump file for the collected information are as follows:

Storage directory: /usr/var/cfm/

Output file: cfmd_dump.gz

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

44 LLDP

show lldp

Shows the configuration and neighboring device information for LLDP.

Syntax

```
show lldp [port <port list>] [detail]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Displays LLDP information for the specified port.

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

Behavior when this parameter is omitted:

The LLDP information for all ports is displayed.

detail

Displays the LLDP configuration information for the Switch and the neighboring device information in detail.

Behavior when this parameter is omitted:

The LLDP configuration information for the Switch and the neighboring device information are displayed in a simplified format.

Behavior when all parameters are omitted:

The LLDP configuration information for the Switch and all neighboring device information are displayed in a simplified format.

Example 1

The following figure shows an example of displaying the LLDP configuration information in a simplified format.

Figure 44-1: Example of displaying the LLDP configuration information and neighboring device information in a simplified format

```
> show lldp
Date 20XX/11/09 19:16:20 UTC
Status: Enabled     Chassis ID: Type=MAC             Info=0012.e268.2c21
Interval Time: 30       Hold Count: 4     Std TTL: 120      Draft TTL: 120
Port Counts=3
1/0/1   (CH:1)   Link: Up      Neighbor Counts:    2
1/0/2            Link: Down    Neighbor Counts:    0
1/0/3            Link: Down    Neighbor Counts:    0
>
```

Display items in Example 1

Table 44-1: Simplified display items for the LLDP configuration information and neighboring device information

Item	Meaning	Displayed detailed information
Status	Status of the LLDP function on the Switch	Enabled: The LLDP function is enabled. Disabled: The LLDP function is disabled.

Item	Meaning	Displayed detailed information
Chassis ID	Chassis ID of the Switch	—
Type	Sub type for the chassis ID	MAC: Indicates that a MAC address is displayed for Info.
Info	Information about the chassis ID	MAC address of the Switch
Interval Time	Sending interval for LLDPDUs that has been set on the Switch (in seconds)	5 to 32768
Hold Count	Multiplier for Interval Time, used for calculating the LLDPDU retention time to be reported to neighboring devices	2 to 10
Std TTL	LLDPDU retention time to be reported to neighboring devices running on IEEE Std 802.1AB (in seconds)	11 to 65535
Draft TTL	LLDPDU retention time to be reported to neighboring devices running on IEEE 802.1AB Draft 6 (in seconds)	10 to 65535
Port Counts	Number of ports	Number of ports on which the "lldp enable" configuration command has been set
<switch no.>/<nif no.>/<port no.>	Port number	Switch number/NIF number/port number of the port whose information is to be displayed
CH	Channel group number	This item is displayed if the applicable port belongs to a channel group.
Link	Port status	Up: Indicates that the port status is Up. Down: Indicates that the port status is Down.
Neighbor Counts	Number of items of information on neighboring devices	Number of items of information on neighboring devices that is retained by the applicable port

Example 2

The following figure shows an example of displaying LLDP information when the detail parameter is specified.

Figure 44-2: Example of displaying the detailed LLDP configuration and neighboring device information

```
> show lldp detail
Date 20XX/11/09 19:16:34 UTC
Status: Enabled     Chassis ID: Type=MAC          Info=0012.e268.2c21
Interval Time: 30       Hold Count: 4     Std TTL: 121      Draft TTL: 120
System Name: LLDP1
System Description: ALAXALA AX2340S AX-2340-48T4X [AX2340S-48T4X] Switching software Ver. 1.0 [
OS-L2N]
Management Address: 192.168.100.1
Total Neighbor Counts=2
Total Std Neighbor Counts=1
Total Draft Neighbor Counts=1
Port Counts=3
Port  1/0/1  (CH:1)
  Link: Up      PortEnabled: TRUE     AdminStatus: enabledRxTx
  Std Neighbor Counts:   1    Draft Neighbor Counts:   0
  Port ID: Type=MAC          Info=0012.e298.5cc0
  Port Description: GigabitEther 1/0/1
  Port VLAN ID: 10
  VLAN Name: ID=10,100-102,4093
  Std Neighbor 1      TTL: 110
    Chassis ID: Type=MAC          Info=0012.e268.2505
    System Name: LLDP2
    System Description: ALAXALA AX3660S AX-3660-24T4XW [AX3660S-24T4XW] Switching software Ver.
12.1.G [OS-L3M]
    Port ID: Type=MAC          Info=0012.e298.dc20
    Port Description: GigabitEther 1/0/5
```

```
    Port VLAN ID: 10
    VLAN Name: ID=10
    VLAN Name: ID=100
    VLAN Name: ID=101
    VLAN Name: ID=102
    VLAN Name: ID=4093
Port  1/0/2
  Link: Down    PortEnabled: FALSE    AdminStatus: enabledRxTx
  Std Neighbor Counts:   0    Draft Neighbor Counts:   0
Port  1/0/3
  Link: Up      PortEnabled: TRUE     AdminStatus: enabledRxTx
  Std Neighbor Counts:   1    Draft Neighbor Counts:   0
  Port ID: Type=MAC          Info=9424.e144.56b4
  Port Description: GigabitEther 1/0/47
  Port VLAN ID: 1
  VLAN Name: ID=1
  Std Neighbor 1      TTL: 16
    Chassis ID: Type=MAC          Info=0012.e24e.368e
    System Name: K0M#IP38
   System Description: ALAXALA AX3660S AX-3660-48T4XW [AX3660S-48T4XW] Switching software Ver.
12.1.R [OS-L3M]
    Port ID: Type=MAC          Info=0012.e24e.36be
    Port Description: GigabitEther 1/0/47
    System Capabilities: Bridge, Router
    Enable Capabilities: Bridge, Router
    Port VLAN ID: 1
    VLAN Name: ID=1
>
```

Display items in Example 2

Table 44-2: Items displayed for the detailed LLDP setting information of the device

Item	Meaning	Displayed detailed information
Status	Status of the LLDP function on the Switch	Enabled: The LLDP function is enabled. Disabled: The LLDP function is disabled.
Chassis ID	Chassis ID of the Switch	—
Type	Sub type for the chassis ID	MAC: Indicates that a MAC address is displayed for Info.
Info	Information about the chassis ID	MAC address of the Switch
Interval Time	Sending interval for LLDPDUs that has been set on the Switch (in seconds)	5 to 32768
Hold Count	Multiplier for Interval Time, used for calculating the LLDPDU retention time to be reported to neighboring devices	2 to 10
Std TTL	LLDPDU retention time to be reported to neighboring devices running on IEEE Std 802.1AB (in seconds)	11 to 65535
Draft TTL	LLDPDU retention time to be reported to neighboring devices running on IEEE 802.1AB Draft 6 (in seconds)	10 to 65535
System Name	System name of the Switch	A string set by using the name parameter of the "hostname" configuration command This item is not displayed if the information has not been set in the configuration.
System Description	System description of the Switch	The same string as the string used for the MIB (sysDescr)
Management Address	Management address for LLDP	LLDP management address sent by the Switch IPv4 address or IPv6 address This item is not displayed if the information has not been set in the configuration.

Item	Meaning	Displayed detailed information
Total Neighbor Counts	Total number of neighboring devices connected to the Switch	Number of items of information on neighboring devices retained by the Switch. 0 to 100
Total Std Neighbor Counts	Total number of neighboring devices running on IEEE Std 802.1AB to be displayed	This item does not include the number of neighboring devices running on IEEE 802.1AB Draft 6.
Draft Neighbor Counts	Total number of neighboring devices running on IEEE 802.1AB Draft 6 to be displayed	—
Port Counts	Number of ports	Number of ports on which the "lldp enable" configuration command has been set
Port	Applicable port number	<switch no.>/<nif no.>/<port no.>
CH	Channel group number	This item is displayed if the applicable port belongs to a channel group.
Link	Link status of the applicable port	Up: Indicates that the port status is Up. Down: Indicates that the port status is Down.
PortEnabled	LLDP availability status	TRUE: LLDPDUs can be sent and received. FALSE: LLDPDUs packets cannot be sent or received.
AdminStatus	LLDP management status	Management status of LLDP availability enabledRxTx: LLDPDUs can be sent and received. This item has a fixed value of enabledRxTx because the port information is displayed only for ports for which the "lldp enable" configuration command is executed.
Std Neighbor Counts	Number of neighboring devices running on IEEE Std 802.1AB	Number of items of information on neighboring devices running on IEEE Std 802.1AB, retained by the applicable port. This item does not include the number of neighboring devices running on IEEE 802.1AB Draft 6.
Draft Neighbor Counts	Number of neighboring devices running on IEEE 802.1AB Draft 6.	Number of items of information on neighboring devices running on IEEE 802.1AB Draft 6, retained by the applicable port.
Port ID	Port ID of the applicable port	__#
Type	Sub type for the port ID	MAC: Indicates that a MAC address is displayed for Info.#
Info	Information about the port ID	MAC address of the port#
Port Description	Port description for the applicable port	The same string as the string used for the MIB (ifDescr)#
When running on IEEE Std 802.1AB		
Port VLAN ID	Port VLAN ID of the applicable port	This item is not displayed if there is no Untagged port for the port VLAN.#
Protocol VLAN ID	Port and Protocol VLAN ID of the applicable port	Displays VLAN IDs in list format. This item is not displayed if there is no protocol VLAN.#

Item	Meaning	Displayed detailed information
VLAN Name	VLAN Name of the applicable port	Displays VLAN IDs in list format. This item is not displayed if there is no port VLAN or MAC VLAN.#
When running on IEEE 802.1AB Draft 6		
Tag ID	List of VLANs to which the applicable port belongs	Displays VLAN IDs in list format. Untagged: Untagged setting Tagged: VLAN ID This item is not displayed if the information has not been set in the configuration.#
IPv4 Address	IP address (IPv4) of the applicable port and VLAN ID to be used	Untagged: Untagged setting Tagged: VLAN ID If there is more than one VLAN ID, the youngest VLAN ID is displayed. <ip address>: IPv4 address This item is not displayed if the information has not been set in the configuration.#
IPv6 Address	IP address (IPv6) of the applicable port and VLAN ID to be used	Untagged: Untagged setting Tagged: VLAN ID If there is more than one VLAN ID, the youngest VLAN ID is displayed. <ip address>: IPv6 address This item is not displayed if the information has not been set in the configuration.#

#: The item is not displayed when Link is in Down state.

Table 44-3: Items displayed for the detailed IEEE Std 802.1AB neighbor information

Item	Meaning	Displayed detailed information
Std Neighbor	ID number of information on neighboring devices running on IEEE Std 802.1AB	Unique value for each port
TTL	Remaining LLDPDU retention time (in seconds)	0 to 65535
Chassis ID	Chassis ID of the neighboring device	—
Type	Sub type for the chassis ID	CHAS-COMP: Indicates that entPhysicalAlias of the Entity MIB is displayed for Info. IF-ALIAS: Indicates that ifAlias of the Interfaces Group MIB is displayed for Info. PORT-COMP: Indicates that EntPhysicalAlias of the Entity MIB when the entPhysicalClass value is port or backplane is displayed for Info. MAC: Indicates that macAddress of the LLDP MIB is displayed for Info. NET: Indicates that networkAddress of the LLDP MIB is displayed for Info. IF-NAME: Indicates that ifName of the Interfaces Group MIB is displayed for Info. LOCL: Indicates that local of the LLDP MIB is displayed for Info.
Info	Information about the chassis ID	Information displayed for the subtype
System Name	System name of the neighboring device	This item is not displayed if it has not been reported.

Item	Meaning	Displayed detailed information
System Description	System description of the neighboring device	This item is not displayed if it has not been reported.
Port ID	Port ID for the neighboring device	—
Type	Sub type for the port ID	IF-ALIAS: Indicates that ifAlias of the Interfaces Group MIB is displayed for Info. PORT-COMP: Indicates that EntPhysicalAlias of the Entity MIB when the entPhysicalClass value is port or backplane is displayed for Info. MAC: Indicates that macAddress of the LLDP MIB is displayed for Info. NET: Indicates that networkAddress of the LLDP MIB is displayed for Info. IF-NAME: Indicates that ifName of the Interfaces Group MIB is displayed for Info. AGENT: Indicates that agent circuit ID of DHCP Relay Agent Information is displayed for Info. LOCL: Indicates that local of the LLDP MIB is displayed for Info.
Info	Information about the port ID	Information displayed for the sub type
Port Description	Port description of the neighboring device	This item is not displayed if it has not been reported.
System Capabilities	Function supported by the neighboring device	Repeater: Repeater function Bridge: Bridge function WLAN-AP: Wireless LAN access point Router: Router function Telephone: Voice call function DOCSIS: DOCSIS cable device Station: Station Only reception only C-VLAN: C-VLAN Component of a VLAN Bridge S-VLAN: S-VLAN Component of a VLAN Bridge TPMR: Two-port MAC relay Other: None of the above Multiple functions are displayed if multiple notifications are reported. This item is not displayed if it has not been reported.
Enable Capabilities	Functions running on the neighboring device	Repeater: Repeater function Bridge: Bridge function WLAN-AP: Wireless LAN access point Router: Router function Telephone: Voice call function DOCSIS: DOCSIS cable device Station: Station Only reception only C-VLAN: C-VLAN Component of a VLAN Bridge S-VLAN: S-VLAN Component of a VLAN Bridge TPMR: Two-port MAC relay Other: None of the above Multiple functions are displayed if multiple notifications are reported. This item is not displayed if it has not been reported.
Management Address	Management address of the neighboring device	This item is not displayed if it has not been reported.
Port VLAN ID	Port VLAN ID of the neighboring device	This item is not displayed if it has not been reported.

Item	Meaning	Displayed detailed information
Protocol VLAN ID	Port and Protocol VLAN ID of the neighboring device	This item is not displayed if it has not been reported.
VLAN Name	VLAN Name of the neighboring device	This item is not displayed if it has not been reported.
ID	VLAN ID of VLAN Name of the neighboring device	This item is not displayed if it has not been reported.
Name	VLAN Name of VLAN Name of the neighboring device	This item is not displayed if it has not been reported.

Table 44-4: Items displayed for the detailed IEEE 802.1AB Draft 6 neighbor information

Item	Meaning	Displayed detailed information
Draft Neighbor	ID number of information on neighboring devices running on IEEE 802.1AB Draft 6	Unique value for each port
TTL	Remaining LLDPDU retention time (in seconds)	0 to 65535
Chassis ID	Chassis ID of the neighboring device	—
Type	Sub type for the chassis ID	CHAS-COMP: Indicates that entPhysicalAlias of the Entity MIB is displayed for Info. CHAS-IF: Indicates that ifAlias of the Interfaces Group MIB is displayed for Info. PORT: Indicates that portEntPhysicalAlias of the Entity MIB is displayed for Info. BACK-COMP: Indicates that backplaneEntPhysicalAlias of the Entity MIB is displayed for Info. MAC: Indicates that macAddress of the LLDP MIB is displayed for Info. NET: Indicates that networkAddress of the LLDP MIB is displayed for Info. LOCL: Indicates that local of the LLDP MIB is displayed for Info.
Info	Information about the chassis ID	Information displayed for the subtype
System Name	System name of the neighboring device	This item is not displayed if it has not been reported.
System Description	System description of the neighboring device	This item is not displayed if it has not been reported.
Port ID	Port ID for the neighboring device	—
Type	Sub type for the port ID	PORT: Indicates that ifAlias of the Interfaces Group MIB is displayed for Info. ENTRY: Indicates that portEntPhysicalAlias of the Entity MIB is displayed for Info. BACK-COMP: Indicates that backplaneEntPhysicalAlias of the Entity MIB is displayed for Info. MAC: Indicates that macAddress of the LLDP MIB is displayed for Info. NET: Indicates that networkAddress of the LLDP MIB is displayed for Info. LOCL: Indicates that local of the LLDP MIB is displayed for Info.
Info	Information about the port ID	Information displayed for the sub type
Port Description	Port description of the neighboring device	This item is not displayed if it has not been reported.

Item	Meaning	Displayed detailed information
Tag ID	List of VLAN IDs of VLANs to which the neighboring device ports belong	Displays VLAN IDs in list format. Untagged: Untagged setting Tagged: VLAN ID This item is not displayed if it has not been reported.
IPv4 Address	IP address (IPv4) allocated to the neighboring device and VLAN ID to be used	Untagged: Untagged setting Tagged: VLAN ID If there is more than one VLAN ID, the youngest VLAN ID is displayed. <ip address>: IPv4 address This item is not displayed if it has not been reported.
IPv6 Address	IP address (IPv6) allocated to the neighboring device and VLAN ID to be used	Untagged: Untagged setting Tagged: VLAN ID If there is more than one VLAN ID, the youngest VLAN ID is displayed. <ip address>: IPv6 address This item is not displayed if it has not been reported.

Impact on communication

None

Notes

None

show lldp statistics

Displays LLDP statistics.

Syntax

```
show lldp statistics [port <port list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Displays LLDP statistics for the specified ports in list format.

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

Behavior when this parameter is omitted:

Statistics for all LLDP frames are displayed by port.

Example

Figure 44-3: Example of displaying the LLDP statistics

```
> show lldp statistics
Date 20XX/11/09 23:09:59 UTC
Port Counts: 3
1/0/1    LLDPDUs    : Tx     =      1300  Rx     =      1294  Invalid=         0
                      Discard=         0  Ageouts=         0
         Discard TLV: TLVs   =         0  Unknown=         0
   Draft LLDPDUs    : Tx     =         0  Rx     =         0  Invalid=         0
         Discard TLV: TLVs   =         0  LLDPDUs=         0
1/0/2    LLDPDUs    : Tx     =       890  Rx     =       547  Invalid=         0
                      Discard=         0  Ageouts=         0
         Discard TLV: TLVs   =         0  Unknown=         0
   Draft LLDPDUs    : Tx     =         0  Rx     =         0  Invalid=         0
         Discard TLV: TLVs   =         0  LLDPDUs=         0
1/0/3    LLDPDUs    : Tx     =        20  Rx     =         0  Invalid=         0
                      Discard=         0  Ageouts=         0
         Discard TLV: TLVs   =         0  Unknown=         0
   Draft LLDPDUs    : Tx     =       869  Rx     =       870  Invalid=         0
         Discard TLV: TLVs   =         0  LLDPDUs=         0
>
```

Display items

Table 44-5: Items displayed for the LLDP statistics

Item	Meaning	Displayed detailed information
Port counts	Number of ports subject to this statistics	—
<switch no.>/<nif no.>/<port no.>	Port number	Switch number, NIF number, or port number of the port whose statistics are to be displayed
Statistics on IEEE Std 802.1AB		
LLDPDUs	Statistics for frames	—

Item	Meaning	Displayed detailed information
Tx	Number of LLDPDUs that have been sent	—
Rx	Number of LLDPDUs that have been received	—
Invalid	Number of invalid LLDPDUs	—
Discard	Number of LLDPDUs that have been discarded	—
Ageouts	Number of LLDPDUs whose neighbor information retention period expired	—
Discard TLV	TLV statistics	—
TLVs	Number of TLVs that have been discarded	—
Unknown	Number of TLVs that cannot be recognized	—
Statistics on IEEE 802.1AB Draft 6		
Draft LLDPDUs	Statistics for frames	—
Tx	Number of LLDPDUs that have been sent	—
Rx	Number of LLDPDUs that have been received	—
Invalid	Number of invalid LLDPDUs	—
Discard TLV	TLV statistics	—
TLVs	Number of TLVs that have been discarded	—
LLDPDUs	Number of LLDPDUs that contain discarded TLVs	—

Impact on communication

None

Notes

None

clear lldp

Clears LLDP neighboring device information.

Syntax

```
clear lldp [port <port list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Clears neighboring device information of the specified port.

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

Behavior when this parameter is omitted:

Information about all neighboring devices retained on the Switch is cleared.

Example

Figure 44-4: Example of executing the clear lldp command

```
> clear lldp
>
```

Display items

None

Impact on communication

None

Notes

None

clear lldp statistics

Clears the LLDP statistics.

Syntax

```
clear lldp statistics [port <port list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Clears LLDP statistics for the specified port.

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

Behavior when this parameter is omitted:

All LLDP statistics for the Switch are cleared.

Example

Figure 44-5: Example of executing the clear lldp statistics command

```
> clear lldp statistics
>
```

Display items

None

Impact on communication

None

Notes

None

restart lldp

Restarts the LLDP program.

Syntax

```
restart lldp [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the LLDP program without displaying a restart confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file when the program is restarted.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

After the restart confirmation message is output, the LLDP program is restarted.

Example

Figure 44-6: Example of restarting LLDP

```
> restart lldp
LLDP restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of the core file are as follows:

Storage directory: /usr/var/core/

Core file: lldpd.core

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

dump protocols lldp

Dumps detailed event trace information and control table information collected by the LLDP program to a file.

Syntax

```
dump protocols lldp
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 44-7: Example of taking an LLDP dump

```
> dump protocols lldp
>
```

Display items

None

Impact on communication

None

Notes

The storage directory and the name of the output dump file are as follows:

Storage directory: /usr/var/lldp/

File: lldpd_dump.gz

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

45 Response Messages

45.1 Response messages

The following tables list and describes the response messages that can be displayed after command execution.

Note that error messages displayed by the entry-error location detection function are not described here. For details on these messages, see "Error messages displayed by the entry-error location detection function".

The Switch assigns names to corresponding interfaces set by configuration. If <interface name> is shown in Response messages, the Switch displays the interface names listed in "Table 1-2: List of interface names assigned by the command in each input format".

45.1.1 Common

Table 45-1: Common response messages

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. <switch no.>: Switch number
Other process is accessing, please try again.	Another process is accessing the device information. Try again after the process ends.
The command cannot be executed. Try again.	The command could not be executed. Re-execute the command.

45.1.2 Switching the command input mode

For details about error messages displayed during configuration editing, see "Configuration Command Reference, 43.1.2 Configuration editing and operation information".

Table 45-2: Response messages on switching the command input mode

Message	Description
Login timed out after 60 seconds.	A timeout occurred because no password was entered within 60 seconds.
Sorry	The mode cannot be changed to administrator mode because a password entry error occurred.

45.1.3 Operation terminals and remote operations

Table 45-3: Response messages on operation terminals and remote operations

Message	Description
?Ambiguous command	Multiple commands contain the specified characters.
?Ambiguous help command <command>	Multiple help commands correspond to the specified characters. <command>: Command name
?Invalid command	The specified command could not be found.
?Invalid help command <command>	The help command applicable to the specified characters could not be found. <command>: Command name

Message	Description
<file name>: No such file or directory	The specified file or directory could not be found. <file name>: The specified file name or directory name
<host>: bad port number -- <port>usage: open host-name [port]	An invalid port number was entered. <port>: Port number
<host>: Host name lookup failure	An unknown host name was entered. <host>: Remote host
<host>: Name or service not known	The connection to the host could not be established because the address could not be resolved. <host>: Remote host
<host>: Unknown host	An unknown host name was entered. <host>: Remote host IP address
<value>: bad value	The parameter value is invalid. <value>: Invalid parameter
Already connected to <host>, use close first.	Communication with the remote device has already been established. To connect to another host, use the "(ftp)close" command or "(ftp)quit" command to stop the communication. <host>: Remote host IP address
bind: Cannot assign requested address	An invalid source IP address has been set.
bind: Invalid argument	An invalid source IP address has been set.
connect to address <host>: Connection refused	The host rejected the connection. <host>: Remote host
connect to address <host>: No route to host	The connection to the host cannot be established because no route exists. <host>: Remote host
connect to address <host>: Operation timed out	The connection timed out. <host>: Remote host
connect: Connection refused	Connection has failed.
connect: No route to host	A connection cannot be established because the routing table to the remote host does not exist.
connect: Operation timed out	The connection timed out.
Connected to <host>.	A connection to <host> was established. <host>: Remote host
Connection closed by foreign host.	The connection was closed from the host.
Connection closed.	The connection was closed from the host.
Error code <number>: <message>	Other TFTP error messages are displayed: <number>: Error code <message>: Error description

Message	Description
getting from <host>:<remote file> to <local file> [<mode>]	<remote file> on <host> is being received as <local file> (with the transfer mode in <mode>). <host>: Remote host <remote file>: Remote file name <local file>: Local file name <mode>: File transfer mode
Login failed.	A login attempt has failed.
Name or service not known	The connection to the host could not be established because the address could not be resolved.
No control connection for command: Bad file descriptor	The command could not be executed because the control connection with the remote host was lost.
No target machine specified, Use connect command.	The connection destination has not been set. Use the "connect" command to set it.
Not connected.	No remote communication.
putting <local file> to <host>:<remote file> [<mode>]	<local file> is being sent to <host> as <remote file> (with the transfer mode in <mode>). <local file>: Local file name <host>: Remote host <remote file>: Remote file name <mode>: File transfer mode
quit for Ctrl+Z pushed.	The command was ended by pressing the Ctrl + Z keys.
Service not available, remote server has closed connection	The command could not be executed because the connection was closed on the remote host.
tftp: <file name>: Is a directory	The specified file is a directory. <file name>: File name
tftp: <file name>: Permission denied	Access permission for the specified file does not exist. <file name>: File name
tftp: bind: Cannot assign requested address	An invalid source IP address has been set.
tftp: bind: Invalid argument	An invalid source IP address has been set.
tftp: No address associated with hostname	The connection to the host could not be established because the address could not be resolved.
tftp: sendto: No route to host	The connection to the remote host cannot be established because no route exists.
tftp: Servname not supported for ai_socktype	An invalid port number was entered.
Transfer timed out.	Transfer timed out. Check the route to the server or the server settings.
Trying <host>:<port> ...	Trying to connect to <host>. <host>: Remote host <port>: Port number
Unable to connect to remote host	The connection to the host could not be established.

Message	Description
Unable to connect to remote host: Connection refused	The host rejected the connection.
Unable to connect to remote host: Connection timed out	The connection timed out.
usage: <parameters>	Shows how to use the command. <parameters>: Command and its arguments

45.1.4 Configurations and file operations

For details about error messages displayed during configuration editing, see "Configuration Command Reference, 43.1.2 Configuration editing and operation information".

Table 45-4: Response messages on configurations and file operations

Message	Description
### List of remote directory.	Gets and displays the list of the specified directory.
### Total <number> lines.	The number of lines of the displayed file is <number> lines.
Can't create file.	The file could not be copied. Check the state such as free capacity, and then re-execute the command.
Can't open /dev/sda1: Device or resource busy Cannot initialize 'C:'	Another process is accessing the memory card. Wait a while, and then re-execute the command.
Can't open /dev/sda1: Device or resource busy Cannot initialize 'C:' Bad target c: <file path>	Another process is accessing the memory card. Wait a while, and then re-execute the command. <file path>: File path to the copy destination on the memory card
Can't open /dev/sda1: No such file or directory Cannot initialize 'C:'	A memory card was not inserted. Make sure that a memory card is inserted into the device properly.
Can't open /dev/sda1: Permission denied Cannot initialize 'C:'	The memory card is being recognized. Wait a while, and then re-execute the command.
Canceled	The "squeeze" command has been canceled.
Configuration file already exist. Configuration file copy to <target file>? (y/n):	That copy-destination file name already exists. This message asks for confirmation on whether or not to overwrite the file. Entering "y" performs the copy. Entering "n" aborts the copy.
Configuration file copy to <target file>? (y/n):	This message asks for confirmation on whether or not to copy a file to the file with the copy-destination file name. Entering "y" performs the copy. Entering "n" aborts the copy.
Data transfer failed. (<reason>)	File transfer from the remote server failed. <reason>: Additional information Re-execute the command with the debug parameter specified for checking.
delete: Delete command can not be used this flash. (<code>)	This command cannot be used for internal flash memory (<internal code>).
delete: Directory is specified.	A directory has been specified.
delete: No flash file is specified.	The specified file does not exist.

Message	Description
delete: No such file or directory.	The specified file does not exist. Or the current directory is not valid.
delete: Not enough flash space.	There is not enough free space on the internal flash memory to execute this command.
delete: Permission denied.	No deletion permission for the specified file exists.
delete: Specify file name.	Specify a file name.
Deleted files will be erased. OK ? (y/n):	Erases deleted files. Enter "y" to erase, otherwise "n" to abort.
dir: Current directory is not flash.	The current directory is not the internal flash memory. Move to an appropriate directory.
Disk full	The file could not be read from, or written to, the memory card. Check the state of the destination such as the free capacity of the memory card and internal flash memory, and then re-execute the command. ("cp" command)
	A directory could not be created in the memory card. Check the state of the memory card such as free capacity, and then re-execute the command. ("mkdir" command)
Done	The erasure has been completed.
Drive 'C:' not supported Cannot initialize 'C:'	A memory card was not inserted. Make sure that a memory card is inserted into the device properly.
Drive 'C:' not supported Cannot initialize 'C:' Bad target c:<file path>	A memory card was not inserted. Make sure that a memory card is inserted into the device properly. <file path>: File path to the copy destination on the memory card
init C: non DOS media Cannot initialize 'C:'	A memory card in unsupported format is installed. Format your memory card.
init C: non DOS media Cannot initialize 'C:' Bad target c:<file path>	A memory card in unsupported format is installed. Format your memory card. <file path>: File path to the copy destination on the memory card
Long file name "<dir name>" already exists. a)utorename A)utorename-all r)ename R)ename-all o)verwrite O)verwrite-all s)kip S)kip-all q)uit (aArRoOsSq):	A file with the same name already exists. Specify the directory name according to the displayed options. <dir name>: Specified directory name • If you specify a or A: The directory to be generated is renamed automatically to create a directory. • If you specify r or R: Re-enter the name of the directory to be generated. The directory is created with the name you re-enter. • If you specify o or O: The target file is deleted and the specified directory is created. • If you specify s, S, or q: No directory is generated.

Message	Description
Long file name "<dir name>" already exists. a)utorename A)utorename-all r)ename R)ename-all s)kip S)kip-all q)uit (aArRsSq):	A directory with the same name already exists. Specify the directory name according to the displayed options. <dir name>: Specified directory name • If you specify a or A: The directory to be generated is renamed automatically to create a directory. • If you specify r or R: Re-enter the name of the directory to be generated. The directory is created with the name you re-enter. • If you specify s, S, or q: No directory is generated.
squeeze: Current directory is not flash.	The current directory is not internal flash memory.
squeeze: No such file or directory.	The current directory is not valid. Move to an appropriate directory.
squeeze: Permission denied.	You do not have access permission for the current directory. Move to an appropriate directory.
squeeze: Squeeze command can not be used this flash.(<code>)	This command cannot be used for internal flash memory (<internal code>).
Squeezing	Erasing the file.
undelete: Current directory is not flash.	The current directory is not the internal flash memory. Move to an appropriate directory.
undelete: Directory is not found for undelete file.	No directory found for restoring undeleted files to. Create a directory for storing the file.
undelete: Exist same name file or directory.	A file or directory that has the same name as that of the specified file already exists in the directory for executing the "undelete" command.
undelete: Invalid index value.	Specify a decimal value for the index value.
undelete: No such file or directory.	The current directory is not valid.
undelete: Not found undelete file.	The specified file does not exist.
undelete: Permission denied of directory for undelete file.	You do not have write permission for the directory where the specified file is to be stored.
undelete: Permission denied.	You do not have access permission for the current directory or specified file.
undelete: Specify correct deleted index number.	Specify a proper index number for the deleted file.
undelete: Specify correct index number [1-64].	Specify a numeric value between 1 and 64 for the index value.
undelete: Specify index number.	Specify an index number.
undelete: Undelete command can not be used this flash. (<code>)	This command cannot be used for internal flash memory (<internal code>).

45.1.5 Login security and RADIUS/TACACS+

Table 45-5: Response message on login security and RADIUS/TACACS+

Message	Description
accounting program failed to be restarted.	An attempt to restart the accounting program by this command failed. Re-execute the command.
already a '<user name>' user	The specified user has already been registered. <user name>: User name
Connection failed to accounting program.	Communication with the accounting program failed. Make sure the accounting settings have been set. If this error occurs frequently, use the "restart accounting" command to restart the accounting program. ("show accounting" command)
	Communication with the accounting program failed. Re-execute the command. If this error occurs frequently, use the "restart accounting" command to restart the accounting program. ("clear accounting" and other commands)
different user.	Users other than that of the same account cannot be forcibly logged out. For details, see item 3 in Notes. Alternatively, the previously login user is currently logging out, and cannot be forced to log out. Wait for 10 or more seconds, and then try again.
File open error.	An attempt to open or access a dump file failed.
invalid Login-No: <login no.>	The specified login number is invalid. <login no.>: Specified login number
kill myself?	The user who is executing this command cannot forcibly log themselves out.
killuser: no user(<tty>)	The user does not exist. <tty>: Terminal information
Last user.	The last user cannot be deleted.
Mismatch; try again.	The new password and the re-entered password are not the same. Re-enter both passwords.
no changes made	The registration of the specified user was canceled. Re-execute the command. ("adduser" command)
	The deletion of the specified user was canceled. Re-execute the command. ("rmuser" command)
No such user '<user name>'.	The specified user has not been registered. <user name>: User name
Now another user is executing user account command, please try again.	Another use is executing a user account related command. Re-execute the command after the related command completes.
Permission denied	The password change is not allowed. ("adduser" command, "password" command)
	The specified user cannot be deleted. ("rmuser" command)

Message	Description
	The password of the specified user cannot be changed. ("clear password" command)
Please don't use an all-lower case password. Unusual capitalization, control characters or digits are suggested.	We recommend that upper-case alphabetic characters, symbols, or numbers be used in addition to lower-case alphabetic characters.
Please don't use an all-lower case password.Unusual capitalization, control characters or digits are suggested.	We recommend that upper-case alphabetic characters, symbols, or numbers be used in addition to lower-case alphabetic characters.
Please enter a longer password.	Enter at least six characters for a password.
Remove myself?	The account of the user executing this command cannot be deleted.
unknown user <user name>	The specified user has not been registered. <user name>: User name

45.1.6 SSH

Table 45-6: Response messages on SSH

Message	Description
'@@@ @ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @ @@@ IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY! Someone could be eavesdropping on you right now (man-in-the-middle attack)! It is also possible that a host key has just been changed. The fingerprint for the <key type> key sent by the remote host is SHA256:<SHA256 fingerprint> MD5:<MD5 fingerprint> Please contact your system administrator. Add correct host key in [/usr]/home/<user>/.ssh/known_hosts to get rid of this message. Offending <key type> key in [/usr]/home/<user>/.ssh/known_hosts:<number> Are you sure you want to continue connecting (yes/no)?	The host key is different from the one of the servers with which a connection is established previously. Check if the host key has been changed on the destination server. If there is no problem, enter yes to connect. <host>: Server name or its address <key type>: Type of the host key <SHA256 fingerprint>: SHA256 fingerprint of the host key <MD5 fingerprint>: MD5 fingerprint of the host key <user>: User name <number>: Line number written in the database file
<host>: Connection closed by remote host.	The connection was disconnected by the remote host.
<key type> key fingerprint is SHA256:<SHA256 fingerprint>. <key type> key fingerprint is MD5:<MD5 fingerprint>. Are you sure you want to continue connecting (yes/no)?	Check the fingerprint of the host key and make sure if you want to establish the connection. <key type>: Type of the host key <SHA256 fingerprint>: SHA256 fingerprint of the host key <MD5 fingerprint>: MD5 fingerprint of the host key

Message	Description
<path>: No such file or directory	<path> specified was not found. <path>: File name
<path>: not a regular file	<path> specified is not a regular file. <path>: File name
<path>: Permission denied	There are no permissions. <path>: File name
Can't execute (<reason>).	The command cannot be executed due to the invalid host key. Alternatively, a command execution error occurred. ("show ssh hostkey" command) <reason>: Internal detailed information [Action] 1. Re-create the host key with the "set ssh hostkey" command. 2. Re-execute the command.
	The command could not be executed. ("set ssh hostkey" and other commands) <reason>: Internal detailed information [Action] Re-execute the command.
Canceled. SSH server's log was NOT cleared.	The clearing of logs was canceled. (The logs were not cleared.)
Cannot download non-regular file: <path>	The specified <path> file is invalid. It cannot be downloaded. <path>: Specified file name
Clear Complete.	The logs were cleared successfully.
Connected to <host>.	A connection has been established. <host>: Host name or address
Connection closed	The line was disconnected.
Connection closed by <host> port <port>	The connection was disconnected by the server. <host>: Server name or its address <port>: Port number
Connection to <host> closed by remote host.	The connection was disconnected by the remote host. <host>: Server name or its address
Connection to <host> closed.	The connection was lost. <host>: Server name or its address
Couldn't stat remote file: <reason>	The specified remote file does not exist. <reason>: Error details
Host key verification failed.	An attempt to verify the host key failed.
Interrupted. Please, Re-try.	Canceled because a signal (such as [Ctrl] + [C]) was received. [Action] Re-execute the command.
Invalid command.	The specified command is invalid.
lost connection	The connection was closed.

Message	Description
No valid SSH1 cipher, using <type> instead.	The SSHv1 encryption method is not valid. <type> is used. <type>: Encryption method
Not tty allocation error.	Specify the -t parameter and allocate a virtual terminal to reconnect.
Permission denied (<authentication method>).	Authentication failed. <authentication method>: Authentication method
Permission denied, please try again.	No permissions are granted. Re-execute the command.
Permission denied.	No permissions are granted.
Protocol major versions differ: <number1> vs. <number2>	The specified version for the SSH protocol is incorrect. <number1>: Version of the protocol on the client <number2>: Version of the protocol on the server
Received disconnect from <host> port <port>:<code>: <message>	The connection was disconnected by the server. <host>: Server name or its address <port>: Port number <code>: Identification code for the SSH protocol <message>: Message from the server
Remote machine has too old SSH software version.	The SSH software on the remote operation terminal is obsolete.
Selected cipher type <type> not supported by server.	The server does not support the specified <type>. <type>: Encryption method
ssh: connect to host <host> port <port>: <reason>	The connection to the host could not be established. <host>: Server name or its address <port>: Port number <reason>: Cause
ssh: Could not resolve hostname <host>: <reason>	The host name could not be resolved. <host>: Host name <reason>: Cause
ssh_exchange_identification: Connection closed by remote host	The connection was disconnected by the server.
subsystem request failed on channel <id>	Could not connect with the specified server over sftp. <id>: Internal information value
The authenticity of host '<host>' can't be established.	The authenticity of the destination server has not been verified. <host>: Server name or its address
The command was canceled.	The deletion of the host key was canceled by the user.
The command was interrupted. Try again.	As either a signal (such as Ctrl + C) was received or an internal error occurred, the creation of the host key was interrupted. ("set ssh hostkey" command) [Action] Re-execute the command.

Message	Description
	As either a signal (such as Ctrl + C) was received or an internal error occurred, the deletion of the host key was interrupted. ("erase ssh hostkey" command) [Action] Re-execute the command.
The hostkey generation is completed.	The host key was generated successfully.
The hostkey generation was canceled.	The creation of the host key was canceled by the user.
The hostkey was erased successfully.	The host key was deleted.
Unable to negotiate with <host> port <port>: <reason>. Their offer: <offer>	The negotiation with the server failed. <host>: Server name or its address <port>: Port number <reason>: Cause <offer>: Server request
WARNING: <key type> key found for host <host> in [/usr]/home/<user>/.ssh/known_hosts: <number> <key type> key fingerprint <fingerprint>.	The host key for the destination server was found (but this time you are trying to connect with it using a different type of host key). <key type>: Type of the host key <host>: Server name or its address <user>: User name <number>: Line number written in the database file <fingerprint>: Fingerprint of the host key
Warning: Permanently added '<host>' (<key type>) to the list of known hosts.	The host key of the destination server was stored in the database of the client. <host>: Server name or its address <key type>: Type of the host key
Warning: remote port forwarding failed for listen port <port>	The remote port forwarding failed. <port>: Designated port
You must specify a path after a <command> command.	The path must be specified after <command>.

45.1.7 Time settings and NTP

Table 45-7: Response messages on time settings and NTP

Message	Description
Connection refused	A connection with the NTP server for the device could not be established.
illegal time format.	The input format of the time is incorrect.
illegal time.	The date and time values are outside the valid range. Set a value within the range.
invalid day of month supplied.	The day value is outside the valid range. Set a value within the range.
invalid hour supplied.	The hour value is outside the valid range. Set a value within the range.
invalid minute supplied.	The minute value is outside the valid range. Set a value within the range.

Message	Description
invalid month supplied.	The month value is outside the valid range. Set a value within the range.
invalid second supplied.	The second value is outside the valid range. Set a value within the range.
No association ID's returned	The NTP server cannot be found.
ntp is not running	NTP is not running.

45.1.8 Device management

Table 45-8: Response messages on device management

Message	Description
another user is executing now.	This command cannot be executed because the "restore" or "ppupdate" command executed by another user is still in progress.
another user is executing update command.	This command cannot be executed because the "restore" or "ppupdate" command executed by another user is still in progress.
Another user is using the 'show tech-support' command. Wait a while, and then try again.	Another user is executing the "show tech-support" command.
Do you want to type a password again? (y/n):	Is the password for administrator mode? When "y" is selected in response to the message, the password can be re-entered. When "n" is selected, the command execution is continued assuming that an incorrect password was entered.
Enter the file name for the log and dump files. :	Specify the name of a log file and dump file. If not specified, a 14-digit number is specified as the file name by using the command execution date and time. Note that the file name entered in response to this message is reflected in <File Name> in subsequent response messages.
Enter the host name of the FTP server. :	Specify a host name. Note that the host name entered in response to this message is reflected in <Host Name> in subsequent response messages.
Enter the password for the administrator mode. :	Enter the password for administrator mode.
Enter the password for the FTP server connection. :	Enter the password for <user name> you entered.
Enter the path name of the FTP server. :	Specify a destination directory name. Note that the destination directory name entered in response to this message is reflected in <Path> in subsequent response messages.
Enter the user name for the FTP server connection. :	Specify a login user name. Note that the login user name entered in response to this message is reflected in <user name> in subsequent response messages.
File transfer ended successfully.	The file transfer ended normally.
Filename is invalid.	The file with the specified name cannot be created. Specify another file name.

Message	Description
Flash memory file write error.	Writing to the internal flash memory failed. Check that the file with the specified name can be created and that there is not enough free space, and then re-execute the command.
ftp transfer failed.	An attempt to transfer the device information by using the "backup ftp" command failed. Check that the file with the specified name can be created and that there is not enough free space, and then re-execute the command.
Restore operation failed.	An attempt to restore the device information failed. An attempt to read the specified file failed, or there might not be enough free space on the disk of the Switch. Check that the specified file is accessible and delete unnecessary files, and then re-execute the command.
Saving file(<file name>) to MC failed.	Writing to the memory card failed. Check that the file with the specified name can be created and that there is not enough free space, and then re-execute the command.
The file is invalid.	The specified file cannot be restored on the Switch. Check that the correct file was specified and it is not corrupt, and then re-execute the command.
The file transfer failed.	An attempt to transfer the file failed. Check the free capacity of the destination and the state of the communication line.
The password for the administrator mode is invalid.	The password for administrator mode specified in the <password> parameter is incorrect.
This command is executable only the start-up from flash memory(primary).	This command can be executed only when normally invoked on the internal flash memory.
Verification failed.	The device information may have changed during backup output, or an attempt to output a file may have failed. Check that the output destination is accessible and then re-execute the command.

If you specify the ftp parameter with the "show tech-support" command, the command shows the same messages as those from the "ftp" command. For these messages, see "Table 45-3: Response messages on operation terminals and remote operations".

45.1.9 Checking internal memory and memory cards

Table 45-9: Response messages on checking internal memory and memory cards

Message	Description
Can't gain access to MC.	The memory card is not inserted, or an attempt to access the memory card failed.

45.1.10 Dump information

Table 45-10: Response messages on dump information

Message	Description
<file name>: No such file or directory.	The specified file does not exist. Or, the specified file is not a dump file.

45.1.11 Memory card operation mode

Table 45-11: Response messages on memory card operation mode

Message	Description
Flash memory file write error.	Writing to the internal flash memory failed.
MC file write error.	Writing to the memory card failed. There might not be enough free space on the memory card or internal flash memory. Delete unnecessary files and then re-execute the command.
MC is busy.	Another process is accessing the memory card. Wait a while, and then re-execute the command.
MC is not inserted.	A memory card was not inserted. Make sure that a memory card is inserted into the device properly. Make sure there is no dust in the memory card slot. If there is dust, wipe it off with a dry cloth and then insert the memory card.
The mc-configuration mode is disabled.	Enable the memory card operation mode.
This command is executable only the start-up from flash memory(primary).	This command can be executed only when normally invoked on the internal flash memory.

45.1.12 Software management

Table 45-12: Response messages on software management

Message	Description
<license key> is not for this system.	The license key is not for this system. <license key.>: License key
A license key cannot be added any more.	The number of optional licenses exceeds the maximum allowed number.
another user is executing now.	This command cannot be executed because the "restore" or "ppupdate" command executed by another user is still in progress.
Can't open <file-name>.	The specified file could not be opened. Specify the correct file name.
extract failed.	Updating has failed. Re-execute the command.
Invalid contents of <file name>.	The contents of the specified license key file are invalid. Specify a valid license key file. <file name>: Specified license key file
Invalid file <file-name>.	The contents of the specified file are invalid. Specify a valid file.
Invalid license key <license key>.	The entered license key is invalid.
Invalid serial number <license key>.	The license key is invalid. <license key>: License key
Invalid serial number <serial no.>	The optional license of the specified serial number does not exist. <serial no.>: Serial number

Message	Description
No such file <file name>	The specified license key file does not exist. <file name>: Specified license key file
OS Type mismatch. Can not apply this package.	The specified file cannot be used because it is intended for a different device.
OS version mismatch. Can not apply this package.	The specified file cannot be used for the Switch.
This license is already registered.	This optional license has already been set.

45.1.13 SNMP

Table 45-13: Response messages on SNMP

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Cannot translate variable class: <MIB Object Name>	The object name <MIB Object Name> is invalid.
Connection failed to SNMP program.	Communication with the SNMP program failed. Re-execute the command.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
make_obj_id_from_dot, bad character : x,y,z	An object ID specified in dot notation contains invalid characters, such as x, y, and z.
no entries.	There are no inform events bound for the SNMP manager.
No match found for <MIB object name>	The applicable <MIB object name> cannot be found by using this command.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.

Message	Description
receive error.	A receive error occurred.
request ID mismatch. Got: <ID1>, expected: <ID2>	A frame whose request ID number of the SNMP frame is <ID2> was expected, but an SNMP frame whose request ID number is <ID1> was received. Alternatively, a timeout occurred during the MIB search.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

45.1.14 Advanced script

Table 45-14: Response messages on advanced scripts

Message	Description
Permission denied. (file name = <file name>)	No read permission for the specified script file exists. <file name>: Script file name
Specified applet name is not registered.	The specified applet name has not been registered.
Specified script is not running.	The specified script has not been started.
The command cannot be executed because you are in user mode.	This command cannot be executed in user mode.
The number of script files exceeds the maximum.	The number of script files exceeds the upper limit.
The number of scripts currently running exceeds the maximum.	The number of currently running scripts exceeded the upper limit.
The number of scripts that started per unit time exceeds the maximum.	The number of scripts that were started per unit time exceeded the upper limit.
The Python script with the specified process ID is not running. (process ID = <pid>)	The Python script with the specified process ID has not started. <pid>: Process ID
The script file exceeds the maximum size.	The size of the script file exceeds the upper limit.
The script file name exceeds the maximum length.	The length of the script file name exceeds the upper limit.
The specified script file already exists.	The specified script file is already installed. If you want to change the script file, delete and then reinstall it.
The specified script file does not exist. (file name = <file name>)	The specified script file does not exist. <file name>: Script file name
The specified script file is not installed. (file name = <file name>)	The specified script file is not installed. <file name>: Script file name
The total size of the script files exceeds the maximum.	The total size of the script files exceeds the upper limit.

45.1.15 Ethernet

Table 45-15: Response messages on Ethernet

Message	Description
<nif no.>/<port no.> is disabled.	The specified port is in disable status due to the configuration. Make sure the specified parameter is correct. <nif no.>: NIF number <port no.>: Port number
<nif no.>/<port no.> is failed.	The specified port has failed. Make sure the specified parameter is correct. <nif no.>: NIF number <port no.>: Port number
<nif no.>/<port no.> is not gigabitethernet.	The interface of the specified port is not gigabitethernet. Make sure the specified parameter is correct. <nif no.>: NIF number <port no.>: Port number
<nif no.>/<port no.> is not tengigabitethernet.	The interface of the specified port is not tengigabitethernet. Make sure the specified parameter is correct. <nif no.>: NIF number <port no.>: Port number
<switch no.>/<nif no.>/<port no.> is already active.	The specified port is already active. The command does not need to be executed if you correctly specified the port. <switch no.>: Switch number <nif no.>: NIF number <port no.>: Port number
<switch no.>/<nif no.>/<port no.> is already inactive.	The specified port is already inactive. The command does not need to be executed if you correctly specified the port. <switch no.>: Switch number <nif no.>: NIF number <port no.>: Port number
<switch no.>/<nif no.>/<port no.> is already initializing.	The specified port is already being initialized. The command does not need to be executed if you correctly specified the port. <switch no.>: Switch number <nif no.>: NIF number <port no.>: Port number
<switch no.>/<nif no.>/<port no.> is disabled.	The specified port is in disable status due to the configuration. Make sure the specified parameter is correct. ("activate" command, "inactivate" command) <switch no.>: Switch number <nif no.>: NIF number <port no.>: Port number
	The command cannot be executed because the port is shut down or the port does not supply power. ("activate power inline" command, "inactivate power inline" command) <switch no.>: Switch number <nif no.>: NIF number <port no.>: Port number

Message	Description
<switch no.>/<nif no.>/<port no.> is failed.	A failure has occurred or a line test is being conducted on the specified port. Make sure the specified parameter is correct. ("activate" command) <switch no.>: Switch number <nif no.>: NIF number <port no.>: Port number
	The specified port is not in active status. Make sure the specified parameter is correct. ("inactivate" command) <switch no.>: Switch number <nif no.>: NIF number <port no.>: Port number
<switch no.>/<nif no.>/<port no.> is not gigabitethernet.	The interface of the specified port is not gigabitethernet. Make sure the specified parameter is correct. <switch no.>: Switch number <nif no.>: NIF number <port no.>: Port number
<switch no.>/<nif no.>/<port no.> is not tengigabitethernet.	The interface of the specified port is not tengigabitethernet. Make sure the specified parameter is correct. <switch no.>: Switch number <nif no.>: NIF number <port no.>: Port number
Connection failed to L2 Manager.	Communication with the L2Manager program failed. Re-execute the command. If the failure occurs frequently, use the "reload" command to restart the device.
Connection failed to Link Aggregation.	Communication with the link aggregation program failed. Re-execute the command. If this message is output frequently, execute the "restart link-aggregation" command to restart the link aggregation program.
Connection failed to LLDP.	Communication with the LLDP program failed. Re-execute the command. If the failure occurs frequently, use the "restart lldp" command to restart the LLDP program.
Connection failed to Ring Protocol.	Communication with the Ring Protocol program failed. Re-execute the command. If this message is output frequently, execute the "restart axrp" command to restart the Ring Protocol program.
Connection failed to Spanning Tree.	Communication with the Spanning Tree program failed. Re-execute the command. If this message is output frequently, execute the "restart spanning-tree" command to restart the Spanning Tree program.
Illegal Port -- <port no.>.	The port number is outside the valid range. Make sure the specified parameter is correct. <port no.>: Port number
Invalid port number.	The port specified as the parameter is not a PoE port. ("activate power inline" command, "inactivate power inline" command)
	The port specified as the parameter is not a PoE port. (This message is also displayed if any non-POE ports are included when multiple ports are specified.) ("show power inline" command)

Message	Description
Line test executing.	A line test is being conducted. To change the status of the specified port to inactive, cancel the line test, and then re-execute the command. To cancel the line test, execute the "no test interfaces" command.
No auto negotiation Port <nif no.>/<port no.>	The specified port is not subject to auto-negotiation. Make sure the specified parameter is correct. <nif no.>: NIF number <port no.>: Port number
No operational Port <port no.>.	The specified port is not in a state in which commands can be executed. Make sure the specified parameter is correct. <port no.>: Port number
No operational port--<port no.>.	The specified port is not in a state in which commands can be executed. Make sure the specified parameter is correct. <port no.>: Port number
No operational Port.	There are no available ports. Make sure the specified parameter is correct.
No support auto negotiation parameter.	The specified port does not support auto-negotiation parameters. Make sure the specified parameter is correct.
Test already executing.	A test is already being conducted on the specified port or another port. The command does not need to be executed if you correctly specified the port. Alternatively, stop the test for the other port, and then re-execute the command.
Test not executing.	No line test has been conducted. Make sure the specified parameter is correct.
This command is not supported with this model.	This command is not supported by this model.

45.1.16 Link aggregation

Table 45-16: Response messages on link aggregation

Message	Description
Connection failed to L2 Manager.	Communication with the L2 Manager program failed. Re-execute the command. If the failure occurs frequently, use the "reload" command to restart the device.
Connection failed to Link Aggregation.	Communication with the link aggregation program failed. Re-execute the command. If this message is output frequently, execute the "restart link-aggregation" command to restart the link aggregation program.
Link Aggregation doesn't seem to be running.	Because the link aggregation program has not started, the command could not be executed. The link aggregation program starts only when link aggregations are set up. If no link aggregations are set up, this message is output. If this message is output when link aggregations have been set up, wait until the link aggregation program is restarted, and then re-execute the command.
Specified channel-group is not configured.	The channel group has not been configured. Check the configuration.

45.1.17 MAC address table

Table 45-17: Response messages on the MAC address table

Message	Description
Command is accepted, but it takes time for setting to hardware.	The command was executed, but it takes time for the settings to be applied to hardware (you do not need to re-execute the command).
Connection failed to L2 Mac Manager.	Communication with the L2MAC manager program failed. Re-execute the command. If this message is output frequently, execute the "restart vlan mac-manager" command to restart the L2MAC manager program.
Connection failed to L2 Manager.	Communication with the L2Manager program failed. Re-execute the command. If the failure occurs frequently, use the "reload" command to restart the device.
Connection failed to Snoopd.	Communication with the IGMP snooping/MLD snooping program failed. Re-execute the command. If this message is output frequently, execute the "restart snooping" command to restart the IGMP snooping/MLD snooping program.
No mac-address-table entry.	There is no information in the MAC address table. Make sure the specified parameter is correct, and then try again.
No operational Port.	There are no available ports. Make sure the specified parameter is correct, and then try again.
Specified VLAN is not configured.	The specified VLAN has not been configured. Make sure the specified parameter is correct, and then try again.

45.1.18 VLAN

Table 45-18: Response messages on VLAN

Message	Description
Connection failed to L2 Mac Manager.	Communication with the L2MAC manager program failed. Re-execute the command. If this message is output frequently, execute the "restart vlan mac-manager" command to restart the L2MAC manager program.
Connection failed to L2 Manager.	Communication with the L2Manager program failed. Re-execute the command. If the failure occurs frequently, use the "reload" command to restart the device.
Connection failed to Link Aggregation.	Communication with the link aggregation program failed. Re-execute the command. If this message is output frequently, execute the "restart link-aggregation" command to restart the link aggregation program.
Connection failed to Ring Protocol.	Communication with the Ring Protocol program failed. Re-execute the command. If this message is output frequently, execute the "restart axrp" command to restart the Ring Protocol program.
Connection failed to Snoopd.	Communication with the IGMP snooping/MLD snooping program failed. Re-execute the command. If this message is output frequently, execute the "restart snooping" command to restart the IGMP snooping/MLD snooping program.

Message	Description
Connection failed to Spanning Tree.	Communication with the Spanning Tree program failed. Re-execute the command. If this message is output frequently, execute the "restart spanning-tree" command to restart the Spanning Tree program.
No MAC address entry.	The relevant MAC address does not exist. Make sure the specified parameter is correct, and then try again.
No operational Port.	There are no available ports. Make sure the specified parameter is correct, and then try again.
No operational VLAN.	There are no available VLANs. Make sure the specified parameter is correct, and then try again.

45.1.19 Spanning tree protocols

Table 45-19: Response messages on spanning tree protocols

Message	Description
Connection failed to Spanning Tree program.	Communication with the Spanning Tree program failed.
File open error.	An attempt to open or access a dump file failed.
No corresponding port information.	No port and channel group information exists as Spanning Tree information.
No corresponding Spanning Tree information.	The relevant Spanning Tree information does not exist.
Spanning Tree is not configured.	The spanning Tree Protocol has not been configured. Check the configuration.
Spanning Tree program failed to be restarted.	The command could not restart the Spanning Tree program. Re-execute the command.
Specified Spanning Tree is not configured.	The specified Spanning Tree Protocol has not been configured. Check the configuration.

45.1.20 Ring Protocol

Table 45-20: Response messages on Ring Protocol

Message	Description
Connection failed to Ring Protocol program.	Communication with the Ring Protocol program failed. Re-execute the command. If this message is output frequently, execute the "restart axrp" command to restart the Ring Protocol program.
File open error.	An attempt to open or access a dump file failed.
Ring Protocol doesn't seem to be running.	The Ring Protocol program is not running. Check the configuration.
Ring Protocol is initializing.	The Ring Protocol is performing initialization. Processing, such as loading configuration entries, has not been completed. Wait a while, and then re-execute the command.
Ring Protocol is not configured.	The Ring Protocol has not been configured. Check the configuration.

Message	Description
Ring Protocol program failed to be restarted.	This command could not restart the Ring Protocol program. Re-execute the command.
Specified Ring ID is not configured:<ring id>.	The specified ring ID has not been configured. <ring id>: Ring ID

45.1.21 IGMP/MLD snooping

Table 45-21: Response messages on IGMP/MLD snooping

Message	Description
<command name> connection failed to snoopd.	Command execution failed because the IGMP snooping/MLD snooping program had not been started. If this message is output when IGMP snooping/MLD snooping is enabled, wait for the IGMP snooping/MLD snooping program to be restarted, and then re-execute the command. <command name>: Name of the entered command
<command name>IGMP snooping not active.	IGMP snooping is not running. <command name>: Name of the entered command
<command name>MLD snooping not active.	MLD snooping is not running. <command name>: Name of the entered command
No operational Port.	The ports specified in <port list> did not include active ones.
No operational VLAN.	There are no available VLANs.
pid file <file name> mangled!	The PID file for the IGMP snooping/MLD snooping program is corrupted. <file name>: PID file name
pid in file <file name> unreasonably small (<pid>)	The PID file for the IGMP snooping/MLD snooping program is corrupted. <file name>: PID file name <pid>: Process ID
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: write: Write error during socket communication read: Read error during socket communication select: Select function error during socket communication
snoopd doesn't seem to be running.	Command execution failed because the IGMP snooping/MLD snooping program had not been started. If this message is output when IGMP snooping/MLD snooping is enabled, wait for the IGMP snooping/MLD snooping program to be restarted, and then re-execute the command.
snoopd failed to terminate.	The "restart snooping" command could not restart the IGMP snooping/MLD snooping program. Re-execute the command.

Message	Description
snoopd restarted after termination: old pid <pid>, new pid <pid>	Command execution failed because the PID was changed during execution of the "restart snooping" command. The IGMP snooping/MLD snooping program might be restarted automatically. If necessary, wait until the program is restarted, and then re-execute the command. <pid>: Process ID
snoopd signaled but still running, waiting 6 seconds more.	The IGMP snooping/MLD snooping program is being restarted by using the "restart snooping" command. Wait a while.
snoopd still running, sending KILL signal.	The Kill signal is being sent to the IGMP snooping/MLD snooping program so that the program can be restarted by using the "restart snooping" command. Wait a while.
snoopd terminated.	The IGMP snooping/MLD snooping program was stopped by the "restart snooping" command. The program will restart automatically. Wait a while.

45.1.22 IPv4 communication

Table 45-22: Response messages on IPv4 communication

Message	Description
bad timing interval	The value specified for interval is out of valid range.
bind: Cannot assign requested address	The specified IP address has not been set on the Switch (when the source option is specified).
Cannot resolve "<host>" (Host name lookup failure)	An attempt to resolve the address of the specified host failed. <host>: Host name
Do you want to ping broadcast? Then -b	A broadcast address can be specified for <host> only when the broadcast option is specified.
Incomplete command.	The entered parameter was invalid. Make sure the specified parameter is correct, and then try again.
max hops cannot be more than 255	Specify a value equal to or smaller than 255 for ttl.
No arp entry.	ARP information does not exist.
no more than 10 probes per hop	Specify a value equal to or smaller than 10 for probe.
No such interface -- <interface name>.	The specified interface has not been set. <interface name>: Name assigned to the specified interface
No such interface.	The specified interface does not exist. Make sure the specified parameter is correct, and then try again.
tcpdump: '<protocol> proto' is bogus	The protocol specified as <protocol> is invalid.
tcpdump: '<string>' modifier applied to <host> host	The <string> qualifier has been added to the host <host> (invalid).
tcpdump: '<string>' modifier applied to host	The <string> qualifier has been added to the host (invalid).

Message	Description
tcpdump: <file name>: Is a directory	<file name> is a directory. (Specify the name of a file.)
tcpdump: <file name>: No such file or directory	<file name> could not be found.
tcpdump: <file name>: Permission denied	Access to <file name> has not been permitted.
tcpdump: <filter> host filtering not implemented	The host filter of <filter> is not supported.
tcpdump: <host> resolved to multiple address	<host> has been resolved as multiple addresses.
tcpdump: archaic file format	The file format is old.
tcpdump: bad dump file format	The file format is invalid.
tcpdump: BIOCSETIF: Device not configured	An invalid interface has been specified. The command execution ends now.
tcpdump: BIOCSETIF: Network is down	An invalid interface has been specified. The command execution ends now.
tcpdump: bogus savefile header	The file header is invalid.
tcpdump: ethernet addresses supported only on ethernet, FDDI or token ring	Layer 2 monitoring is not supported.
tcpdump: expression rejects all packets	The specified filter condition <expression> filters all packets. So, change the condition.
tcpdump: fread: Operation not permitted	The file could not be read (an invalid file might be specified).
tcpdump: fread: Undefined error: 0	The file is abnormal (an unusually short file might be specified).
tcpdump: fwrite: No space left on device	The file could not be written (the disk space might be insufficient).
tcpdump: illegal char: <character>	An invalid <character> has been specified.
tcpdump: illegal Interface name -- <interface name>.	The specified interface has not been set. <interface name>: Name assigned to the specified interface
tcpdump: illegal qualifier of 'port'	An invalid port condition has been specified.
tcpdump: illegal token: <token>	An invalid <token> has been specified.
tcpdump: inbound/outbound not supported on linktype 0	inbound/outbound specification is not supported.
tcpdump: invalid ip6 address <address>	The IPv6 address <address> is invalid.
tcpdump: invalid packet count <count>	The <count> value is invalid.
tcpdump: invalid qualifier against IPv6 address	An invalid qualifier has been specified for the IPv6 address.
tcpdump: invalid snaplen <snaplen>	The <snaplen> value is invalid.
tcpdump: link layer applied in wrong context	Layer 2 monitoring is not supported.

Message	Description
tcpdump: listening on <interface name>	The interface <interface name> is being monitored. <interface name>: Name assigned to the specified interface
tcpdump: mask length must be <= <length>	The mask length should be <length> or less.
tcpdump: Mask syntax for networks only	Masks can be specified only by the net qualifier.
tcpdump: No match.	The specified file does not exist.
tcpdump: no VLAN support for data link type 0	Specifying a VLAN is not supported.
tcpdump: non-network bits set in "<address>"	<address> whose host bit is not 0 has been specified.
tcpdump: only IP multicast filters supported on ethernet/FDDI	To specify multicast, place ip or ip6 in front of it.
tcpdump: parse error	The syntax of the specified filter condition <expression> is invalid.
tcpdump: pcap_loop: link-layer type <type> isn't supported in savefiles	The link layer type <type> of the read file is not supported.
tcpdump: pcap_loop: truncated dump file; tried to read <bytes1> captured bytes, only got <bytes2>.	The read file has been dropped on the way. <byte1> bytes were captured, but there are only <bytes2> bytes.
tcpdump: pcap_loop: truncated dump file; tried to read <bytes1> header bytes, only got <bytes2>.	The read file has been dropped on the way. The header is <byte1>-bytes, but there are only <bytes2> bytes.
tcpdump: port '<port>' is <protocol>	The port specified as <port> is <protocol> protocol.
tcpdump: syntax error	The syntax of the specified filter condition <expression> is invalid.
tcpdump: unknown host '<host>'	An unknown host name <host> was specified. Write the network with the address.
tcpdump: unknown host '<host>' for specified address family	The address of the host <host> could not be resolved by the specified address family.
tcpdump: unknown ip proto '<protocol>'	The protocol name <protocol> of the specified filter condition <expression> could not be specified. Specify the protocol with the protocol number.
tcpdump: unknown network '<network>'	An unknown network name <network> was specified. Write the network with the address.
tcpdump: unknown osi proto '<protocol>'	An unknown osi protocol <protocol> was specified.
tcpdump: unknown port '<port>'	The port name <port> of the specified filter condition <expression> could not be specified. Specify the port with the port number.
tcpdump: unknown protocol: <protocol>	An unknown protocol <protocol> was specified.
tcpdump: WARNING: no IPv4 address assigned	This is displayed if an IPv4 address is not assigned.
tcpdump: WARNING: SIOCGIFADDR: Operation not permitted	An invalid interface has been specified. Exit by pressing the Ctrl + C key.
There is no information.	There is no route information.

Message	Description
ttl <ttl> out of range	The value specified in ttl is out of valid range.

45.1.23 IPv6 communication

Table 45-23: Response messages on IPv6 communication

Message	Description
bind icmp socket: Cannot assign requested address	The specified IPv6 address has not been set on the Switch (when the source option is specified).
max hops cannot be more than 255	Specify a value equal to or smaller than 255 for hoplimit.
ndp: Incomplete Command.	The specified interface has not been configured. Make sure the specified parameter is correct, and then try again.
no more than 10 probes per hop	Specify a value equal to or smaller than 10 for probe.
No ndp entry.	There is no NDP information.
No such interface -- <interface name>.	The specified interface has not been set. <interface name>: Name assigned to the specified interface
There is no information.	There is no route information.
unknown host	The host name is not correct. Specify the correct host name.
unknown iface <interface name>	The specified interface has not been set. <interface name>: Name assigned to the specified interface

45.1.24 DHCP server function

Table 45-24: Response messages on the DHCP server functions

Message	Description
Canceled dhcp restart command.	The command on the DHCP server was canceled by the user.
dhcp_server failed to terminate.	An attempt to restart the DHCP server by using the command failed. Re-execute the command.
dhcp_server has already stopped.	The command failed because the DHCP server program already stopped. The DHCP server program might have been restarted automatically. If necessary, wait until the program is restarted, and then re-execute the command.
dhcp_server restarted after termination: old pid <PID>, new pid <PID>	The command failed because the PID was changed during command execution. The DHCP server program might have been restarted automatically. If necessary, wait until the program is restarted, and then re-execute the command. <PID>: Process ID
dhcp_server signaled but still running, waiting 6 seconds more.	The command is restarting the DHCP server program. Wait a while.
dhcp_server terminated.	The DHCP server was stopped by the command. The program will restart automatically. Wait a while.

Message	Description
For the feature to be stopping, it isn't possible to use this command.	This command cannot be used because the DHCP server function is disabled.
Input Data Error.	The input data is not correct. Enter y or n.
IP Address check error <IP Address>.	The format of the specified IP address is not correct.
No such IP Address.	The specified IP address could not be found.
Now another user used dhcp command, Try again.	Another user is using the "DHCP" command.
pid file <File Name> mangled!	The PID file for the DHCP server program is corrupted. <File Name>: PID file name
pid in file <File Name> unreasonably small (<PID>)	The PID file for the DHCP server program is corrupted. <File_Name>: PID file name <PID>: Process ID in the PID file
program error occurred: <Error Message>	A program error occurred. Re-execute the command. <Error Message>: Location of the error

45.1.25 Filters

Table 45-25: Response messages on filters

Message	Description
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Port number
No configuration.	No access group was set for the Ethernet interface or VLAN interface. Make sure the specified parameter or access-group setting is correct, and then try again.
No such access-list.	The access list number or the access group of the access list name you specified has not been set. Make sure the specified parameter is correct, and then try again.
No such interface.	The specified interface has not been configured. Make sure the specified parameter is correct, and then try again.

45.1.26 QoS

Table 45-26: Response messages on QoS

Message	Description
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Port number
No configuration.	No QoS flow group was set for the Ethernet interface or VLAN interface. Make sure the specified parameter or QoS flow group setting is correct, and then try again.

Message	Description
No such interface.	The specified interface has not been configured. Make sure the specified parameter is correct, and then try again.
No such qos-flow-list-name.	No QoS flow group that is specified with the QoS flow list name <qos flow list name> was applied to the interface. Make sure the specified parameter is correct, and then try again.

45.1.27 IEEE 802.1X

Table 45-27: Response messages on IEEE 802.1X

Message	Description
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the "restart dot1x" command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Receive Error)	An attempt to receive data from the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the "restart dot1x" command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Send Error)	An attempt to send data to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the "restart dot1x" command to restart IEEE 802.1X.
Dot1x doesn't seem to be running.	The IEEE 802.1X program is restarting. Re-execute the command.
Dot1x is not configured.	The IEEE 802.1X setting has not been enabled. Check the configuration.
No operational Channel Group.	There are no available channel groups. Check the authentication mode set by the configuration.
No operational Port.	There are no available ports. Check the authentication mode set by the configuration.
Now another user is using dot1x command, please try again.	Another user is using the "dot1x" command. Wait a while, and then retry the operation.

45.1.28 Web authentication

Table 45-28: Response messages on Web authentication

Message	Description
Already user '<user name>' exists.	The specified user has already been registered.
Can not commit.	An attempt to update the authentication information failed. Execute the "restart web-authentication" command to update the authentication information again.
Can not load.	An attempt to apply Web authentication information failed. Execute the "restart web-authentication" command, and then execute the "load web-authentication" command again to restore the Web authentication user information.
Can't clear because it is default now.	The file could not be deleted because it had default status.
Can't put a sub directory in the directory.	The specified directory contains a subdirectory.

Message	Description
Can't specify "/config" in this command.	The "/config/" directory cannot be specified.
Clear operation failed.	A deletion attempt failed.
Command information was damaged.	Information was discarded because the execution information is corrupted.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the "restart web-authentication" command to restart the Web authentication program.
Delete Error.	An attempt to delete a user failed.
Directory size over.	The capacity of the specified directory exceeds the limit (1024 KB).
File format error.	Registration is not possible because the file is not a backup file.
Install operation failed.	A registration attempt failed.
Load operation failed.	Restoration from the backup file failed.
No login.html file in the directory.	There is no login.html file in the specified directory.
No such directory.	The specified directory does not exist.
No such file.	The specified file does not exist.
No such html-fileset 'xxx'.	The specified fileset does not exist. xxx: Name of the fileset
Now another user is using WA command, please try again.	Another user is using a command for the Web authentication function. Wait a while, and then retry the operation.
Store operation failed.	Creation of the backup file failed.
The number of html-filesets exceeds 4.	The number of filesets to be registered exceeds 4.
The number of users exceeds 300.	The number of users to be registered exceeds 300.
The old-password is different.	The old password for the specified user is incorrect.
The specified user is not login user.	The specified user is not a logged-in user.
Too many files.	The number of files exceeds the limit of 100.
Unknown user '<user name>'.	The specified user has not been registered.

Message	Description
WA is not configured.	The Web authentication function is not enabled. Check the configuration. ("set web-authentication user" command)
	If the Web authentication function has not been configured, check the configuration. If the "web-authentication system-auth-control" configuration command has been set, perform the following operation: • Use the "no web-authentication system-auth-control" configuration command to stop Web authentication. Wait at least 10 seconds, and then use the "web-authentication system-auth-control" configuration command to restart Web authentication. ("restart web-authentication" command)

45.1.29 MAC-based authentication

Table 45-29: Response messages on MAC-based authentication

Message	Description
Already mac address "<mac>","<vlan id>" exists.	The specified MAC address has already been registered.
Can not commit.	An attempt to update the authentication information failed. Execute the "restart mac-authentication" command to update the authentication information again.
Can not load.	An attempt to update the internal MAC-based authentication DB failed. Execute the "restart mac-authentication" command, and then execute the "load mac-authentication" command again to restore the internal MAC-based authentication DB.
Command information was damaged.	Information was discarded because the execution information is corrupted.
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the "restart mac-authentication" command to restart the MAC-based authentication program.
Delete Error.	An attempt to delete the terminal failed.
File format error.	Registration is not possible because the file is not a backup file.
Load operation failed.	Restoration from the backup file failed.
Mac-authentication command is not configured.	The MAC-based authentication function is not configured. Check the configuration.
Mac-authentication is not configured.	The MAC-based authentication function is not configured. Check the configuration.
Now another user is using mac-authentication command, please try again.	Another user is using a command related to the MAC-based authentication function. Wait a while, and then retry the operation.
Store operation failed.	Creation of the backup file failed.
The number of client exceeds 1024.	The number of registered MAC addresses exceeds the capacity limit.

Message	Description
Unknown mac-address '<mac>'.	The specified MAC address has not been registered.

45.1.30 Multistep authentication

Table 45-30: Response messages on multistep authentication

Message	Description
Authentication multi-step is not configured.	The multistep authentication function is not configured. Check the configuration.
Connection failed to 802.1X program.	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the "restart dot1x" command to restart IEEE 802.1X.
There is no authentication multi-step to show.	The specified multistep authentication port has no authentication terminal information.

45.1.31 DHCP snooping

Table 45-31: Response messages on DHCP snooping

Message	Description
ARP Inspection doesn't seem to be running.	The command could not be executed because dynamic ARP inspection is not running.
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not running.
dhcp_snoopingd failed to restart.	An attempt to restart the DHCP snooping program failed. Re-execute the command.
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Port number
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: Location of the error
Restarting dhcp_snoopingd, wait awhile.	The DHCP snooping program is being restarted. Wait a while.

45.1.32 GSRP aware

Table 45-32: Response messages on GSRP aware

Message	Description
Connection failed to GSRP program.	Communication with the GSRP program failed. Re-execute the command. If the failure occurs frequently, use the "restart gsrp" command to restart the GSRP program.
File open error.	An attempt to open or access a dump file failed.
GSRP program failed to be restarted.	An attempt to restart the GSRP program by using this command failed. Re-execute the command.
No received flush request frame.	No GSRP Flush request frames were received.

45.1.33 Uplink redundancy

Table 45-33: Response messages on uplink redundancy

Message	Description
Can't change, Because port is changing in an active port.	For the specified port or channel group, a switchover or switchback of the active port is being performed.
Can't change, Because port is down.	The specified port or channel group has gone down.
Connection failed to Uplink Redundant program.	Communication with the uplink redundancy program failed. Re-execute the command.
File open error.	An attempt to open or access a dump file failed.
No operational Port.	There are no available ports or channel groups. Make sure the specified parameter is correct, and then try again.
Port is already active port.	The specified port or channel group is already operating as the active port.
Uplink Redundant program failed to be restarted.	An attempt to restart the uplink redundancy program by this command failed. Re-execute the command.

45.1.34 L2 loop detection

Table 45-34: Response messages on L2 loop detection

Message	Description
Connection failed to L2 Loop Detection program.	Communication with the L2 loop detection program failed. Re-execute the command.
File open error.	An attempt to open or access a dump file failed.
L2 Loop Detection doesn't seem to be running.	The L2 loop detection program has not been started. Check the configuration.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the function has not been enabled. Check the configuration.
No corresponding port information.	No port and channel group information for L2 loop detection was found.

45.1.35 Storm control

Table 45-35: Response messages on storm control

Message	Description
Storm Control is not configured.	Storm control has not been configured. Check the configuration.

45.1.36 sFlow statistics

Table 45-36: Response messages on sFlow statistics

Message	Description
sflow doesn't seem to be running.	This command failed because the flow statistics program is not started. If this message appears when sFlow statistics are enabled, wait until the sFlow statistics program is restarted, and then re-execute the command.

45.1.37 IEEE 802.3ah/UDLD

Table 45-37: Response messages on IEEE 802.3ah/UDLD

Message	Description
Connection failed to IEEE802.3ah/OAM program.	Communication with the IEEE 802.3ah/OAM program failed. Re-execute the command. If the failure occurs frequently, use the "restart efmoam" command to restart the IEEE 802.3ah/OAM program.
File open error.	An attempt to open or access a dump file failed. Re-execute the command later.
IEEE802.3ah/OAM doesn't seem to be running.	This command failed because the IEEE 802.3ah/OAM program is being restarted. Re-execute the command.
There is no statistics to show.	There are no statistics to be displayed.

45.1.38 CFM

Table 45-38: Response messages on CFM

Message	Description
CFM doesn't seem to be running.	The CFM program is not running. Check the configuration.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.
File open error.	An attempt to open or access a dump file failed.
No such Remote MEP.	The specified remote MEP is unknown. Make sure the specified parameter is correct, and then try again.
Now another user is using CFM command, please try again.	Another user is using the "CFM" command. Wait a while, and then retry the operation.
Specified Domain Level is not configured.	The specified domain level has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MA is not configured.	The specified MA ID number or the primary VLAN for the specified MA has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MEP is not configured.	The specified MEP ID has not been configured. Make sure the specified parameter is correct, and then try again.

45.1.39 LLDP

Table 45-39: Response messages on LLDP

Message	Description
Connection failed to LLDP program.	Communication with the LLDP program failed. Re-execute the command. If the failure occurs frequently, use the "restart lldp" command to restart the LLDP program.
File open error.	An attempt to open or access a dump file failed. Re-execute the command later.
LLDP doesn't seem to be running.	This command failed because the LLDP program is not started. Wait until the LLDP program restarts, and then re-execute the command.
LLDP is not configured.	LLDP has not been configured. Check the configuration.