AX3660S Software Manual

Operation Command Reference Vol.1

For Version 12.1 Rev.11

AX38S-S015X-C0

AlaxalA

■ **Relevant products**

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

■ **Precautions in exporting**

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

■ **Trademarks**

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

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

Ethernet is a registered trademark of Xerox Corporation.

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

IPX is a registered trademark of Novell,Inc.

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

Octpower is a registered trademark of NEC Corporation.

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

Python is a registered trademark of Python Software Foundation.

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

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

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

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

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

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

■ **Reading and storing this manual**

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

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

■ **Note**

Information in this document is subject to change without notice.

■ **Editions history**

December 2023 (Edition 1) AX38S-S015X-C0

■ **Copyright**

Preface

■ Applicable products and software versions

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

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

Unless otherwise noted, this manual describes the functions common to both the SL-L3A and SL-L3L software licenses. Functions that are not common are indicated as follows.

[SL-L3A]:

The description applies to the SL-L3A software license.

■ Corrections to the manual

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

■ Intended readers

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

Readers must have an understanding of the following:

- The basics of network system management

■ Manual URL

You can view this manual on our website at:

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

■ Reading sequence of the manuals

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

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

```
Quick Start Guide

        (AX36S-Q002X)
```

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

```
Hardware Instruction Manual

        (AX36S-H002X)
```

```
Transceiver
Hardware Instruction Manual
        (AX-COM-H001X)
```

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

```
Configuration Guide
Vol.1
        (AX38S-S010X)
    Vol.2
        (AX38S-S011X)
      Vol.3
        (AX38S-S012X)
```

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

```
Configuration
Command Reference
Vol.1    (AX38S-S013X)
    Vol.2
        (AX38S-S014X)
```

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

```
Operation Command
Reference
Vol.1
        (AX38S-S015X)
    Vol.2
        (AX38S-S016X)
```

● **To check messages and logs**

```
Message Log Reference

        (AX38S-S017X)
```

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

```
Troubleshooting Guide

        (AX36S-T002X)
```

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

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

● AX3660S series switch

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

■ Abbreviations used in the manual

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line

AES	Advanced Encryption Standard
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second (can also appear as bps)
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DNSSL	Domain Name System Search List
DR	Designated Router
DSA	Digital Signature Algorithm
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DSS	Digital Signature Standard
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
ECDHE	Elliptic Curve Diffie-Hellman key exchange, Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GCM	Galois/Counter Mode
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol

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

QSFP+	Quad Small Form factor Pluggable Plus
QSFP28	28Gbps Quad Small Form factor Pluggable
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
RDNSS	Recursive Domain Name System Server
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSA	Rivest, Shamir, Adleman
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SFP+	enhanced Small Form-factor Pluggable
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
Sync-E	Synchronous Ethernet
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLS	Transport Layer Security
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VLAN	Virtual LAN
VNI	VXLAN Network Identifier
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
VTEP	VXLAN Tunnel End Point
VXLAN	Virtual eXtensible Local Area Network
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web

■ Conventions: KB, MB, GB, and TB

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

Contents

PART 3: Network Interfaces

PART 4: Layer 2 Switching

Contents

PART 6: Layer 2 Authentication

31.　IEEE 802.1X　647

32.　Web Authentication　685

33.　MAC-based Authentication　749

PART 7: Security

PART 8: High Reliability Based on Redundant Configurations

37. Uplink Redundancy   893

PART 9: Network Monitoring Function

38. L2 Loop Detection   911

PART 10: Network Management

39. sFlow Statistics   927

40. IEEE 802.3ah/UDLD   937

41. CFM   951

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".

Operation when a stack configuration is used

Describes the behavior when a stack configuration is used. This section does not apply to the software license or optional license of your use that does not includes the stack function.

This section describes the format for entering an operation command if the "remote command" command can be used to execute the command. For details on the input mode and general notes on the "remote command" command, see the description for the "remote command" command.

Example

Provides examples of appropriate command usage.

Display items

Describes the display items generated by the example.

The following table describes the Switch display item displayed as the command execution result in Example for each command when a stack configuration is used.

Table 1-1: Display of the switch number and switch status

Item	Meaning	Displayed detailed information

Switch	Switch number. The switch status is displayed in parentheses.	Switch number
		Switch status
		    Init: Now configuring a stack
		    Master: In the stack configuration (Master)
		    Backup: In the stack configuration (Backup)
		    -------: No stack configured

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

Table 1-2: 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 1-3: List of interface names assigned for input formats

Input format	Interface name <interface name>
interface gigabitethernet	geth1/0/1 The numeric values represent <switch no.>/<nif no.>/<port no.>.
interface tengigabitethernet	tengeth1/0/24 The numeric values represent <switch no.>/<nif no.>/<port no.>.
interface fortygigabitethernet	ftygeth1/0/52 The numeric values represent <switch no.>/<nif no.>/<port no.>.
interface hundredgigabitethernet	hndgeth1/0/52 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
interface loopback <loopback id> [SL-L3A]	loopback1 The numerical value represents <loopback id>.
interface null 0	null0
interface mgmt 0	MGMT0

Impact on communication

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

Response messages

Lists 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 1-3: List of interface names assigned for input formats.

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 1-4: 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%VLAN 0001

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

The table below lists the range of <switch no.>, <nif no.>, and <port no.> parameter values. Specify any command that does not support the stack configuration, in the format without <switch no.>.

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

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

■ How to specify <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 range of permitted values is the same as the range of <switch no.>, <nif no.>, and <port no.> values in the above table.

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

For a command applicable to a stack configuration:

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

For a command not applicable to a stack configuration:

0/1-3,5

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

For a command applicable to a stack configuration:

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

For a command not applicable to a stack configuration:

/: Specifies all ports on the device.

■ Range of <channel group number>

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

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

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

■ 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 <vni list> [SL-L3A]

The <vni list> parameter can accept multiple VNIs, separated by hyphens (-) and commas (,). You can also specify one VNI. The range of permitted values is all the VNIs set by the configuration command. Note that the maximum number of VNIs that can be specified at a time is 8191.

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

   1-3,5000,1010020-1010049

■ Range of <loopback id> [SL-L3A]

The range of values the <loopback id> parameter accepts is from 1 to 256.

■ 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 specified for <interface number>
Ethernet interface	gigabitethernet	<switch no.>/<nif no.>/<port no.>
	tengigabitethernet	<switch no.>/<nif no.>/<port no.>
	fortygigabitethernet	<switch no.>/<nif no.>/<port no.>
	hundredgigabitethernet	<switch no.>/<nif no.>/<port no.>
Port channel interface	port-channel	<channel group number>
VLAN interface	vlan	<vlan id>
Loopback interface	loopback	0
		<loopback id> [SL-L3A]
Null interface	null	0
Management port	mgmt	0

List of character codes

Character codes are listed in the following table.

Table 1-8: 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 1-9: 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

Operation when a stack configuration is used

The command can be executed only on the master switch.

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

Response messages

Table 2-1: List of response messages for the enable command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
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.

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

Operation when a stack configuration is used

The command can be used in the same way as for a standalone configuration.

Example

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

```
#  disable
>
```

Display items

None

Impact on communication

None

Response messages

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.)
3. If you are accessing the switch through the "session" command, the session is over, and you are back to the connecting member switch.

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

Operation when a stack configuration is used

The command can be used in the same way as for a standalone configuration.

Example

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

```
# quit
>
```

Display items

None

Impact on communication

None

Response messages

None

Notes

None

exit

Ends user mode or administrator mode and logs out from the device. Note that if you are accessing the switch through the "session" command, the session is over, and you are back to the connecting member switch.

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

Operation when a stack configuration is used

The command can be used in the same way as for a standalone configuration.

Example

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

```
# exit
```

Display items

None

Impact on communication

None

Response messages

None

Notes

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

logout

Logs out from the device. Note that if you are accessing the switch through the "session" command, the session is over, and you are back to the connecting member switch.

Syntax

```
logout
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

The command can be used in the same way as for a standalone configuration.

Example

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

```
# logout
login:
```

Display items

None

Impact on communication

None

Response messages

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.

Operation when a stack configuration is used

The command enables editing of the configuration only on the master switch.

Example

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

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

Display items

None

Impact on communication

None

Response messages

For details about error messages displayed during configuration editing, see "Configuration Command Reference Vol. 1, 45.1.2 Configuration editing and operation information".

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" and "erase configuration" commands 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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

Example

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

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

Display items

None

Impact on communication

None

Response messages

Table 3-1: List of response messages for the set exec-timeout command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

- If an account added by the "adduser" command with the no-flash parameter specified configures the settings using this command, they revert to the default (60 minutes) when the device is restarted.

- If any of exec-timeout, terminal-pager, or terminal-help is set using the "username" configuration command, the exec-timeout setting value (specified value, or default value when the parameter is omitted) in the configuration applies to the corresponding user.

- A user with the settings of the "username" configuration command applied can also temporarily change the behavior of the configuration command only in the target session by executing this command after login.

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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

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

Response messages

Table 3-2: List of response messages for the set terminal help command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

- If an account added by the "adduser" command with the no-flash parameter specified configures the settings using this command, they revert to the default (all) when the device is restarted.

- If any of exec-timeout, terminal-pager, or terminal-help is set using the "username" configuration command, the terminal-help setting value (specified value, or default value when the parameter is omitted) in the configuration applies to the corresponding user.

- A user with the settings of the "username" configuration command applied can also temporarily change the behavior of the configuration command only in the target session by executing this command after login.

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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

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

Response messages

Table 3-3: List of response messages for the set terminal pager command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

- If an account added by the "adduser" command with the no-flash parameter specified configures the settings using this command, they revert to the default (enable) when the device is restarted.

- If any of exec-timeout, terminal-pager, or terminal-help is set using the "username" configuration command, the terminal-pager setting value (specified value, or default value when the parameter is omitted) in the configuration applies to the corresponding user.

- A user with the settings of the "username" configuration command applied can also temporarily change the behavior of the configuration command only in the target session by executing this command after login.

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

Operation when a stack configuration is used

The command can be used in the same way as for a standalone configuration.

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

Response messages

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>]
telnet <host> [{/ipv4 | /ipv6}][/source-interface <source address>]
                    [/vrf <vrf id>][<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.
>
>   When /vrf \<vrf id\> is specified, the destination host name cannot be specified to \<host\>. [SL-L3A]

{/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.

/vrf \<vrf id\> [SL-L3A]

>   Establishes a connection with the specified VRF. For \<vrf id\>, specify a VRF ID that was set in the configuration.
>
>   Behavior when this parameter is omitted:
>
>>   Displays the information for the global network.

\<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\> in global networks.

Operation when a stack configuration is used

The command can be executed only on the master switch.

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. Accesses 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

Response messages

Table 3-4: List of response messages for the telnet command

Message	Description
<host>: hostname nor servname provided, or not known	The address specified for the host and the connection method specified by option are invalid or inconsistent. <host>: Remote host
<host>: No address associated with hostname	The connection to the host could not be established because the address could not be resolved. <host>: Remote host
bind: Can't assign requested address	An invalid source IP address has been set.
bind: Invalid argument	An invalid source IP address has been set.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot specify hostname with VRF	VRF and a host name cannot be specified at the same time.
connect to address <host>: Connection refused	The host rejected the connection. <host>: Remote host

Message	Description
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
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.
Trying <host>...	Trying to connect to <host>. <host>: Remote host
Unable to connect to remote host	The connection to the host could not be established.
Unable to connect to remote host: Connection refused	The host rejected the connection.
Unable to connect to remote host: Operation timed out	The connection timed out.

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>]]
    [/vrf <vrf id>]
```

Input mode

User mode and administrator mode

Parameters

<host>

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

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.

/vrf <vrf id> [SL-L3A]

Establishes a connection with the specified VRF. For <vrf id>, specify a VRF ID that was set by using the configuration command.

Behavior when this parameter is omitted:

A connection is established to the global network.

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.

Operation when a stack configuration is used

The command can be executed only on the master switch.

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

Response messages

Table 3-5: List of response messages for the ftp command

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>: hostname nor servname provided, or not known	The address specified for the host and the connection method specified by option are invalid or inconsistent. <host>: Remote host
<host>: Unknown host	An unknown host name was entered. <host>: Remote host IP address
?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.

Message	Description
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: Can't assign requested address	An invalid source IP address has been set.
bind: Invalid argument	An invalid source IP address has been set.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot specify hostname with VRF	VRF and a host name cannot be specified at the same time.
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
Login failed.	A login attempt has failed.
No address associated with hostname	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.
Not connected.	No remote communication.
quit for Ctrl+Z pushed.	The "ftp" 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.
Trying <host>...	Trying to connect to <host>. <host>: Remote host

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>] [/vrf <vrf id>] [<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.

/vrf <vrf id> [SL-L3A]

Establishes a connection with the specified VRF. For <vrf id>, specify a VRF ID that was set by using the configuration command.

If you specify a host name for <host>, you cannot specify this parameter.

Behavior when this parameter is omitted:

A connection is established to the global network.

<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.

Operation when a stack configuration is used

The command can be executed only on the master switch.

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.

? [<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

Response messages

Table 3-6: List of response messages for the tftp command

Message	Description
?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
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot specify hostname with VRF	VRF and a host name cannot be specified at the same time.
Error code <number>: <message>	Other TFTP error messages are displayed: <number>: Error code <message>: Error description
Error code 1: File not found	The specified file could not be found.
Error code 2: Access violation	The specified file could not be accessed.
Error code 3: Disk full or allocation exceeded	The disk is full or allocation exceeds the limit.
Error code 6: File already exists	The file already exists.
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
No target machine specified, Use connect command.	The connection destination has not been set. Use the "connect" command to set it.
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

Message	Description
quit for Ctrl+Z pushed.	The "tftp" command was ended by pressing the Ctrl + Z keys.
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: Can't 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.

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

Operation when a stack configuration is used

Automatically synchronizes the configuration of the master switch with that of other member switches.

Example and display items

None

Impact on communication

None

Response messages

For details about error messages displayed during configuration editing, see "Configuration Command Reference Vol. 1, 45.1.2 Configuration editing and operation information".

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

Operation when a stack configuration is used

Automatically synchronizes the configuration of the master switch with that of other member switches.

Example and display items

None

Impact on communication

None

Response messages

For details about error messages displayed during configuration editing, see "Configuration Command Reference Vol. 1, 45.1.2 Configuration editing and operation information".

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): [2001:240:400::101]

> \<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.

>As was the case for \<source file> (above), \<file name>, running-config, 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.

When the stack is configured, 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.

Operation when a stack configuration is used

The command can be executed only on the master switch.

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@[2001:240:400::101]/backup.cnf
  Configuration file copy to ftp://staff@[2001:240:400::101]/backup.cnf?
  (y/n): y

  Authentication for 2001:240:400::101.
  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

If you do a copy that changes the running configuration, the operating port restarts.

Response messages

Table 4-1: List of response messages for the copy command

Message	Description
Can't execute this command in back-up switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't set stack enable in running-config because stack is not active.	The "stack enable" configuration command cannot be set in the running configuration because the stack function is not active.
Can't specify running-config for <target file> because stack is active.	When the stack function is active, the running configuration cannot be specified in the <target file> parameter. To change the operation mode, execute this command with the startup configuration file specified in the <target file> parameter, and then restart all the switches.

Message	Description
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.

For details about error messages displayed during configuration editing, see "Configuration Command Reference Vol. 1, 45.1.2 Configuration editing and operation information".

Notes

1. You cannot copy to a running configuration that is being edited. Execute the "copy" command after the edit is completed.

2. When the running configuration is updated, the edited contents of the configuration are also updated.

3. Editing the startup configuration has no effect on the running configuration or communication.

4. 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.

5. If you copy a configuration to the running configuration, the specified configuration becomes the running configuration. Note that if you were logged in via the network, the operating port is restarted.

6. 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, use the "erase configuration" command to reset the configuration, and then edit it again.

7. 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.

8. 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.

9. 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.

10. 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.

erase configuration

Resets startup configuration and running configuration to the defaults.

Syntax

```
erase configuration
```

Input mode

Administrator mode

Parameters

None

Operation when a stack configuration is used

This command is not supported

Example

```
#erase configuration
Do you wish to erase both running-config and startup-config? (y/n):
#
```

Display items

None

Impact on communication

When this command is executed, all operating ports stop all operations.

Response messages

Table 4-2: List of response messages for the erase configuration command

Message	Description
Can't execute this command because stack is active.	The command cannot be executed when the stack function is active.
Do you wish to erase both running-config and start-up-config? (y/n):	This message asks you to confirm whether you want to reset the current startup configuration file and running configuration file to the defaults. Entering "y" resets those files to the default. Entering "n" aborts the "erase" command.

For details about error messages displayed during configuration editing, see "Configuration Command Reference Vol. 1, 45.1.2 Configuration editing and operation information".

Notes

1. This command cannot be used while the configuration is being edited. Use this command to reset the configuration file to the default, after the configuration edit is completed.

2. When this command is executed, the operating ports stop all operations. You need to be careful if you

logged in via a network because the session is terminated by executing this command.

3. This command cannot be executed if the "stack enable" configuration command is set.

4. If a configuration that requires a device restart is deleted, the device must be restarted for the deletion to take effect. In addition, if the "system interface hundredgigabitethernet enable" configuration command is set, the interface will be reconfigured by restarting the device after the command is executed.

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): [2001:240:400::101]
>
>   <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.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example

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

```
> show file ftp://staff@[2001:240:400::101]/backup.cnf
Date 20XX/01/20 12:00:00 UTC
Authentication for 2001:240:400::101.
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@[2001:240:400::101]//usr/home/staff/
Date 20XX/01/20 12:00:00 UTC
Authentication for 2001:240:400::101.
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

Response messages

Table 4-3: List of response messages for the show file command

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 execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
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.

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.

Operation when a stack configuration is used

The command can be used in the same way as for a standalone configuration.

Example and display items

None

Impact on communication

None

Response messages

None

Notes

If this command is executed with another member switch specified by the "remote command" command, the execution result becomes invalid.

pwd

Shows the path to the current directory.

Syntax

```
pwd
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

The command can be used in the same way as for a standalone configuration.

Example and display items

None

Impact on communication

None

Response messages

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} ls [<option>] [<names>]
remote command {<switch no.> | all} ls mc-dir
```

Example

Shows the list of files on a memory card.

```
>ls mc-dir
```

Display items

None

Impact on communication

None

Response messages

Table 4-4: List of response messages for the ls command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
MC is busy.	Another process is accessing the memory card. Wait a while, and then re-execute the command.
MC not found.	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 insert the memory card.

Notes

1. The mc-dir parameter cannot be used when a memory card is not inserted.

2. When the mc-dir parameter is specified, the ACC LED is on while the command is being executed. Do not remove or insert the memory card while the ACC LED is on.

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 [ ].

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch. You can also execute the command with the switch number of the member switch specified.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} dir /all [summary]
remote command {<switch no.> | all} dir /deleted
```

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 4-5: 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 4-6: 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

Response messages

Table 4-7: List of response messages for the dir command

Message	Description
dir: Current directory is not flash.	The current directory is not the internal flash memory. Move to an appropriate directory.

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} cat [<option>] <file name>
```

Example and display items

None

Impact on communication

None

Response messages

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.)
cp <file name1> switch <switch no.> <switch file name2>
   (Copies the file in internal flash memory to the member switch having the specified switch
   number)
cp switch <switch no.> <switch file name1> <file name2>
   (Copies the file in the member switch having the specified switch number 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.

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.

switch <switch no.>

Specifies the switch number of the member switch that contains the copy-source file. Alternatively, specifies the switch number of the copy-destination member switch.

<switch file name2>

Specifies the name of a file on the copy-destination member switch by using an absolute path.

<switch file name1>

Specifies the name of a file on the copy-source member switch by using an absolute path. Wildcards cannot be used to specify file names in other member switches.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} cp [<option>] <file name1> <file name2>
remote command {<switch no.> | all} cp <file name1> mc-file <mc file name2>
  (Copies the file in internal flash memory of the member switch to the memory card of the member
  switch)
remote command {<switch no.> | all} cp mc-file <mc file name1> <file name2>
  (Copies the file in the memory card of the member switch to the internal flash memory of the
  member switch)
```

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
  ```

- Copies /var/tmp/file1 from the current member switch to the /var/tmp directory of the member switch having the switch number 2, and name the file as file2.

  ```
  >cp /var/tmp/file1 switch 2 /var/tmp/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.

Response messages

Table 4-8: List of response messages for the cp command

Message	Description
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 execute.	The command could not be executed. Re-execute the command.
copy error	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.
MC is busy.	Another process is accessing the memory card. Wait a while, and then re-execute the command.

Message	Description
MC is write protected.	Make sure the memory card's protect switch is not set to "▼ Lock". If the switch is set to "▼ Lock", slide the switch, and then insert the memory card again. Make sure there is no dust in the memory card slot. If there is dust, wipe it off with a dry cloth and insert the memory card.
MC not found.	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 insert the memory card.
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

Notes

1. The mc-file parameter cannot be used when a memory card is not inserted.

2. When the mc-file parameter is specified, the ACC LED is on while the command is being executed. Do not remove or insert the memory card while the ACC LED is on.

3. Accessing a memory card increases load on the device. Before specifying mc-file, if monitoring time and sending interval of the Layer 2 or Layer 3 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.

4. The switch <switch no.> parameter can be specified only on the master switch when the stack is configured.

5. If this command is executed by the "remote command" command, the current directory of the other member switch becomes the home directory of the user who executes this command.

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} mkdir [<option>] <directory>
remote command {<switch no.> | all} mkdir mc-dir <directory>
```

Example

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

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

Display items

None

Impact on communication

None

Response messages

Table 4-9: List of response messages for the mkdir command

Message	Description
Can't create directory.	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.
Can't execute.	The command could not be executed. 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 write protected.	Make sure the memory card's protect switch is not set to "▼Lock". If the switch is set to "▼Lock", slide the switch, and then insert the memory card again. Make sure there is no dust in the memory card slot. If there is dust, wipe it off with a dry cloth and insert the memory card.
MC not found.	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 insert the memory card.

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. When the mc-dir parameter is specified, the ACC LED is on while the command is being executed. Do not remove or insert the memory card while the ACC LED is on.

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} mv [<option>] <file name1> <file name2>
remote command {<switch no.> | all} mv [<option>] <directory1> <directory2>
remote command {<switch no.> | all} mv [<option>] <names> <dir>
```

Example and display items

None

Impact on communication

None

Response messages

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

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} rm [<option>] <file name>
remote command {<switch no.> | all} rm mc-file <mc file name>
```

Example

Deletes a file called file1 on the memory card.

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

Display items

None

Impact on communication

None

Response messages

Table 4-10: List of response messages for the rm command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
MC is busy.	Another process is accessing the memory card. Wait a while, and then re-execute the command.
MC is write protected.	Make sure the memory card's protect switch is not set to "▼Lock". If the switch is set to "▼Lock", slide the switch, and then insert the memory card again. Make sure there is no dust in the memory card slot. If there is dust, wipe it off with a dry cloth and insert the memory card.
MC not found.	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 insert the memory card.

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. When the mc-file parameter is specified, the ACC LED is on while the command is being executed. Do not remove or insert the memory card while the ACC LED is on.

3. 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".

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} rmdir <directory>
remote command {<switch no.> | all} rmdir mc-dir <directory>
```

Example

Deletes a directory, deldir, on the memory card.

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

Display items

None

Impact on communication

None

Response messages

Table 4-11: List of response messages for the rmdir command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
MC is busy.	Another process is accessing the memory card. Wait a while, and then re-execute the command.

Message	Description
MC is write protected.	Make sure the memory card's protect switch is not set to "▼Lock". If the switch is set to "▼Lock", slide the switch, and then insert the memory card again. Make sure there is no dust in the memory card slot. If there is dust, wipe it off with a dry cloth and insert the memory card.
MC not found.	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 insert the memory card.

Notes

1. The mc-dir parameter cannot be used when a memory card is not inserted.

2. When the mc-dir parameter is specified, the ACC LED is on while the command is being executed. Do not remove or insert the memory card while the ACC LED is on.

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} delete <file name>
```

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

Response messages

Table 4-12: List of response messages for the delete command

Message	Description
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.
delete: No such file or directory.	The specified file does not exist. Or the current directory is not valid.

Message	Description
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.

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} undelete <index>
```

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

Response messages

Table 4-13: List of response messages for the undelete command

Message	Description
undelete: Current directory is not flash.	The current directory is not the internal flash memory. Move to an appropriate directory.

Message	Description
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>).

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

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} squeeze
```

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

Response messages

Table 4-14: List of response messages for the squeeze command

Message	Description
Canceled	The "squeeze" command has been canceled.
Deleted files will be erased. OK ? (y/n):	Erases deleted files. Enter "y" to erase, otherwise "n" to abort.
Done	The erasure has been completed.
squeeze: Current directory is not flash.	The current directory is not internal flash memory.

Message	Description
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.

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.

zmodem

Transfers files between the Switch and console connected by RS232C.

Syntax

```
zmodem get
zmodem put <file name>
```

Input mode

User mode and administrator mode

Parameters

get

Transfers files from the console to the Switch.

put <file name>

Transfers the file (<file name>) from the Switch to the console.

Operation when a stack configuration is used

The command can be used in the same way as for a standalone configuration.

Example

The following are examples of executing the command when Tera Term Pro (Version 2.3) is used as communication software.

- In the example below, the file /config/system.cnf is transferred from the Switch to the console.

  After you execute the following command, the file transfer starts when you choose File, Transfer, ZMODEM, and then Receive in Tera Term Pro (Version 2.3) on the console.

  ```
  zmodem put /config/system.cnf
  ```

- In the following example, the file backup.cnf is transferred from the console to the Switch:

  ```
  zmodem get
  ```

  After you enter the command, in Tera Term Pro (Version 2.3) on the console, choose File, Transfer, ZMODEM, and then Send. After that, in the ZMODEM Send dialog page, enter backup.cnf for "File Name". When you click the "Open" button, the file transfer starts.

Display items

None

Impact on communication

None

Response messages

Table 4-15: List of response messages for the zmodem command

Message	Description
<file name>: No such file.	The file to be transferred (<file name>) was not found. <file name>: File name
Execute only console machine.	This command can be executed only from the console. This command cannot be executed on a remote operation terminal.
Receive skipped : <file name> (already exists)	Reception was interrupted because a file with the same name as the file being received already exists. <file name>: File name
Receive skipped : <file name> (permission denied)	Reception was skipped because the user who executed the command did not have the write permission for the file or directory. <file name>: File name
ttyname error.	The terminal type cannot be recognized.

Notes

1. This command can be executed only from the console. This command cannot be executed on a remote operation terminal.

2. If a file transfer is interrupted for reasons such as a cable failure during execution of this command and the interruption continues for a long period of time, the file transfer fails as follows:

   - When zmodem get is executed, the command prompt is displayed if the interruption lasts for one minute.

   - When zmodem put is executed, the command prompt is displayed if the interruption lasts for one minute.

3. Control codes displayed during file transfers do not affect the behavior of the system. It can be ignored. The displayed characters do not have any special meanings.

4. The "zmodem" command can be used to transfer a file under the following communication conditions:

   - Character length: 8 bits

   - Communication speed: 9600 bit/s, 4800 bit/s, or 2400 bit/s

   - Stop bit length: 1 bit or 2 bits

   - Parity bit: None

5 Stack

remote command

When a stack configuration is used, this command is used to execute an operation command from the master switch to the specified member switch. In the specified member switch, the operation command is executed in administrator mode.

Syntax

```
remote command {<switch no.> | all} <command>
```

Input mode

Administrator mode

Parameters

{<switch no.> | all}

<switch no.>

Executes the operation command for the member switch whose switch number is specified. For the specifiable range of values, see "Specifiable values for parameters".

all

Executes the operation command for all member switches that configure the stack. The command is executed for the master switch first, and then for other switches in ascending order of switch number.

<command>

Specifies an operation command to be executed. However, the "remote command" command and the "session" command cannot be specified.

To execute an operation command that uses the pipe and redirection function for the member switch specified in the <switch no.> parameter, enclose the <command> parameter in single quotation marks (').

For details about the operation commands that can be specified, see the manual for each operation command.

Operation when a stack configuration is used

The command can be executed only on the master switch.

Example

Figure 5-1: Executing the show clock command for the member switch with switch number 2

```
# remote command 2 show clock
Switch 2 (Backup)
-----------------
Wed Jun 22 15:30:00 UTC 20XX
#
```

Figure 5-2: Executing the show clock command on all the member switches

```
# remote command all show clock
Switch 1 (Master)
-----------------
Wed Jun 22 15:30:00 UTC 20XX

Switch 2 (Backup)
-----------------
Wed Jun 22 15:30:00 UTC 20XX
#
```

Figure 5-3: Executing the show clock command for the member switch with switch number 2 and outputting the result to the home directory of that switch as a file with the file name nowtime.txt

```
# remote command 2 'show clock > ./nowtime.txt'
Switch 2 (Backup)
-----------------
#
```

Figure 5-4: Executing the show clock command for the member switch with switch number 2 and outputting the result to the current directory of the master switch on which this command is executed as a file with the file name nowtime.txt

```
# remote command 2 show clock > ./nowtime.txt
#
```

Display items

Table 5-1: Items displayed by the remote command command

Item	Meaning	Displayed detailed information
Switch	Switch number. The switch status is displayed in parentheses.	Switch number Switch status Init: Now configuring a stack Master: In the stack configuration (Master) Backup: In the stack configuration (Backup)

Impact on communication

None

Response messages

Table 5-2: List of response messages for the remote command command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
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. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

1. This command can be executed only on the master switch.

2. When using this command to execute an operation command, command authorization is disabled on switches other than the master switch. To ensure security, we recommend that you use command authorization to limit the users who can execute this command.

3. When this command is used to execute an operation command, command accounting is disabled on switches other than the master switch.

4. When this command is used to execute an operation command, paging is disabled on switches other than the master switch.

5. When the pipe function is used to pass the result of an operation command executed by using this command to another command, such as the "more" command or the "less" command, keys might be temporarily unavailable. In this case, press the same key again.

6. When the pipe function is used to pass the result of an operation command executed by using this command to another command, such as the "more" command or the "less" command, a response message might be displayed in the execution result. In this case, check the execution result without using the pipe function.

7. When this command is used to execute an operation command, the operation command is executed in a different session than the operation terminal that executes the command.

8. When operation commands including this command are executed in succession, wait until this command finishes and the prompt appears, and then execute the next operation command.

show switch

Displays information about member switches that configure a stack.

Syntax

```
show switch [detail]
```

Input mode

User mode and administrator mode

Parameters

detail

> Displays detailed information about member switches.

> Behavior when this parameter is omitted:

>> Summary information about member switches is displayed.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} show switch [detail]
```

Example 1

The following examples show how to display summary information about member switches.

Figure 5-5: Displaying summary information about member switches (stack configuration)

```
> show switch
Date 20XX/12/24 11:38:56 UTC
Stack status : Enable        Switch No : 1
System MAC Address : 0012.e220.5101
No  Switch status           Model        Machine ID      Priority  Ver
 1  Master                  3660-24t4xw  0012.e220.5101  31        1
 2  Backup (Initializing)   3660-24t4xw  0012.e220.5102  11        1
```

Figure 5-6: Displaying summary information about member switches (standalone configuration)

```
> show switch
Date 20XX/10/26 11:38:56 UTC
Stack status : Disable       Switch No : 1
```

Display items in Example 1

Table 5-3: Display items for the summary information about member switches

Item	Meaning	Displayed detailed information
Stack status	Stack behavior status	Enable: The switch is running in a stack configuration Disable: The switch is running in a standalone configuration
Switch No	Switch number of the device	1 to 2 The switch number set by the "set switch" command is displayed.

Item	Meaning	Displayed detailed information
System MAC Address	Device MAC address	Device MAC address of the stack If the master has not been determined, "-" is displayed.
No	Switch number	1 to 2

Switch status	Switch status	Master: Master
		Backup: Backup
		Init: Initial status
		The processing details are displayed during the change processing after a switch status transition.
		  (Initializing): Initializing
		  (Switchover): Switching

Model	Member switch model	3660-24t4x: AX3660S-24T4X 3660-24t4xw: AX3660S-24T4XW 3660-48t4xw: AX3660S-48T4XW 3660-16s4xw: AX3660S-16S4XW 3660-24s8xw: AX3660S-24S8XW 3660-48xt4qw: AX3660S-48XT4QW 3660-24x4qw: AX3660S-24X4QW 3660-48x4qw: AX3660S-48X4QW
Machine ID	Chassis MAC address	——
Priority	Master selection priority of member switches	1 to 31
Ver	Stack function version	1

Example 2

The following examples show how to display detailed information about member switches.

Figure 5-7: Displaying detailed information about member switches

```
> show switch detail
Date 20XX/12/24 11:38:56 UTC
Stack status : Enable        Switch No : 1
System MAC Address : 0012.e220.5101
No  Switch status         Model        Machine ID      Priority  Ver
 1  Master                3660-24t4xw  0012.e220.5101  31        1
 2  Backup  (Initializing) 3660-24t4xw 0012.e220.5102  11        1
Port     Status           Neighbor(Port   Model        Machine ID)
1/0/29   Up(Forwarding)           2/0/29  3660-24t4xw  0012.e220.5102
1/0/30   Up(Forwarding)           2/0/30  3660-24t4xw  0012.e220.5102
2/0/29   Up(Forwarding)           1/0/29  3660-24t4xw  0012.e220.5101
2/0/30   Up(Forwarding)           1/0/30  3660-24t4xw  0012.e220.5101
```

Display items in Example 2

Table 5-4: Display items for detailed information about member switches

Item	Meaning	Displayed detailed information
Stack status	Stack behavior status	Enable: The switch is running in a stack configuration Disable: The switch is running in a standalone configuration

Item		Meaning	Displayed detailed information
Switch No		Switch number of the device	1 to 2 The switch number set by the "set switch" command is displayed.
System MAC Address		Device MAC address	Device MAC address of the stack If the master has not been determined, "-" is displayed.
No		Switch number	1 to 2
Switch status		Switch status	Master: Master Backup: Backup Init: Initial status The processing details are displayed during the change processing after a switch status transition. 　(Initializing): Initializing 　(Switchover): Switching
Model		Member switch model	3660-24t4x: AX3660S-24T4X 3660-24t4xw: AX3660S-24T4XW 3660-48t4xw: AX3660S-48T4XW 3660-16s4xw: AX3660S-16S4XW 3660-24s8xw: AX3660S-24S8XW 3660-48xt4qw: AX3660S-48XT4QW 3660-24x4qw: AX3660S-24X4QW 3660-48x4qw: AX3660S-48X4QW
Machine ID		Chassis MAC address	—
Priority		Master selection priority of member switches	1 to 31
Ver		Stack function version	1
Port		Stack port number	Switch number/NIF number/port number
Status		Link status of the stack port. The frame transfer status is displayed in parentheses.	Up (Forwarding): Indicates that the port status is Up and frame transfer is available. Down: Indicates that the port status is Down, or the port status is Up and frame transfer is unavailable (the neighboring device is not a member switch).
Neighbor	Port	Stack port number of the neighboring member switch	Switch number/NIF number/port number -: Unknown
	Model	Model of the neighboring member switch	3660-24t4x: AX3660S-24T4X 3660-24t4xw: AX3660S-24T4XW 3660-48t4xw: AX3660S-48T4XW 3660-16s4xw: AX3660S-16S4XW 3660-24s8xw: AX3660S-24S8XW 3660-48xt4qw: AX3660S-48XT4QW 3660-24x4qw: AX3660S-24X4QW 3660-48x4qw: AX3660S-48X4QW -: Unknown
	Machine ID	Chassis MAC address of the neighboring member switch	-: Unknown

Impact on communication

None

Response messages

Table 5-5: List of response messages for the show switch command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

Notes

None

set switch

Changes the switch number of a switch that makes up the stack.

To enable the change, restart the device.

Syntax

```
set switch <switch no.>
```

Input mode

User mode and administrator mode

Parameters

<switch no.>

> Changes the switch number to the specified number. For the specifiable range of values, see "Specifiable values for parameters".

Operation when a stack configuration is used

The command can be used in the same way as for a standalone configuration.

Example

Figure 5-8: Changing the switch number

```
> set switch 2
The switch number was changed to 2.
When device restart, the change in the switch number is reflected.
>
```

Display items

None

Impact on communication

None

Response messages

Table 5-6: List of response messages for the set switch command

Message	Description
Can't change to new switch number because new switch number exist.	The switch number could not be changed because the specified switch number already existed. Make sure the specified parameter is correct.
Can't execute.	The command could not be executed. Re-execute the command.
The switch number was changed to <switch no.>. When device restart, the change in the switch number is reflected.	The switch number was changed. The change in the switch number is applied after the device is restarted. <switch no.>: Switch number

Notes

1. The new switch number takes effect after the device is restarted.

2. If you restart the device without setting the "stack enable" configuration command, the switch number is changed to "1". Note that the switch number before the change is displayed in the operation message logged during restart of the device that causes the switch number change.

dump stack

Outputs to a file detailed event trace information and control table information collected by the stack management program.

Syntax

```
dump stack
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} dump stack
```

Example

Figure 5-9: Taking a dump of the stack management program

```
> dump stack
>
```

Display items

None

Impact on communication

None

Response messages

Table 5-7: List of response messages for the dump stack command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

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

Storage directory: /usr/var/stack/

File name: stack_dump.gz

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

session

Used to connect with a specified member switch in a stack configuration.

Syntax

```
session switch <switch no.>
```

Input mode

User mode and administrator mode

Parameters

switch <switch no.>

Used to connect with the member switch with the specified switch number. However, you cannot specify the switch number of the device on which you executed the command. For the specifiable range of values, see "Specifiable values for parameters".

Operation when a stack configuration is used

Commands can be executed on a member switch that makes up the stack.

Example

Figure 5-10: Connecting with the master switch from the backup switch

```
02B> session switch 1           <-1

> enable                        <-2
# exit                          <-3
Connection closed by foreign host.
02B>
```

1. On the backup switch, connect with the master switch.

2. Switch to administrator mode on the master switch.

3. End the "session" command.

Display items

None

Impact on communication

None

Response messages

Table 5-8: List of response messages for the session command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
Can't specify switch number of own.	The switch number of the device on which you executed the command cannot be specified.
Connection closed by foreign host.	The connection is closed. If this message is displayed and no further connection can be established, the number of concurrent connections by the "session" command may have been exceeded. Check the number of session connections on the member switch you are trying to establish a connection with.
Connection closed.	The connection is closed.
Connection disconnected.	The connection was lost. The member switch you had a connection with or the member switch on which you executed the command may have been removed from the stack configuration. Check the status of the stack configuration.
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number

Notes

1. The user name at the connection destination and the contents of the command list for command authorization are the same as the information at the time when this command is executed.

2. If the connected member switch or the member switch on which you executed the command is removed from the stack configuration while a connection is established, the connection is automatically disconnected after 15 seconds at maximum, and you are returned to the console on the member switch on which you executed the command.

3. A single member switch can accept concurrent connections from up to four processes.

4. If there is no key entry for a set duration, the connection will be closed due to auto-logout (see "Configuration Guide Vol. 1, 4.3(3) Auto-logout").

5. When, for example, character strings are being displayed on the screen with a connection established with a member 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 "session" command and then make a connection again.

6 Management Port

inactivate mgmt 0

Changes the status of the management port from the active status to inactive.

Syntax

```
inactivate mgmt 0
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command <switch no.> inactivate mgmt 0
```

Example

Turn the management port into the inactive status.

```
> inactivate mgmt 0
>
```

Display items

None

Impact on communication

Communication using the management port becomes unavailable.

Response messages

Table 6-1: List of response messages for the inactivate mgmt 0 command

Message	Description
Can't accept command (system is busy).	The command cannot be accepted (because the system is busy). Re-execute the command later.
Can't execute.	The command could not be executed. Re-execute the command.
Management port is disabled.	The management port is in inactive status.
No such interface -- management port.	The management port cannot be not found.
Not operational interface management port.	The management port is not in runnable state.

Notes

1. Executing this command does not change the configuration.

2. If the device is restarted after the management port is inactivated by using this command, the inactive status of the management port is canceled.

3. Use the "activate mgmt 0" command to restore the active status of the management port that was inactivated by this command.

activate mgmt 0

Returns the status of the management port to the active status from inactive when the port is inactivated by the "inactivate mgmt 0" command.

Syntax

```
activate mgmt 0
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command <switch no.> activate mgmt 0
```

Example

Turn the management port back into the active status.

```
> activate mgmt 0
>
```

Display items

None

Impact on communication

Communication using the management port resumes.

Response messages

Table 6-2: List of response messages for the activate mgmt 0 command

Message	Description
Can't accept command (system is busy).	The command cannot be accepted (because the system is busy). Re-execute the command later.
Can't execute.	The command could not be executed. Re-execute the command.
Management port is already active.	The management port is already in active status.
Management port is disabled.	The management port is in inactive status.
No such interface -- management port.	The management port cannot be not found.
Not operational interface management port.	The management port is not in runnable state.

Notes

1. Executing this command does not change the configuration.

7 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, toor, daemon, bin, games, postfix, named, ntpd, sshd, smmsp, uucp, nobody, 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.

Operation when a stack configuration is used

Automatically synchronizes the account of the master switch with that of other member switches.

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 the password configuration is interrupted (press the Ctrl + D keys or 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

Response messages

Table 7-1: List of response messages for the adduser command

Message	Description
\<user name\> is not a valid login name	This user name cannot be used.
already a '\<user name\>' user	The specified user has already been registered. \<user name\>: User name
Can't add user \<user name\>: can't lock \<file name\> : \<reason\>	The addition of a user was canceled because the password file was locked. Re-execute the command. \<user name\>: User name \<file name\>: Password file name \<reason\>: Detailed information
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't synchronize accounts to backup switch or transit switch.	Synchronization of the account to the backup switch or the transit switch failed. Re-execute the command.
Mismatch; try again.	The new password and the re-entered password are not the same. Re-enter the password.
no changes made	The registration of the specified user was canceled. Re-execute the command.
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.
Password unchanged. /etc/master.passwd: unchanged	The password change was canceled.
Permission denied	The password change is not allowed.
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.
synchronize accounts to backup switch or transit switch.	Synchronization of the account to the backup switch or the transit switch will start.

Notes

1. To abort password configuration, press the Ctrl + D keys. If the Ctrl + D keys are pressed while retyping, Mismatch; try again. appears, and then the input prompt reappears. If password configuration is aborted, a new login user with no password is created.

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.

6. When a stack is configured, synchronization of the account might take a long time.

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.

Operation when a stack configuration is used

Automatically synchronizes the account of the master switch with that of other member switches.

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

Response messages

Table 7-2: List of response messages for the rmuser command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
can't lock <file name> : <reason>	The deletion of a user was canceled because the password file was locked. Re-execute the command. <file name>: Password file name <reason>: Detailed information
Can't synchronize accounts to backup switch or transit switch.	Synchronization of the account to the backup switch or the transit switch failed. Re-execute the command.

Message	Description
Last user.	The last user cannot be deleted.
no changes made	The deletion of the specified user was canceled. Re-execute the 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 specified user could not be deleted.
Remove myself?	The account of the user executing this command cannot be deleted.
synchronize accounts to backup switch or transit switch.	Synchronization of the account to the backup switch or the transit switch will start.

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.

5. When a stack is configured, synchronization of the account might take a long time.

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.

Operation when a stack configuration is used

Automatically synchronizes the account of the master switch with that of other member switches.

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

Response messages

Table 7-3: List of response messages for the password command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't synchronize accounts to backup switch or transit switch.	Synchronization of the account to the backup switch or the transit switch failed. Re-execute the command.
Mismatch; try again.	The new password and the re-entered password are not the same. Re-enter both passwords.
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.
Password unchanged./etc/master.passwd: unchanged	The password change was canceled.
Permission denied.	The password change is not allowed.
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.
synchronize accounts to backup switch or transit switch.	Synchronization of the account to the backup switch or the transit switch will start.
unknown user <user name>	The specified user has not been registered. <user name>: User name

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. To abort password configuration, press the Ctrl + D keys. If the Ctrl + D keys are pressed while retyping, the input prompt (Mismatch; try again.) is displayed. If this happens, press the Ctrl + D keys again.

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. When a stack is configured, synchronization of the account might take a long time.

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.

Operation when a stack configuration is used

Automatically synchronizes the account of the master switch with that of other member switches.

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

Response messages

Table 7-4: List of response messages for the clear password command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't synchronize accounts to backup switch or transit switch.	Synchronization of the account to the backup switch or the transit switch failed. Re-execute the command.
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 of the specified user could not be changed.
synchronize accounts to backup switch or transit switch.	Synchronization of the account to the backup switch or the transit switch will start.
unknown user <user name>	The specified user has not been registered. <user name>: User name

Notes

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

2. When a stack is configured, synchronization of the account might take a long time.

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

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show sessions
remote command {<switch no.> | all} who
```

Example

Figure 7-1: Displaying users currently logged in to the Switch

```
> show sessions
Date 20XX/06/16 12:00:00 UTC
kikuchi console  -----  0   Jun 15 14:16                      <-1
shimizu ttyp0    admin  2   Jun 15 14:16 (192.168.0.1)        <-2
shimizu ttyp1    -----  3   Jun 15 14:17 (192.168.0.1)        <-3
tanaka  ttyp2    -----  4   Jun 15 15:52 (192.168.0.1 VRF:2)  <-4
tanaka  ttyp3    -----  5   Jun 15 16:53 (session)            <-5
>
```

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 (VRF 2) [SL-L3A]

5. Connected through the "session" command

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) or

session (displayed only when the user has established the connection through the "session" command)

- VRF ID (displayed only when the user has logged in from VRF) [SL-L3A]

Impact on communication

None

Response messages

Table 7-5: List of response messages for the show sessions (who) command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

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

Operation when a stack configuration is used

The command can be used in the same way as for a standalone configuration.

Example

Figure 7-2: Displaying the login name of the current login user

```
> show whoami
Date 20XX/01/07 12:00:00 UTC
shimizu ttyp0    -----  2   Jan  6 14:17 (192.168.0.1)
>
```

Figure 7-3: Displaying the login name of the current login user when the user logged in from VRF2 [SL-L3A]

```
> show whoami
Date 20XX/06/16 12:00:00 UTC
tanaka   ttyp2    -----  4   Jun 15 15:52 (192.168.0.1 VRF:2)
>
```

Figure 7-4: Displaying the current user name when the user established the connection with the session command

```
> show whoami
Date 20XX/06/16 12:00:00 UTC
tanaka   ttyp3    -----  5   Jun 15 16:53 (session)
>
```

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 ttyp0    -----  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"
  ```

129

```
        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 ttyp0    -----  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 ttyp0    -----  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 7-6: 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) or "session" (displayed only when the user has established the connection through the "session" command) • VRF ID (displayed only when the user has logged in from VRF) [SL-L3A]
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+.

Item		Displayed information
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.
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

Response messages

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 [switch <switch no.>] <login no.>
```

Input mode

User mode and administrator mode

Parameters

switch <switch no.>

Executes the command on the member switch whose switch number is specified.

This parameter can be specified only on the master switch when the stack is configured. For the specifiable range of values, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

The command is executed on the local device.

<login no.>

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

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} killuser <login no.>
```

Example 1

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 7-5: Executing the command with the user's login number specified

```
> show sessions
Date 20XX/01/07 12:00:00 UTC
kikuchi console  -----  0#   Jan  6 14:16
shimizu ttyp0    admin  2#   Jan  6 14:16 (192.168.0.1) <--(Note 1)
shimizu ttyp1    -----  3#   Jan  6 14:17 (192.168.0.1)
kikuchi ttyp2    -----  4#   Jan  6 14:20 (localhost)
>
> killuser 2
```

\#: Login number
Note 1: To force this user to log out, specify login number 2.

Example 2

This example shows, when a stack is configured, how to forcibly log out a user who is currently logged in to another member switch.

Execute the "show sessions" command on the master switch to check the login number of the user you want to get logged out. Execute the command with the switch number of the member switch and the login number specified.

Figure 7-6: Executing the command with the switch number of the member switch and the login number specified (in the stack configuration)

```
> show sessions
Switch 1 (Master)
----------------
Date 20XX/01/07 12:00:00 UTC
kikuchi ttyp1    admin  1#   Jan  7 11:30

Switch 2 (Backup)
----------------
Date 20XX/01/07 12:00:00 UTC
kikuchi console  -----  0#   Jan  6 14:16 <--(Note 2)
>
> killuser switch 2 0
```

\#: Login number
Note 2: To force this user to log out, specify login number 0.

Display items

None

Impact on communication

None

Response messages

Table 7-7: List of response messages for the killuser command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
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.
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.
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number

Message	Description
no user(UserName)	The user does not exist.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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, shimizu with login number 3 can forcibly log out "shimizu" with login number 2, but not kikuchi with login number 4. However, when this command is executed from the console, users with different accounts can be forcibly logged out.

   Also, if the switch number of the backup switch is specified for the switch parameter, or if the "remote command" command is used to execute this command on the backup switch, 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

Operation when a stack configuration is used

The command can display information only for the master switch.

Example

Figure 7-7: 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 7-8: 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.	

Item	Meaning	Displayed detailed 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.
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.

Item	Meaning	Displayed detailed information
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

Response messages

Table 7-9: List of response messages for the show accounting command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
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.

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

Operation when a stack configuration is used

The command can clear information only from the master switch.

Example

Figure 7-8: Clearing accounting information

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

Display items

None

Impact on communication

None

Response messages

Table 7-10: List of response messages for the clear accounting command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to accounting program.	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.

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.

Operation when a stack configuration is used

The command can be executed only on the master switch.

Example

Figure 7-9: 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

Response messages

Table 7-11: List of response messages for the restart accounting command

Message	Description
accounting program failed to be restarted.	An attempt to restart the accounting program by this command failed. Re-execute the command.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to accounting program.	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.

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

Operation when a stack configuration is used

The command can be executed only on the master switch.

Example

Figure 7-10: Example of taking an accounting dump

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

Display items

None

Impact on communication

None

Response messages

Table 7-12: List of response messages for the dump protocols accounting command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to accounting program.	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.
File open error.	An attempt to open or access a dump file failed.

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.

8

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] [-vrf <vrf id>] [<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 when a secure command is executed on the Switch.

Behavior when this parameter is omitted:

A virtual terminal is not forcibly allocated to .

-vrf \<vrf id\> [SL-L3A]

Establishes a connection with the specified VRF. For \<vrf id\>, specify a VRF ID that was set by using the configuration command.

Behavior when this parameter is omitted:

A connection is established to the global network.

\<user\>@

Specifies the user name for authentication. Specifiable characters are alphanumeric characters and special characters. For details, see "Table 1-8: 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.

You cannot specify the host name if the -vrf \<vrf id\> parameter is specified. [SL-L3A]

>   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.

Operation when a stack configuration is used

The command can be executed only on the master switch.

Example

Figure 8-1: Remotely logging in to host hostA.example.jp using an SSH client

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

Figure 8-2: Remotely logging to VRF 2 host 192.168.0.1 using an SSH client [SL-L3A]

```
> ssh -vrf 2 192.168.0.1
operator@192.168.0.1's password:******
```

Figure 8-3: 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 8-4: 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

Response messages

Table 8-1: List of response messages for the ssh command

Message	Description
'@@@@@@@@@@@@@@@@@@@@@ @@@@@@@@@@@@@@@@@@@@@ @@@@@@@@@@@@@@@@@@@@@ @ WARNING: REMOTE HOST IDENTIFI-CATION HAS CHANGED! @ @@@@@@@@@@@@@@@@@@@@@ @@@@@@@@@@@@@@@@@@@@@ @@@@@@@@@@@@@@@@@@@@@ IT IS POSSIBLE THAT SOMEONE IS DO-ING 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:<num-ber> 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 fin-gerprint>. 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
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot specify hostname with VRF	VRF and a host name cannot be specified at the same time.
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

Message	Description
Connection to <host> closed.	The connection was lost. <host>: Server name or its address
Host key verification failed.	An attempt to verify the host key failed.
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.
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
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

Message	Description
WARNING: <key type> key found for host <host> in [/usr]/home/<user>/.ssh/known_hosts: <number> <key type> key fingerprint <finger-print>.	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

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>] [-vrf <vrf id>] [<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.

-vrf <vrf id> [SL-L3A]

> Establishes a connection with the specified VRF. For <vrf id>, specify a VRF ID that was set by using the configuration command.
>
> Behavior when this parameter is omitted:
>
> > A connection is established to the global network.

<user>@

> Specifies the user name for authentication. Specifiable characters are alphanumeric characters and special characters. For details, see "Table 1-8: 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.
>
> You cannot specify the host name if the -vrf <vrf id> parameter is specified. [SL-L3A]

Behavior when all parameters are omitted:

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

Operation when a stack configuration is used

The command can be executed only on the master switch.

Example

Figure 8-5: 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

Response messages

In addition to the same messages related to SSH connections as those for the "ssh" command, the messages listed in the following table are output.

Table 8-2: List of response messages for the sftp command

Message	Description
Cannot download non-regular file: <path>	The specified <path> file is invalid. It cannot be downloaded. <path>: Specified file name
Connected to <host> [on VRF <vrf id>].	A connection has been established. <host>: Host name or address <vrf id>: VRF ID (which is not displayed when a connection to the global network is made)
Connection closed	The line was disconnected.
Couldn't stat remote file: <reason>	The specified remote file does not exist. <reason>: Error details
Invalid command.	The specified command is invalid.
subsystem request failed on channel <id>	Could not connect with the specified server over sftp. <id>: Internal information value
You must specify a path after a <command> command.	The path must be specified after <command>.

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>] [-vrf <vrf id>] [<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.

-vrf <vrf id> [SL-L3A]

> Establishes a connection with the specified VRF. For <vrf id>, specify a VRF ID that was set by using the configuration command.

Behavior when this parameter is omitted:

> A connection is established to the global network.

<user>@

> Specifies the user name for authentication. Specifiable characters are alphanumeric characters and special characters. For details, see "Table 1-8: 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 [1234::1]:aaa.txt

You cannot specify the host name if the -vrf <vrf id> parameter is specified. [SL-L3A]

<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.

Operation when a stack configuration is used

The command can be executed only on the master switch.

Example

Figure 8-6: 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

Response messages

In addition to the same messages related to SSH connections as those for the "ssh" command, the messages listed in the following table are output.

Table 8-3: List of response messages for the scp command

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
lost connection	The connection was closed.

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

Operation when a stack configuration is used

The command can be used in the same way as for a standalone configuration.

Example

Figure 8-7: Displaying the SSHv1/SSHv2 host public key and fingerprint

```
> show ssh hostkey
Date 20XX/01/20 12:00:00 UTC
******* SSHv1 Hostkey *******
1024 65537 14320839755744008246845582928031274177723538140036830074896289790281147097161719068130329961764685888351434661056975452466508609208470597192976847466387347351427370908874719325645964193723193907055708167608860751013667295765744933251420901184326738697523138805658247435623233890731225462450600011096509047484 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

Response messages

Table 8-4: List of response messages for the show ssh hostkey command

Message	Description
Can't execute (<reason>).	The command cannot be executed due to the invalid host key. Alternatively, a command execution error occurred. <reason>: Internal detailed information [Action] 1. Re-create the host key with the "set ssh hostkey" command. 2. Re-execute the command.

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.

In a stack configuration, the host key pair is automatically synchronized from the master switch to other member switches when the host key pair is created and the member switches are started.

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 a DSA host key pair for SSHv2 are created.

Operation when a stack configuration is used

The command can be executed only on the master switch. The host key pair created on the master switch is automatically synchronized with other member switches.

Example

Figure 8-8: Changing an SSHv1/SSHv2 host key pair

```
# set ssh hostkey

WARNING!!
Would you wish to generate SSHv1 RSA and SSHv2 DSA 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 dsa key pair.
The key fingerprint is:
SHA256:O+GPxz5QtjOD8wCEK2HhhHDkjocEY3IEIeF+ltuwJU4
MD5:e8:f8:71:1b:31:ba:c0:21:ee:ce:88:0f:78:e4:d7:09

The hostkey generation is completed.
```

```
#
```

Figure 8-9: 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

Response messages

Table 8-5: List of response messages for the set ssh hostkey command

Message	Description
Can't execute (<reason>).	The command could not be executed. <reason>: Internal detailed information [Action] Re-execute the command.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
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. [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.

Notes

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

Operation when a stack configuration is used

The command can be executed only on the master switch. The host key pair deleted on the master switch is automatically removed from other member switches.

Example

Figure 8-10: 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

Response messages

Table 8-6: List of response messages for the erase ssh hostkey command

Message	Description
Can't execute (<reason>).	The command could not be executed.

Message	Description
	<reason>: Internal detailed information [Action] Re-execute the command.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
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 deletion of the host key was interrupted. [Action] Re-execute the command.
The hostkey was erased successfully.	The host key was deleted.

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 [switch <switch no.>]
```

Input mode

User mode and administrator mode

Parameters

switch <switch no.>

> Executes the command on the member switch whose switch number is specified in a stack configuration. This parameter can be specified only on the master switch when the stack is configured. For the specifiable range of values, see "Specifiable values for parameters".

> Behavior when this parameter is omitted:

>> The command is executed on the local device.

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show ssh logging
```

Example

Figure 8-11: 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 8-7: Trace log messages and their descriptions

Message	Description
<authentication method> authentication disabled.	<authentication method> cannot be used. <authentication method>: User authentication method
<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> [on VRF <vrf id>]	The connection with <host> was closed. <host>: Remote host <vrf id>: VRF ID
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

Message	Description
Connection from <host> port <port> on <local host> port <local port> [VRF <vrf id>]	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 <vrf id>: VRF ID
Connection reset by <host> port <port>	A connection with <host> was disconnected. <host>: Remote host <port>: Port of the remote host
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

Message	Description
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
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.

Message	Description
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.	A RSA server key is being generated.
input_userauth_request: invalid user \<user\>	An invalid user name was specified. \<user\>: User name
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

Message	Description
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.	A 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
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

Message	Description
User uucp not allowed because shell /usr/libex-ec/uucp/uucico does not exist	The specified user (uucp) cannot log in.
Warning: keysize mismatch for cli-ent_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 chal-lenge.	A wrong response was made to an RSA authentication request.

Impact on communication

None

Response messages

Table 8-8: List of response messages for the show ssh logging command

Message	Description
Can't execute (\<reason\>).	The command could not be executed. \<reason\>: Internal detailed information [Action] Re-execute the command.
No such Switch \<switch no.\>.	The specified switch number does not exist. Make sure the speci-fied parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. \<switch no.\>: Switch number

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 [switch <switch no.>]
```

Input mode

Administrator mode

Parameters

switch <switch no.>

Executes the command on the member switch whose switch number is specified in a stack configuration. This parameter can be specified only on the master switch when the stack is configured. For the specifiable range of values, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

The command is executed on the local device.

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} clear ssh logging
```

Example

Figure 8-12: 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

Response messages

Table 8-9: List of response messages for the clear ssh logging command

Message	Description
Can't execute (<reason>).	The command could not be executed. <reason>: Internal detailed information

Message	Description
	[Action] Re-execute the command.
Canceled. SSH server's log was NOT cleared.	The clearing of logs was canceled. (The logs were not cleared.)
Clear Complete.	The logs were cleared successfully.
Interrupted. Please, Re-try.	Canceled because a signal (such as [Ctrl] + [C]) was received. [Action] 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. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number

Notes

None

9

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} show clock
```

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

Response messages

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 69 to 99 (for the 1900s) and from 00 to 38 (for the 2000s). (For example, 00 indicates the year of 2000.)

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).

Operation when a stack configuration is used

Automatically synchronizes the time of the master switch with that of other member switches.

Example

To set the date and time as June 22, 2005 at 15:30, enter the following command:

```
> set clock 0506221530
Wed Jun 22 15:30:00 UTC 2005
>
```

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".

Response messages

Table 9-1: List of response messages for the set clock command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
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.
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.

Notes

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

   - In a standalone configuration, the time is changed.

   - In a stack configuration, the time is changed in the master switch. For member switches other than the master switch, if the time difference between before and after the change is five seconds or more, the CPU usage information collected for each second is cleared to zero.

2. The specifiable values are from 1969/01/01 00:00:00 to 2038/01/19 03:14:07.

show ntp associations

Shows the behavior status of the connected NTP server.

Syntax

```
show ntp associations [{vrf <vrf id> | global}]
```

Input mode

User mode and administrator mode

Parameters

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

> Displays the behavior status of the NTP server for the specified VRF. Only the behavior status of the NTP server for the specified VRF is displayed when <vrf id> is specified, and only the behavior status of the NTP server on the global network is displayed when global is specified. The range of the specifiable values for <vrf id> is all the VRF IDs specified by the configuration command.

> Behavior when this parameter is omitted:
>> The behavior status of the NTP server for all VRFs, including the global network, is displayed.

Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

Example 1

Figure 9-1: Displaying the behavior 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
>
```

Example 2

Figure 9-2: Displaying the behavior status of NTP servers for all VRF [SL-L3A]

```
> show ntp associations
Date 20XX/12/10 11:01:35 UTC
VRF: global
  remote          refid        st t when poll reach   delay   offset   disp
================================================================================
*10.10.10.10    10.10.10.20    4 u  968 1024  177     1.16    0.085   76.46
VRF: 10
  remote          refid        st t when poll reach   delay   offset   disp
================================================================================
+10.10.10.10    10.10.10.20    4 u  981 1024  377     1.21   -4.727   14.82
>
```

Figure 9-3: Displaying the behavior status of the NTP server for the specified VRF [SL-L3A]

```
> show ntp associations vrf 10
Date 20XX/12/10 11:01:35 UTC
VRF: 10
  remote          refid        st t when poll reach   delay   offset   disp
================================================================================
+10.10.10.10    10.10.10.20    4 u  981 1024  377     1.21   -4.727   14.82
>
```

Display items

Table 9-2: Information displayed by the show ntp associations command

Item	Meaning
VRF [SL-L3A]	VRF ID
remote	Indicates the name of the time server host. If a local time server is specified, "LO-CAL(1)" is displayed. [Meaning of the code at the beginning of the host name] " ": A host that is treated as invalid because the activity cannot be checked, or the stratum value is high. "+": A host remaining as an available choice. "#": A selected, synchronized host. However, the upper limit of the distance is exceeded. "*": A selected, synchronized host. Other symbols: Hosts that are found to be invalid by test results.
refid	The destination host to which the time server is synchronized.
st	The stratum value of the host
t	Indicates a server type. [Meaning of displayed server types] "u": Unicast server "b": Broadcast server "l": Local server
when	When the Switch is connected to the host, this item indicates the time elapsed since the last packet was received from the host. If the Switch is disconnected from the host, this item indicates the time elapsed since the host 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 host 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

Response messages

Table 9-3: List of response messages for the show ntp associations command

Message	Description
Connection refused	A connection with the NTP server could not be established.
No association ID's returned	The time server could not be found.
no such VRF <vrf id>	The specified VRF was not found. <vrf id>: Specified VRF ID
ntp is not running	NTP is not running.

Notes

None

restart ntp

Restarts the local NTP server.

Syntax

```
restart ntp
```

Input mode

Administrator mode

Parameters

None

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} restart ntp
```

Example

Figure 9-4: Restarting the NTP server

```
# restart ntp
#
```

Display items

None

Impact on communication

None

Response messages

Table 9-4: List of response messages for the restart ntp command

Message	Description
Connection refused	A connection with the NTP server could not be established.
No association ID's returned	The time server could not be found.

Notes

None

10 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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} diff [<option>] <file name1> <file name2>
remote command {<switch no.> | all} diff [<option>] <directory1> <directory2>
```

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

Response messages

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>.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} grep[<option>] <pattern> [<file name>]
```

Example and display items

None

Impact on communication

None

Response messages

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.

Operation when a stack configuration is used

The command can be used in the same way as for a standalone configuration.

Example and display items

None

Impact on communication

None

Response messages

None

Notes

If this command is executed with another member switch specified by the "remote command" command, paging is not performed.

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.

Operation when a stack configuration is used

The command can be used in the same way as for a standalone configuration.

Example and display items

None

Impact on communication

None

Response messages

None

Notes

If this command is executed with another member switch specified by the "remote command" command, paging is not performed.

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} tail [<option>] <file name>
```

Example and display items

None

Impact on communication

None

Response messages

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} hexdump [<option>] <file name>
```

Example and display items

None

Impact on communication

None

Response messages

None

Notes

None

11 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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show version [software]
```

Example

Figure 11-1: Displaying the software version only

```
> show version software
Date 20XX/04/01 02:54:45 UTC
S/W: OS-L3M Ver. 12.0
>
```

Figure 11-2: Displaying information about the Switch software and the boards installed

```
> show version
Date 20XX/04/01 02:56:29 UTC
Model: AX3660S-24T4XW
S/W: OS-L3M Ver. 12.1.B
H/W: Main board
     AX-3660-24T4XW [TB03GL24TSX0S4089H6K001:0:730F01:0:612:11B567]
       Model No.: AX-3660-24T4XWSXL
     Power slot 1 PS-M(AC)
       AX-F2430-PSA06 [L101SJ000103P]
     Power slot 2 PS-M(AC)
       AX-F2430-PSA06 [L101SJ000203P]
     Fan slot     FAN-M
       AX-F2430-FAN05 [TA0FAN030000C140306W011]
>
```

Display items

Table 11-1: Information displayed by the show version command

Item	Displayed information	Displayed detailed information
Model	Device model	—
S/W[#1]	Software information	Software type, version
H/W		

Item	Displayed informa-tion	Displayed detailed information
Main board	Information about the main board	AX-xxxx-xxxxxx: Abbreviation of the model name [ssss….ssss]: Serial information Model No.: Model name
Power slot[#2]	Power supply unit type	PS-M(AC): AC power supply unit PS-M(DC): DC power supply unit notconnect: Not installed
	Power supply unit infor-mation	AX-xxxxx-xxxxx: Model name of the power supply unit[#1] [ssss….ssss]: Serial information
Fan slot[#2]	Fan unit type	FAN-M: Fan unit notconnect: Not installed notsupport: Not supported
FAN-M[#2]	Fan unit information	AX-xxxxx-xxxxx: Model name of the fan unit[#1] [ssss….ssss]: Serial information

#1

  If a power supply unit or a fan unit that is not supported by software is installed, "--------" is displayed.

#2

  It is displayed only in replaceable power supply models.

Impact on communication

None

Response messages

Table 11-2: List of response messages for the show version command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using ac-count operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

None

show system

Shows the operating status.

Syntax

```
show system
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show system
```

Example 1

Figure 11-3: Displaying the result of executing the show system command (on a fixed power supply model)

```
> show system
Date 20XX/01/16 17:53:12 UTC
System: AX3660S-24T4X, OS-L3M (SL-L3A-001) Ver. 12.1.E
Node : Name=
    Contact=
    Locate=
    Elapsed time : 00:45:03
    LED Brightness mode : normal
    Machine ID : 0012.e23e.b20f
    Power redundancy-mode : check is not executed
    Fan: active No = Fan(1) , Fan(2) , Fan(3) , Fan (4)
        Speed = normal, Direction = F-to-R
    PS1: active
    PS2: unused
            :
            :
            :
```

Figure 11-4: Displaying the result of executing the show system command (on a replaceable power supply model)

```
> show system
Date 20XX/01/16 17:53:12 UTC
System: AX3660S-48XT4QW, OS-L3M (SL-L3A-001) Ver. 12.0
Node : Name=
    Contact=
    Locate=
    Elapsed time : 00:45:03
    LED Brightness mode : normal
    Machine ID : 0012.e23e.b20f
    Power redundancy-mode : check is not executed
    Power slot 1 : active PS-M(AC)
        Fan  : active No = Fan1(1)  Speed = --------, Direction = F-to-R
        PS   : active
        Lamp : Power LED=green , ALM1 LED=light off
```

```
Power slot 2 : notconnect
Fan slot : active FAN-M
    Fan  : active No = Fan3(1) , Fan3(2) , Fan3(3) , Fan3(4)
           Speed = normal , Direction = F-to-R
    Lamp : ALM LED=light off
Main board : active
    Boot : 20XX/01/16 17:08:19 , operation reboot
    Fatal restart : CPU 0 times ,  SW 0 times
    Lamp : Power LED=green , Status LED1=green
    Board : CPU=AMD GX-420 2000MHz , Memory=4,194,304KB(4096MB)
    Management port: active up
        100BASE-TX full(auto) 0012.e23e.b20f
    Temperature : normal(26degree)
    Flash :
            user area    config area     dump area    area total
        used  238,599KB          99KB           0KB    238,698KB
        free  229,857KB      116,963KB     131,008KB    477,828KB
        total 468,456KB      117,062KB     131,008KB    716,526KB
    MC  : enabled
        Manufacture ID : 00000030
        24,077KB used
        971,008KB free
        995,085KB total
    System interface hundredgigabitethernet :
        disable (10G)  : 0/21-22,37-44
        enable  (100G) : 0/49,51-52
                          :
                          :
                          :
```

Display items in Example 1

Table 11-3: Information displayed by the show system command

Item	Displayed information	Displayed detailed information
System	Device model	—
	Software information	Software type, software license, and 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
LED Brightness mode	LED brightness status	normal: Normal brightness economy: Power-saving brightness off: LED off auto(xxx): Automatic brightness adjustment xxx: normal/economy/off
Machine ID	Chassis MAC address	—

Power redundancy-mode	Power mode	In a fixed power supply model
		    check is executed: The state of no input power supply and a power failure are notified as a major failure.
		    check is not executed: The state of no input power supply and a power failure are not notified as a major failure.

Item	Displayed information	Displayed detailed information

		In a replaceable power supply model
		  check is executed: Whether the power is in a redundant configuration is checked.
		  check is not executed: Whether the power is in a redundant configuration is not checked.

Power slot[#1]	Power supply unit slots	—
	Power supply unit slot status	active: Supplied normally fault: Failure occurred notconnect: Not installed
	Power supply unit type[#2]	PS-M(AC): AC power supply unit PS-M(DC): DC power supply unit
Fan[#1]	Fan behavior status[#3]	Fan number of an active fan
Speed[#1]	The rotational speed of the fan	Displays "--------".
Direction[#1]	Direction of the fan	F-to-R: Front air intake and rear air exhaust R-to-F: Rear air intake and front air exhaust
	Fan direction mismatch information[#4]	(mismatch): The direction does not match the direction of the fan unit.
PS[#1, #2]	Status of the input power supply unit	active: Supplied normally fault: No power is being supplied or there is an abnormal voltage.
Fan slot[#1]	Fan slot	—
	Status of a fan slot	active: Supplied normally fault: Failure occurred notconnect: Not installed notsupport: Not supported
	Fan slot type	FAN-M: Fan slot
Fan	Fan behavior status[#3]	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 R-to-F: Rear air intake and front air exhaust
PS1[#5]	Status of input power supply unit 1	active: Supplied normally fault: No supply/voltage fault (when the "power redundancy-mode redundancy-check" configuration command is set) unused: No supply/voltage fault (when the "power redundancy-mode redundancy-check" configuration command is not set)
PS2[#5]	Status of input power supply unit 2	active: Supplied normally

Item	Displayed information	Displayed detailed information
		fault: No supply/voltage fault (when the "power redundancy-mode redundancy-check" configuration command is set) unused: No supply/voltage fault (when the "power redundancy-mode redundancy-check" configuration command is not set)

Lamp[#2]

Item	Displayed information	Displayed detailed information
ALM LED	LED indicating the fan status	light off: The LED is off. red: The LED is on and red.
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	power on: Startup because the power switch was turned on operation reboot: Restart due to the reboot command, or due to a switching processor failure or a status change of a member switch in the stack configuration fatal: Restart (a failure occurs) default restart: Restart due to a default restart hardware reset: Restart due to the reset button
Fatal restart	Number of times a restart is performed due to a failure	CPU: 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. red blink: The LED is red and blinking. red: The LED is on and red.
Board	CPU information	The type and clock of the CPU
	Amount of memory installed on the main board	Amount of memory installed on the main board
Management port	Status of the management port	active up: Active (up and running normally) active down: Active (A line failure occurred.) unused: Not used inactive: Inactive status disable: Not active through the configuration

Item	Displayed information	Displayed detailed information
	Line speed	10BASE-T full: 10BASE-T full duplex 100BASE-TX full: 100BASE-TX full duplex (auto): Line speed determined through auto-ne-gotiation --------: Not determined It is not displayed if the management port status is unused.
	MAC address	MAC address of the management port It is not displayed if the management port status is unused.
	Description	What is contained in the Description configura-tion set for the applicable management port It is not displayed if the Description configura-tion is not set or if the management port status is unused.
Temperature	Intake-air temperature informa-tion	normal: Normal caution: Caution (High or low temperature) Note: For specific temperature conditions, see the Display items of the "show environment" command.
Flash	Used capacity[#6, #7]	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
	Unused capacity[#6, #7]	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 configura-tion 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[#6, #7]	Total of capacity being used and capacity not be-ing 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 be-ing used by the file system in the internal flash memory

Item	Displayed information	Displayed detailed information
MC	Memory card status	enabled: The memory card can be accessed. notconnect: The memory card is not inserted. write protect: Writing to the memory card is not allowed. --------: Another process is accessing the memory card.[8]
	Type[6, 7]	Manufacture ID: Memory card manufacturer number
	Used capacity[6, 7]	Capacity in use in the memory card file system
	Unused capacity[6, 7]	Capacity not in use in the memory card file system
	Total capacity[6, 7]	Total of capacity in use and capacity not in use for the memory card file system
System interface hundred-gigabitethernet	Interface status according to the setting of 100-Gbit/s interface	It displays interfaces to be disabled when the 100-Gbit/s interface that can be configured in the AX3660S-48XT4QW model is enabled. This display item is invalid in other models.
disable(10G)	Invalid Ethernet interface[9]	Port number "-" (hyphen) when there are no invalid ports
enable(100G)	Ethernet interface that can work as a 100 Gbit/s interface[9]	Port number "-" (hyphen) when there are no 100 Gbit/s ports

#1

It is displayed only in replaceable power supply models.

#2

This item is displayed when the status of the relevant module is either active or fault.

#3

In fixed power supply models, the fan location is indicated in FAN(y) format, and in replaceable power supply models, it is in FANx(y). 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 11-4: Correspondences between fan numbers, operation log data, and chassis (in fixed power supply models)

Command and operation log display	Location on the chassis
FAN(1)	On the right in the rear of the chassis 1
FAN(2)	On the right in the rear of the chassis 2
FAN(3)	On the right in the rear of the chassis 3
FAN(4)	On the right in the rear of the chassis 4

Table 11-5: Correspondences between fan numbers, operation logs, and chassis (in replaceable power supply models)

Unit	Unit correspondence	
	Command and operation log display	Location on the chassis
PS-M	FAN1(1)	Power supply unit on the right in the rear
	FAN2(1)	Power supply unit on the left in the rear
FAN-M	FAN3(1)	On the right in the rear of the fan unit 1
	FAN3(2)	On the right in the rear of the fan unit 2
	FAN3(3)	On the right in the rear of the fan unit 3
	FAN3(4)	On the right in the rear of the fan unit 4

#4

    If no fan unit is installed, no item is displayed regardless of the fan direction of the power supply unit.

#5

    It is displayed only in fixed power supply models.

#6

    These items are displayed when the memory card status is enabled or write protect.

#7

    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.

    In addition, when the used capacity exceeds 95 percent of the total capacity, the unused capacity might be displayed as a negative value. If unused capacity is displayed as a negative value, delete the user files to free up sufficient unused capacity.

#8

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

#9

    It displays the information about the interface set by the "system interface hundredgigabitethernet" configuration command and the tengigabitethernet interface to be disabled. This item indicates a behavior status, and the ports displayed as disable cannot be used.

    Note that the "system interface hundredgigabitethernet" configuration command takes effect after the device is restarted.

Example 2

The following is an example of displayed resource information.

Figure 11-5: Displaying resource information

```
> show system
Date 20XX/06/17 15:09:34 UTC
System: AX3660S-24T4XW, OS-L3M (SL-L3A-001) Ver. 12.1.C
Node : Name=System Name
 :
 :
   Device resources
       Current selected swrt_table_resource : l3switch-2
       Current selected swrt_multicast_table : Off
       Current selected unicast multipath number: 4
       Current selected port-channel load-balance-all-port: On
       IP routing entry :
           Unicast : current number=98 , max number=8093
           Multicast : current number=0 , max number=2048
```

```
        ARP : current number=2 , max number=15360
    IPv6 routing entry :
        Unicast : current number=34 , max number=3007
        Multicast : current number=0 , max number=1024
        NDP : current number=2 , max number=15360
    Multipath table entry : current number=0 , max number=512
    MAC-Address table entry : current number=1014 , max number=81920
    VXLAN Layer2 Nexthop entry : current number=15 , max number=160
    System Layer2 Table Mode : mode=0
    Flow detection mode : layer3-mirror-5
      Used resources for filter inbound(Used/Max)
              MAC       IPv4      IPv6
              n/a    0/1024    2/1024
      Used resources for QoS(Used/Max)
              MAC       IPv4      IPv6
              n/a    0/ 512       n/a
      Used resources for UPC(Used/Max)
              MAC       IPv4      IPv6
              n/a    0/ 512       n/a
      Used resources for Mirror inbound(Used/Max)
              MAC       IPv4      IPv6
           2/ 512    3/ 512    0/ 512
      Used resources for TCP/UDP port detection pattern
        Resources(Used/Max):  1/32
          Destination Port   Used
            100-200          :      -/  -/mirror
    Flow detection out mode : layer3-2-out
      Used resources for filter outbound(Used/Max)
              MAC       IPv4      IPv6
           0/ 256    2/ 256    0/ 256
    Flow action change
        cos                 : enable
        arp discard class   : enable
        arp reply cos       : enable
```

Display items in Example 2

Table 11-6: Information displayed by the show system command (resource information)

Item	Displayed information	Displayed detailed information
Device resources	Hardware entry information	—
Current selected swrt_table_resource	Hardware table entry pattern	Pattern of the number of entries in the hardware table that is set l3switch-1: Information for only IPv4 is displayed. l3switch-2: Information for both IPv4 and IPv6 is displayed. l3switch-3: IPv6 unicast priority mode
Current selected swrt_multicast_table	Whether both IP multicast routing function and IGMP/MLD snooping function can be used at the same time	On: IP multicast routing function and IGMP/MLD snooping function can be used at the same time. Off: IP multicast routing function and IGMP/MLD snooping function cannot be used at the same time.
Current selected unicast multipath number	Maximum number of multipaths that can be handled as a single unicast route by the Switch	Maximum number of multipaths that can be set in the hardware table for a unicast route (4, 8, or 16). Note that when the maximum number of multipaths is changed by using a configuration command, the change is not immediately applied to the value displayed for this item. To apply the change, restart the device.

Item	Displayed information	Displayed detailed information
Current selected port-channel load-balance-all-port	Transfer allocated among switches with link aggregation enabled in a stack configuration	On: Forwarding packets by selecting a sending port from all ports of member switches belonging to the link aggregation Off: Forwarding packets, with priority, to the port of the member switch that received them
IP routing entry Unicast	Number of IPv4 unicast routing entries set on the hardware	current number: Number of IPv4 unicast routing table entries currently set on the hardware.[1] max number: Maximum number of IPv4 unicast routing table entries that can be set on the hardware. Note: A hyphen (-) is displayed if the status of the Main board item is Fault.
IP routing entry Multicast	Number of IPv4 multicast routing entries set on the hardware	current number: Number of IPv4 multicast routing table entries currently set on the hardware. max number: Maximum number of IPv4 multicast routing table entries that can be set on the hardware. Note: A hyphen (-) is displayed if the status of the Main board item is Fault.
IP routing entry ARP	Number of ARP entries set on the hardware	current number: Number of ARP entries currently set on the hardware. max number: Maximum number of ARP entries that can be set on the hardware. Note: A hyphen (-) is displayed if the status of the Main board item is Fault.
IPv6 routing entry Unicast	Number of IPv6 unicast routing entries set on the hardware	current number: Number of IPv6 unicast routing table entries currently set on the hardware.[2] max number: Maximum number of IPv6 unicast routing table entries that can be set on the hardware. Note: A hyphen (-) is displayed if the status of the Main board item is Fault.
IPv6 routing entry Multicast	Number of IPv6 multicast routing entries set on the hardware	current number: Number of IPv6 multicast routing table entries currently set on the hardware. max number: Maximum number of IPv6 multicast routing table entries that can be set on the hardware. Note: A hyphen (-) is displayed if the status of the Main board item is Fault.
IPv6 routing entry NDP	Number of NDP entries set on the hardware	current number: Number of NDP entries currently set on the hardware. max number: Maximum number of NDP entries that can be set on the hardware. Note: A hyphen (-) is displayed if the status of the Main board item is Fault.

Item	Displayed information	Displayed detailed information
Multipath table entry	Number of multipath table entries set on the hardware	current number: Number of multipath table entries currently set on the hardware. max number: Maximum number of multipath table entries that can be set on the hardware. Note: A hyphen (-) is displayed if the status of the Main board item is Fault.
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. The number of MAC address table entries includes the following MAC addresses in addition to the MAC address entries displayed by the "show mac-address-table" command: • Device MAC addresses as many as VLAN interfaces for which IP addresses have been set, and MAC addresses set by MAC addresses for each VLAN. • MAC address of the virtual router for which the Switch was selected as the master in VRRP. 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.
VXLAN Layer2 Nexthop entry	Number of Nexthop entries when VXLAN Network ports make up a link aggregation	current number: Number of Nexthop entries currently set on the hardware max number: Maximum number of Nexthop entries that can be set on the hardware. Zero (0) is displayed when the VXLAN function is disabled. 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. (For details, see "Configuration Command Reference Vol. 1, 10 Device Management".)
Flow detection mode	Receiving-side flow detection mode for the filters and QoS function	For details, see "Configuration Command Reference Vol. 1, 24. Flow Detection Modes/Flow Performance".
Used resources for filter inbound(Used/Max), and Used resources for filter outbound(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[#3]	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 receiving-side flow detection mode and the sending-side 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[#3]	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 receiving-side flow detection mode, QoS flow lists marked "n/a" are not subject to detection.
Used resources for UPC(Used/Max)	The number of entries with the UPC setting 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[#3]	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 receiving-side flow detection mode, QoS flow lists marked "n/a" are not subject to detection.
Used resources for Mirror inbound(Used/Max), and Used resources for Mirror outbound(Used/Max)	Number of entries currently registered as policy-based mirroring conditions on the target interface, and the maximum number of specifiable entries. The number of the setting entries is the total of the policy-based mirroring condition entries set during configuration.	
	Target access list type	MAC: Policy-based mirroring for MAC
		IPv4: Policy-based mirroring for IPv4
		IPv6: Policy-based mirroring for IPv6
	Number of entries that have been set and the maximum number of entries that can be set	In the receiving-side flow detection mode and the sending-side flow detection mode, access lists marked "n/a" are not subject to detection.
Used resources for TCP/UDP port detection pattern	Of the receiving-side interface filter conditions and QoS flow detection conditions that have been registered on the device, the following items are displayed: the number of TCP/UDP port number detection patterns that use hardware resources, the maximum number of detection patterns that can be set, and the details of TCP/UDP port number detection patterns.	

Item	Displayed information	Displayed detailed information
	Number of detection patterns that have been set/Maximum number of detection patterns that can be set	Resources(Used/Max): Number of TCP/UDP port number detection patterns that use hardware resources, and the maximum number of detection patterns that can be set on the device Note: Enabling the VXLAN PMTU function consumes one hardware resource.
	Source and destination TCP/UDP port numbers	Source Port: Source TCP/UDP port number Destination Port: Destination TCP/UDP port number
	Details of TCP/UDP port number detection patterns	Details of the TCP/UDP port number detection patterns that use hardware resources. filter: The patterns are set with filter conditions. QoS: The patterns are set with QoS flow detection conditions. mirror: Set by policy-based mirroring detection conditions -: Not set
Flow detection out mode	Sending-side flow detection mode for filtering function	For details, see "Configuration Command Reference Vol. 1, 24. Flow Detection Modes/Flow Performance".
Flow action change	Status of the function for changing which frames are subject to priority determination	Status of the function for changing which frames are subject to priority determination. (If this is enabled, enable is displayed for each parameter. If a target parameter is not enabled, nothing is displayed.) cos: Priority arp discard class: Queuing priority of ARP broadcast frames arp reply cos: CoS value of ARP reply broadcast frames received by the Switch

#1

    During startup of the device, the initial routing entries for the device are set. The value displayed during this period might therefore be different from the number of routing entries displayed by the "show ip route" command.

#2

    During startup of the device, the initial routing entries for the device are set. The value displayed during this period might therefore be different from the number of routing entries displayed by the "show ipv6 route" command.

    IPv6 link-local addresses and IPv6 link-local multicast routing entries are not included in the number of entries. Therefore, the number of these entries are different from the number of routing entries displayed by the "show ipv6 route" command.

#3

    There is no capacity limit of each target port.

Impact on communication

None

Response messages

Table 11-7: List of response messages for the show system command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

None

clear control-counter

Resets the number of device restarts due to a failure and the number of device restarts due to a line failure to zero.

Syntax

```
clear control-counter
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} clear control-counter
```

Example

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

```
> clear control-counter
```

Display items

None

Impact on communication

None

Response messages

Table 11-8: List of response messages for the clear control-counter command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show environment [temperature-logging]
```

Example 1

The following shows an example of displaying the operating status.

Figure 11-6: Result of executing the show environment command (in fixed power supply models)

```
> show environment
Fan environment
    Fan      : Fan(1) = active
               Fan(2) = active
               Fan(3) = active
               Fan(4) = active
               Speed = normal
    Fan mode : 1 (silent)

Power environment
    PS1 : active
    PS2 : active

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.
>
```

Figure 11-7: Result of executing the show environment command (in replaceable power supply models)

```
> show environment
Date 20XX/09/14 09:13:21 UTC
Power slot 1 : PS-M(AC), Direction = F-to-R
Power slot 2 : PS-M(AC), Direction = F-to-R
```

```
Fan slot     : FAN-M, Direction = F-to-R

Fan environment
    Power slot 1 : Fan1(1) = active
                   Speed = --------
    Power slot 2 : Fan2(1) = active
                   Speed = --------
    Fan slot     : Fan3(1) = active
                   Fan3(2) = active
                   Fan3(3) = active
                   Fan3(4) = active
                   Speed = normal
    Fan mode     : 1 (silent)

Power environment
    Power slot 1 : active
    Power slot 2 : active

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.
    Fan slot    :  total   : 36 days and 6 hours.
                   critical : 0 days and 0 hours.
>
```

Display items in Example 1

Table 11-9: Information displayed by the show environment command (in fixed power supply models)

Item	Displayed information	Displayed detailed information
Fan environment		
Fan[#1]	Fan behavior status	active: Running fault: A failure has occurred.
Speed	The rotational speed of the fan	normal: Normal rotation high: High-speed rotation stop: Stopped rotation
Mode	Fan operating mode	1 (silent): Reducing switch noise takes priority 2 (cool): Keeping the switch cool takes priority
Power environment		
PS1	Status of input power supply unit 1	active: Supplied normally fault: No supply/voltage fault (when the "power redundancy-mode redundancy-check" configuration command is set) unused: No supply/voltage fault (when the "power redundancy-mode redundancy-check" configuration command is not set)
PS2	Status of input power supply unit 2	active: Supplied normally fault: No supply/voltage fault (when the "power redundancy-mode redundancy-check" configuration command is set) unused: No supply/voltage fault (when the "power redundancy-mode redundancy-check" configuration command is not set)

Item	Displayed information	Displayed detailed information
Temperature environment	Temperature information	—
Main	Intake-air temperature information	Displays temperature information for a device.
Warning level[#2]	Operating condition level	normal: Normal caution: Caution (High or low temperature)
Accumulated running time[#3]		
Main	total: Cumulative operating time of the device critical: Cumulative operating time of the device at 50 degrees Celsius or higher	During normal operation, total is displayed. fault: The operating time could not be loaded. ****: The operating time is being loaded.

#1

The fan location is indicated in FAN(x) format. The x value indicates the fan unit 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 11-10: Correspondences between fan numbers, operation log data, and chassis (in fixed power supply models)

Command and operation log display	Location on the chassis
FAN(1)	On the right in the rear of the chassis 1
FAN(2)	On the right in the rear of the chassis 2
FAN(3)	On the right in the rear of the chassis 3
FAN(4)	On the right in the rear of the chassis 4

#2

Warning level is displayed as a result of evaluating the changes in intake temperature. If the sensor detects a temperature of 60 degrees Celsius or higher, the software stops.

Figure 11-8: Operating environment level and temperature values (in fixed power supply models)
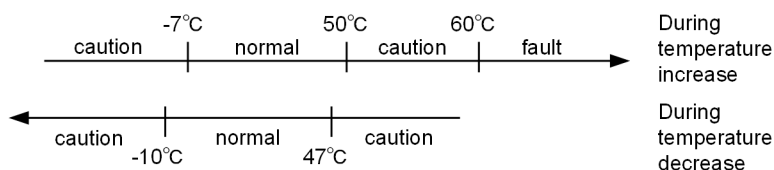
#3

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)

Table 11-11: Information displayed by the show environment command (in replaceable power supply models)

Item	Displayed information	Displayed detailed information
Power slot 1	Power supply unit type	PS-M(AC): AC power supply unit PS-M(DC): DC power supply unit notconnect: Not installed
	Direction: Direction of the fan[#1]	F-to-R: Front air intake and rear air exhaust R-to-F: Rear air intake and front air exhaust
Power slot 2	Power supply unit type	PS-M(AC): AC power supply unit PS-M(DC): DC power supply unit notconnect: Not installed
	Direction: Direction of the fan[#1]	F-to-R: Front air intake and rear air exhaust R-to-F: Rear air intake and front air exhaust
Fan slot	Fan slot type	FAN-M: Fan slot notconnect: Not installed notsupport: Not supported
	Direction: Direction of the fan[#1]	F-to-R: Front air intake and rear air exhaust R-to-F: Rear air intake and front air exhaust
Fan environment		
Power slot	Slot number	—
Fan[#2]	Fan behavior status	active: Running fault: A failure has occurred. notconnect: Not installed
Speed	The rotational speed of the fan	Displays "--------".
Fan slot		
Fan[#2]	Fan behavior status	active: Running fault: A failure has occurred. notconnect: Not installed notsupport: Not supported
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		
Power slot	Status of the input power supply unit	active: Supplied normally fault: No power is being supplied or there is an abnormal voltage. notconnect: Not installed
Temperature environment	Temperature information	—
Main	Intake-air temperature information	Displays temperature information for a device.

Item	Displayed information	Displayed detailed information
Warning level[#3]	Operating condition level	normal: Normal caution: Caution (High or low temperature)
Accumulated running time[#4]		
Main	total: Cumulative operating time of the device critical: Cumulative operating time of the device at 50 degrees Celsius or higher	During normal operation, total is displayed. fault: The operating time could not be loaded. ****: The operating time is being loaded.
Fan slot	total: Cumulative operating time of the fan critical: Cumulative operating time of the fan at 50 degrees Celsius or higher	During normal operation, total is displayed. notconnect: Not installed notsupport: Not supported fault: The operating time could not be loaded. ****: The operating time is being loaded.

#1 The information is displayed only when a power supply unit or a fan is installed.

#2

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 11-12: Correspondences between fan numbers, operation logs, and chassis (in replaceable power supply models)

Unit	Unit correspondence	
	Command and operation log display	Location on the chassis
PS-M	FAN1(1)	Power supply unit on the right in the rear
	FAN2(1)	Power supply unit on the left in the rear
FAN-M	FAN3(1)	On the right in the rear of the fan unit 1
	FAN3(2)	On the right in the rear of the fan unit 2
	FAN3(3)	On the right in the rear of the fan unit 3
	FAN3(4)	On the right in the rear of the fan unit 4

#3 Warning level is displayed as a result of evaluating the changes in intake temperature.

If the sensor detects a temperature of 60 degrees Celsius or higher (for FAN-04) or 50 degrees Celsius or higher (for FAN-04R), the software stops.

Figure 11-9: Operating environment level and temperature values (in replaceable power supply models with FAN-04 installed)
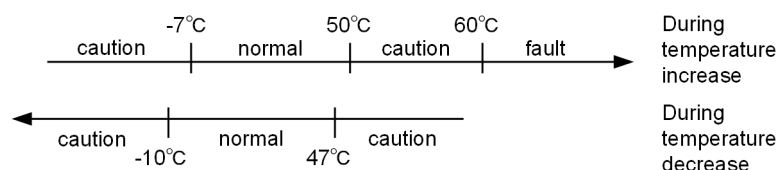
Figure 11-10: Operating environment level and temperature values (in replaceable power supply model with FAN -04R installed)
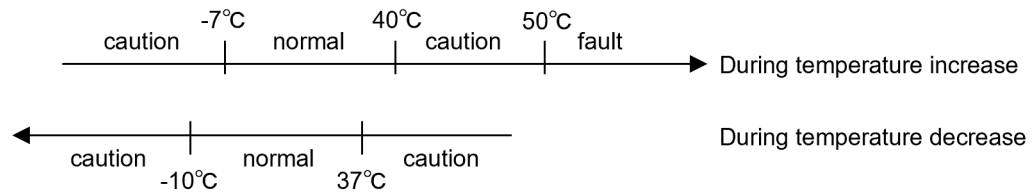
#4

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 11-11: 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 11-13: 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.)

Item	Displayed information	Displayed detailed information
" "	Blank	Temperature aggregation not yet performed

Impact on communication

None

Response messages

Table 11-14: List of response messages for the show environment command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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 [switch <switch no.>] [stop] [{no-dump-image | dump-image}] [-f]
```

Input mode

User mode and administrator mode

Parameters

switch <switch no.>

> Executes the command on the member switch whose switch number is specified.

> This parameter can be specified only on the master switch when the stack is configured. For the specifiable range of values, see "Specifiable values for parameters".

> Behavior when this parameter is omitted:

>> The command is executed on the local device.

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.

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command <switch no.> reload [stop] [{no-dump-image | dump-image}] [-f]
```

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(rmdump   01/01 00:00) 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 memory. 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.

Response messages

Table 11-15: List of response messages for the reload command

Message	Description
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.
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
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. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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] [{unicast | multicast | layer-2}]
show tech-support switch <switch no.> [page] [<password>] [no-config] [{unicast | multicast | l
ayer-2}]
```

Input mode

User mode and administrator mode

Parameters

switch <switch no.>

> Executes the command on the member switch whose switch number is specified.

> This parameter can be specified only in administrator mode on the master switch when the stack is configured. For the specifiable range of values, see "Specifiable values for parameters".

> Behavior when this parameter is omitted:

>> The command is executed on the local device.

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 and switch parameters are 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.

In a stack configuration, this parameter specified for a member switch other than the master switch becomes invalid.

Behavior when this parameter is omitted:

The collected information is output to the console terminal screen.

{unicast | multicast | layer-2}

unicast

Collects information required for communication failure analysis of unicast routing.

multicast

Collects information required for communication failure analysis of multicast routing.

layer-2

Collects information required for communication failure analysis of Layer 2 protocols.

Behavior when this parameter is omitted:

Basic information about the hardware and software is collected.

Behavior when all parameters are omitted:

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

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command {<switch no.> | all}
show tech-support [page] [<password>] [no-config] [{unicast | multicast | layer-2}]
```

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 11-12: 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 11-13: Storing the collected information in the FTP server

  ```
  > show tech-support ftp
  Specify Host Name of FTP Server.        :
  Specify Host Name of FTP Server.        : ftpserver.example.com
  Specify User ID for FTP connections.    : user1
  Specify Password for FTP connections.   : <password for user1>
  Specify Path Name on FTP Server.        : /usr/home/user1
  ```

```
Specify File Name of log and Dump files: support
Mon Dec 18 20:42:58 UTC 20XX
Transferred support.txt .
Executing.
...
Operation normal end.
########## Dump files' Information ##########
***** ls -l /dump0 *****
total 2344
-rwxrwxrwx  1 root  wheel  2400114 Dec  8 16:46 rmdump
***** ls -l /usr/var/hardware *****
total 1368
-rwxrwxrwx  1 root  wheel  738699 Dec 27 11:56:16 20XX 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.
...
Operation normal end.
>
```

Display items

Table 11-16: 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 Tech-Support Unicast Log: Detailed information about unicast routing Tech-Support Multicast Log: Detailed information about multicast routing Tech-Support Layer-2 Log: Detailed information about Layer 2 protocols
########## 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

222

Response messages

Table 11-17: List of response messages for the show tech-support command

Message	Description
<File Name>:Permission denied.	A file that has the same name as <File Name> in the response message already exists in the destination directory. You do not have permissions to modify the file. Change the permissions for the file in the destination directory, or change the name of the file to be saved.
<Host Name>: Unknown host	The host name (<Host-name>) is invalid.
<Path>: No such file or directory.	The directory specified for <Path> does not exist.
<Path>: Not a directory.	<Path> is not a directory.
<Path>: Permission denied.	You do not have permissions to access the <Path> directory.
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
connection Time out.	An attempt to connect with the FTP server failed. Check communication with the FTP server.
Exec failed.	The command execution failed.
Is the Password retyped?(y/n)	When y is selected in response to the message Is the Password retyped?, the password can be re-entered. When n is selected, the command execution is continued assuming that an incorrect password was entered.
Login incorrect.Login failed.	You are not permitted to log in to the specified host. A login attempt has failed.
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Operation normal end.	The file transfer ended normally.
Password for Administrator Mode Invalid.	The password for administrator mode entered in the <password> parameter is incorrect.
Sorry, already execute show tech-support	Another user is executing "show tech-support" command.
Specify File Name of 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.
Specify Host Name of 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.
Specify Password for Administrator Mode.:	Enter the password for administrator mode.

Message	Description
Specify Password for FTP connections. :	Enter the password of the User ID entered for the response message "Specify User ID for FTP connections. :".
Specify Path Name on 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.
Specify User ID for FTP connections. :	Specify a login user name. Note that the login user name entered in response to this message is reflected in <User ID> in subsequent response messages.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number
Write failed.	An attempt to transfer the file failed. Check the free capacity of the destination and the state of the communication line.

Notes

1. If unicast, multicast, or layer-2 parameters are specified, route information and other information are collected. Accordingly, depending on the network configuration, internal flash memory might no longer be available to users if a large amount of information is collected.

   If the information collected by the command is redirected to a file, make sure that the information is saved in compressed format.

   Example

   ```
   > show tech-support unicast | gzip > show-tech.txt.gz
   ```

2. 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, and the display time with the unicast, multicast, or layer-2 parameters depends on the network configuration.

   - When the information is displayed on the remote operation terminal screen, the display interval with no parameter is 30 seconds, and the display interval with the unicast, multicast, or layer-2 parameters depends on the network configuration.

3. 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.

4. 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.

5. 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

show tcpdump (tcpdump)

Monitors incoming and outgoing packets.

This command can be used to check the communication status of the incoming and outgoing Layer 3 (IPv4/IPv6/ARP) traffic. For example, you can monitor packets, such as remote access requests sent to the Switch, or packets sent from the Switch for certain routing protocols.

The following table shows a list of packets that can be monitored and analyzed.

Table 11-18: List of packets that can be monitored and analyzed

Address family	Type	Description
IPv4	TCP	Analyzes various types of TCP communication, such as BGP4 or telnet.
	UDP	Analyzes various types of UDP communication, such as SNMP or RIP.
	ICMP	Analyzes ping packets and the like.
	OSPF	Analyzes packets over the OSPF routing protocol.
	IGMP	Analyzes packets over IGMP.
	PIM	Analyzes packets over PIM multicast.
IPv6	TCP	Analyzes various types of TCP communication, such as BGP4+ or telnet.
	UDP	Analyzes various types of UDP communication, such as SNMP or RIPng.
	ICMP6	Analyzes ping packets and the like.
	OSPF6	Analyzes packets over the OSPFv3 routing protocol.
	PIM	Analyzes packets over PIM multicast.
ARP	ARP	Analyzes packets over the ARP protocol.

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
> - Management port

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 follows:

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.

<u>Combinations of basic elements</u>

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.

<u>Example of specifying <expression></u>

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.

Operation when a stack configuration is used

The command can be used in the same way as for a standalone configuration.

Example 1

When IPv4/IPv6 packets are monitored

Figure 11-14: Monitoring IPv4/IPv6 packets

```
# show tcpdump interface vlan 10
Date 20XX/01/20 18:36:00 UTC
tcpdump: listening on VLAN0010
18:36:53.390062 ip6 56: v6hostA.example.com > v6.hostB.example.com: icmp6: echo request seq 20
18:36:54.220039 ip 84: hostA.example.com > hostB.example.com:
         1          2                3
icmp 64: echo request seq 43
         4
^C
4 packets received by filter      <--5
0 packets dropped by kernel       <--6
```

Display items in Example 1

Table 11-19: Information displayed when IPv4/IPv6 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. For encapsulated packets such as tunneled packets, multiple address pairs are displayed.
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 11-15: 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 46: arp who-has 100.100.100.1 tell 100.100.100.2
16:07:29.683758 arp 46: arp reply 100.100.100.1 is-at 0:12:e2:98:dc:1
        1              2                          3
^C
4 packets received by filter      <--4
0 packets dropped by kernel       <--5
```

Display items in Example 2

Table 11-20: 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.

Example 3

When tcpdump is executed with another parameter specified while ping (IPv4 and IPv6) is being performed from hostA.example.com (10.10.10.10) and v6hostA.example.com (fec0::1) to the Switches myhost.example.com (20.20.20.20) and v6myhost.example.com (fec0::2)

231

Figure 11-16: Result of executing the command with an interface name specified

```
# show tcpdump interface vlan 10
Date 20XX/01/20 20:23:00 UTC
tcpdump: listening on VLAN0010
20:23:10.113591 ip 84: hostA.example.com > myhost.example.com: icmp 64: echo request seq 20
20:23:10.113692 ip 84: myhost.example.com > hostA.example.com: icmp 64: echo reply seq 20
20:23:10.213696 ip6 56: v6hostA.example.com > v6myhost.example.com: icmp6: echo request seq 43
20:23:10.213765 ip6 56: v6myhost.example.com > v6hostA.example.com: icmp6: echo reply seq 43
^C
4 packets received by filter
0 packets dropped by kernel
```

Figure 11-17: Result of executing the command with no-resolv specified not to perform reverse lookup

```
# show tcpdump interface vlan 10 no-resolv
Date 20XX/01/20 20:23:00 UTC
tcpdump: listening on VLAN0010
20:23:10.113591 ip 84: 10.10.10.10 > 20.20.20.20: icmp 64: echo request seq 20
20:23:10.113692 ip 84: 20.20.20.20 > 10.10.10.10: icmp 64: echo reply seq 20
20:23:10.213696 ip6 56: fec0::1 > fec0::2: icmp6: echo request seq 43
20:23:10.213765 ip6 56: fec0::2 > fec0::1: icmp6: echo reply seq 43
^C
4 packets received by filter
0 packets dropped by kernel
```

Figure 11-18: Result of executing the command with no-domain specified not to display the host name and subsequent part (domain name)

```
# show tcpdump interface vlan10 no-domain
Date 20XX/01/20 20:23:00 UTC
tcpdump: listening on VLAN0010
20:23:10.113591 ip 84: hostA > myhost: icmp 64: echo request seq 20
20:23:10.113692 ip 84: myhost > hostA: icmp 64: echo reply seq 20
20:23:10.213696 ip6 56: v6hostA > v6myhost: icmp6: echo request seq 43
20:23:10.213765 ip6 56: v6myhost > v6hostA: icmp6: echo reply seq 43
^C
4 packets received by filter
0 packets dropped by kernel
```

Figure 11-19: Result of executing the command with ip6 specified as <expression>

```
# show tcpdump interface vlan 10 ip6
Date 20XX/01/20 20:23:00 UTC
tcpdump: listening on VLAN0010
20:23:10.213696 ip6 56: v6hostA > v6myhost: icmp6: echo request seq 43
20:23:10.213765 ip6 56: v6myhost > v6hostA: icmp6: echo reply seq 43
^C
4 packets received by filter
0 packets dropped by kernel
```

Figure 11-20: Result of executing the command with count <count> specified

```
# show tcpdump interface vlan 10 count 3
Date 20XX/01/20 20:23:00 UTC
tcpdump: listening on VLAN0010
20:23:10.113591 ip 84: hostA.example.com > myhost.example.com: icmp 64: echo request seq 20
20:23:10.113692 ip 84: myhost.example.com > hostA.example.com: icmp 64: echo reply seq 20
20:23:10.213696 ip6 56: v6hostA.example.com > v6myhost.example.com: icmp6: echo request seq 43
4 packets received by filter
0 packets dropped by kernel
```

Figure 11-21: Result of executing the command with no-time specified not to display a time stamp at each line

```
# show tcpdump interface vlan 10 no-time
Date 20XX/01/20 20:23:00 UTC
tcpdump: listening on VLAN0010
ip 84: hostA.example.com > myhost.example.com: icmp 64: echo request seq 20
ip 84: myhost.example.com > hostA.example.com: icmp 64: echo reply seq 20
ip6 56: v6hostA.example.com > v6myhost.example.com: icmp6: echo request seq 43
ip6 56: v6myhost.example.com > v6hostA.example.com: icmp6: echo reply seq 43
^C
4 packets received by filter
```

```
0 packets dropped by kernel
```

Figure 11-22: Result of executing the command with writefile specified to specify a file name and save a dump to the file

```
# show tcpdump interface vlan 10 writefile mydump
Date 20XX/01/20 20:23:00 UTC
tcpdump: listening on VLAN0010
^C
4 packets received by filter
0 packets dropped by kernel
```

Figure 11-23: Result of executing the command with readfile specified to specify a file name to read and display a dump from the file

```
# show tcpdump readfile mydump
Date 20XX/01/20 20:23:00 UTC
reading from file mydump, link-type NULL (BSD loopback)
20:23:10.113591 ip 84: hostA.example.com > myhost.example.com: icmp 64: echo request seq 20
20:23:10.113692 ip 84: myhost.example.com > hostA.example.com: icmp 64: echo reply seq 20
20:23:10.213696 ip6 56: v6hostA.example.com > v6myhost.example.com: icmp6: echo request seq 43
20:23:10.213765 ip6 56: v6myhost.example.com > v6hostA.example.com: icmp6: echo reply seq 43
```

Figure 11-24: Result of executing the command with readfile specified to read a dump from the file, and with icmp specified as <expression> to display only icmp

```
# show tcpdump readfile mydump icmp
Date 20XX/01/20 20:23:00 UTC
reading from file mydump, link-type NULL (BSD loopback)
20:23:10.113591 ip 84: hostA.example.com > myhost.example.com: icmp 64: echo request seq 20
20:23:10.113692 ip 84: myhost.example.com > hostA.example.com: icmp 64: echo reply seq 20
```

Display items in Example 3

None

Impact on communication

None

Response messages

Table 11-21: List of response messages for the show tcpdump command

Message	Description
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).
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.

Message	Description
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.
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.

Message	Description
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.

Notes

1. This command can monitor incoming and outgoing software processing packets, such as routing protocols.

2. This command cannot monitor packets other than incoming and outgoing packets, such as an IPv4/IPv6 transfer packets, MPLS transfer packets, multicast transfer packets, or tunnel processing packets. Note that filtered packets or packets that are not processed by software (various Layer 2 packets such as PPP), which are one type of incoming and outgoing packet, 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 null/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 null/loopback header section.

5. The length of the null/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.

backup

Saves device information and information about active applications to a memory card or remote FTP server. The device information includes the password information, configuration, license information, and IPv6 DHCP server DUID file.

Syntax

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

Input mode

Administrator mode

Parameters

switch <switch no.>

> Executes the command on the member switch whose switch number is specified.
> This parameter can be specified only on the master switch when the stack is configured. For the specifiable range of values, see "Specifiable values for parameters".
> Behavior when this parameter is omitted:
>> The command is executed on the local device.

mc

> Specifies the memory card as the backup destination.

ftp <ftp-server>

> Specifies a remote FTP server as the backup destination. Specify the IP address or host name of the server (IPv4 address or IPv6 address) for <ftp-server>.
> In a stack configuration, this parameter specified for a member switch other than the master switch becomes invalid.

<filename>

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

no-software

> No software is backed up.
> Behavior when this parameter is omitted:
>> Backup, including software information, is performed.

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} backup mc <filename> [no-software]
```

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.

Executing.
...
Operation normal end.
ftp transfer succeeded.
Backup information success!
```

Example 3

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

```
> enable
# backup mc MCBackup.dat no-software
Backup information to MC (MCBackup.dat).
Copy file to MC...
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 or Layer 3 protocol is set shorter than the initial value on neighboring devices, communication might be interrupted when the connection over the Layer 2 or Layer 3 protocol is disconnected.

Response messages

Table 11-22: List of response messages for the backup command

Message	Description
/usr/var/update/k.img is not exist. please put k.img to /usr/var/update and retry.	The file k.img does not exist in /usr/var/update. Copy k.img to /usr/var/update and then re-execute the command.
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Filename is invalid	A file with the specified name could not be created on a memory card. Specify another file name.
ftp transfer failed.	An attempt to transfer the device information by using the "backup ftp" command failed.
MC file write error.	Writing to the memory card failed. There might not be enough free space on the memory card. 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 write protected.	Make sure the memory card's protect switch is not set to "▼Lock". If the switch is set to "▼Lock", slide the switch, and then insert the memory card again. Make sure there is no dust in the memory card slot. If there is dust, wipe it off with a dry cloth and insert the memory card.
MC not found.	A memory card was not inserted into the slot. 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 insert the memory card.
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Saving file(<file name>) to MC failed.	Writing to the memory card failed.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number
This command is executable only the start-up from flash memory	The command could not be executed because the switch booted from a memory card. Start up the switch from flash memory and then re-execute the command.

Notes

- Before using the "backup ftp" command, make sure that the target FTP server has about 50 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.
- Perform backup and restoration between the same models.
- When the file k.img does not exist in the /usr/var/update directory, this command cannot be executed. Before executing the command, copy the k.img file to /usr/var/update.
- 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.
- Accessing a memory card increases load on the device. Before specifying the mc parameter, if the mon-

itoring time and sending interval of the Layer 2 or Layer 3 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.

restore

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

Syntax

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

Input mode

Administrator mode

Parameters

switch <switch no.>

Executes the command on the member switch whose switch number is specified.
This parameter can be specified only on the master switch when the stack is configured. For the specifiable range of values, see "Specifiable values for parameters".
Behavior when this parameter is omitted:

The command is executed on the local device.

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. Specify the IP address or host name of the server (IPv4 address or IPv6 address) for <ftp-server>.
In a stack configuration, this parameter specified for a member switch other than the master switch becomes invalid.

<filename>

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

no-software

No software is restored.

Behavior when this parameter is omitted:

All the backup data is restored.

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} restore mc <filename> [no-software]
```

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.

Operation normal end.
ftp transfer succeeded.
Restore software.
```

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 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 interrupted when the connection over the Layer 2 or Layer 3 protocol is disconnected.

Response messages

Table 11-23: List of response messages for the restore command

Message	Description
another user is executing now.	This command cannot be executed because the "restore" or "ppup-date" command executed by another user is still in progress.
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
File is not found.	The specified file could not be found.
MC is busy.	Another process is accessing the memory card. Wait a while, and then re-execute the command.
MC not found.	A memory card was not inserted into the slot. 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 insert the memory card.
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Restore operation failed.	An attempt to restore the device information failed. There might not be enough free space on the disk of the Switch. Delete unnecessary files and then re-execute the command.

Message	Description
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

- When the device information has been restored, the device restarts automatically. During the restart, communication is temporarily suspended.

- 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.

- Accessing a memory card increases load on the device. Before specifying the mc parameter, if the monitoring time and sending interval of the Layer 2 or Layer 3 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.

- 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/p pupdate.exec` to delete files, and then re-execute the command.

- When restoring the devices that make up a stack, first restore the devices, and then configure the stack.

- When the "remote command" command is executed with the all parameter specified, the data is restored only to the master switch.

12 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

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show mc
```

Example

```
>show mc
Date 20XX/12/13 06:35:27 UTC
MC  : enabled
    Manufacture ID : 00000030
     24,077KB used
     971,008KB free
     995,085KB total
>
```

Display items

Table 12-1: 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. write protect: Writing to the memory card is not allowed. --------: 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: These items are displayed when the memory card status is enabled or write protect.

Impact on communication

None

Response messages

Table 12-2: List of response messages for the show mc command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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 [switch <switch no.>] [-f]
```

Input mode

User mode and administrator mode

Parameters

switch <switch no.>

>   Executes the command on the member switch whose switch number is specified.

>   This parameter can be specified only on the master switch when the stack is configured. For the specifiable range of values, see "Specifiable values for parameters".

>   Behavior when this parameter is omitted:

>>   The command is executed on the local device.

-f

>   Executes the command without displaying a confirmation message.

>   Behavior when this parameter is omitted:

>>   A confirmation message is displayed.

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} format mc [-f]
```

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

Response messages

Table 12-3: List of response messages for the format mc command

Message	Description
Can't access to MC by write protection.	The write protection switch of the memory card is set for the write-protected status. Reset the write protection switch to the write-permitted status, and then re-execute the command.
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Can't gain access to MC.	The memory card is not inserted, or an attempt to access the memory card failed.
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

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

- When the current directory is a directory on the memory card, if this command is executed, the current directory will no longer be valid. In such a case, use the "cd" command to change the directory by specifying the home directory or full path name.

show flash

Shows internal flash memory usage.

Syntax

```
show flash
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show flash
```

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 12-4: Information displayed by the show flash command

Item		Displayed information	Displayed detailed information
Flash	—	—	—
	used	Used capacity	Capacity being used 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

Item		Displayed information	Displayed detailed information
	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

#: If used capacity exceeds 95 percent of the total capacity, unused capacity might be displayed as a negative value. If unused capacity is displayed as a negative value, delete user files so as to free up enough unused capacity.

Impact on communication

None

Response messages

Table 12-5: List of response messages for the show flash command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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.

13 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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all}
show cpu { days [hours] [minutes] [seconds]
                    | hours [days] [minutes] [seconds]
                    | minutes [days] [hours] [seconds]
                    | seconds [days] [hours] [minutes] } detail
```

Example and display items

Figure 13-1: 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 13-2: 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]  CPU[2]  CPU[3]
Mar 13  09:20:18-23:59:59    5       4       5       6
Mar 14  00:00:00-23:59:59    4       4       2       6
Mar 15  00:00:00-23:59:59   25      30      18      27
     :
Mar 29  00:00:00-23:59:59    3       4       8       5
>
```

Table 13-1: 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 13-3: 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 13-2: 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 13-4: 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 13-3: 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 13-5: 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 13-6: 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]  CPU[2]  CPU[3]
Mar 13  14:43:14       5       4       5       6
Mar 13  14:43:15       4       4       2       6
Mar 13  14:43:16      25      30      18      27
    :
Mar 13  14:44:13       3       4       8       5
>
```

Table 13-4: 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

Response messages

Table 13-5: List of response messages for the show cpu command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show processes memory
remote command {<switch no.> | all} show processes cpu
```

Example 1

Show memory usage of processes with a higher priority.

Figure 13-7: Displaying the memory usage of processes

```
> show processes memory
Date 20XX/01/01 12:00:00 UTC
  PID From                            Text Static Alloc Stack  Real Process
  875 console                        3828    304  1056    44  2292 cli
  949 ??                              172    144  1056    16  1012 rtm
  996 console                         124     24  1056    16   992 sh
 1457 console                          16      4  1056    20   824 process
      :
      :
      :
>
```

Display items in Example 1

Table 13-6: 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.

Item	Displayed information	Displayed detailed information
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.
Static	Static data size	Shows the size of static data area for each running process in KB.
Alloc	Dynamic data size	Shows the size of dynamic data area for each running process in KB.
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 13-8: Displaying the CPU usage of processes

```
> show processes cpu
Date 20XX/01/01 12:00:00 UTC
  PID  LWP CPU   5Sec   1Min   5Min Runtime(ms) Process(lwp)
    0    1   0     3%     2%     0%           1 system(swapper)
    0    2   0     0%     0%     0%           0 system(idle/0)
    0    3   0     0%     0%     0%           0 system(softnet/0)
    0    4   0     0%     0%     0%           0 system(softbio/0)
     :
     :
     :
>
```

Display items in Example 2

Table 13-7: 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		
CPU	Core number	Shows the core number of the core for each running process.
5Sec	CPU usage for the past five seconds	Shows the CPU usage of each running process for the past five seconds in percentages.
1Min	CPU usage for the past minute	Shows the CPU usage of each running process for the past minute in percentages.
5Min	CPU usage for the past five minutes	Shows the CPU usage of each running process for the past five minutes in percentages.

Item	Displayed information	Displayed detailed information
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

Response messages

Table 13-8: List of response messages for the show processes command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number
The command cannot be executed. Try again.	The command could not be executed. Re-execute the command.

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

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show memory
```

Example

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

Figure 13-9: Displaying the information about the physical memory being used

```
> show memory
Date 20XX/01/23 12:00:00 UTC
    physical memory = 4,194,304KB( 4,096MB)
    used     memory = 1,572,864KB( 1,536MB)
    free     memory = 2,621,440KB( 2,560MB)
>
```

Display items

Table 13-9: 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

Response messages

Table 13-10: List of response messages for the show memory command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number
The command cannot be executed. Try again.	The command could not be executed. Re-execute the command.

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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} df [<option>] [<file name>]
```

Example and display items

None

Impact on communication

None

Response messages

Table 13-11: List of response messages for the df command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch \<switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. \<switch no.>: Switch number

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} du [<option>] [<file name>]
```

Example and display items

None

Impact on communication

None

Response messages

None

Notes

None

14 Dump Information

erase dumpfile

Deletes dump files stored in the dump file storage directory.

The dump file storage directory is "/dump0 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
- "ni##.###": NIF failure dump file

Operation when a stack configuration is used

    Execute the command on all member switches that belong to the stack on the master switch.

    You can also use the "remote command" command.

```
remote command {<switch no.> | all} erase dumpfile { all | <file name> }
```

Example

Figure 14-1: Deleting all the dump files

```
> erase dumpfile all
```

Figure 14-2: Deleting the memory dump file (rmdump)

```
> erase dumpfile rmdump
```

Impact on communication

None

Response messages

Table 14-1: List of response messages for the erase dumpfile command

Message	Description
<file name>: No such file or directory.	The specified file does not exist. Or, the specified file is not a dump file.
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show dumpfile
```

Example

Figure 14-3: Displaying a dump file

```
> show dumpfile
Date 20XX/07/16 15:17:50 UTC
  [/dump0]:
    File Name          rmdump
    Date               20XX/07/16 13:57:03
    Version            12.0
    Serial No          AA046AAA0000S40A0XXXXXX
    Factor             2101 25040201

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

>
```

Display items

Table 14-2: 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: Similarly, if there is no dump file storage directory, "No such directory." is displayed.

Note 3: If loading a dump file fails, a blank is displayed.

Impact on communication

None

Response messages

Table 14-3: List of response messages for the show dumpfile command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

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

15 Software Management

ppupdate

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

Syntax

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

Input mode

Administrator mode

Parameters

switch <switch no.>

Executes the command on the member switch whose switch number is specified.

This parameter can be specified only on the master switch when the stack is configured. For the specifiable range of values, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

The command is executed on the local device.

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.

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command <switch no.> ppupdate [test] [no-display] [-f] [no-reload] <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@
        (??) at 15:32 UTC...

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

Current version is 12.0
New version is 12.1
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.

Response messages

Table 15-1: List of response messages for the ppupdate command

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.
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
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 file <file-name>.	The contents of the specified file are invalid. Specify a valid file.
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
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.

Message	Description
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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. In a stack configuration, perform the update for each member switch.

set license

Sets the software license and an optional license.

Syntax

```
set license [switch <switch no.>] {key-file <file name> | key-code <license key>}
```

Input mode

Administrator mode

Parameters

switch <switch no.>

Executes the command on the member switch whose switch number is specified.

This parameter can be specified only on the master switch when the stack is configured. For the specifiable range of values, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

The command is executed on the local device.

key-file <file name>

Sets the software license and an optional license with a file specified.

key-code <license key>

Sets the software license and an optional license with a license key specified. 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.

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command <switch no.> set license {key-file <file name> | key-code <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

Response messages

Table 15-2: List of response messages for the set license command

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.
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. 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 license key \<license key\>.	The entered license key is invalid.
Invalid serial number \<license key\>.	The license key is invalid. \<license key\>: License key
No such file \<file name\>	The specified license key file does not exist. \<file name\>: Specified license key file
No such Switch \<switch no.\>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. \<switch no.\>: Switch number
Switch \<switch no.\> was deleted from stack.	The member switch was deleted from the stack configuration. \<switch no.\>: Switch number
This license is already registered.	This optional license has already been set.

Notes

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

show license

Shows the set software license and optional licenses.

Syntax

```
show license
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show license
```

Example

An example of displaying the software license and optional license is shown below:

```
> show license
Date 20XX/01/23 12:00:00 UTC
  Available: SL-L3L-004 OP-ULTG
    Serial Number        Licensed software
    1500-0001-0200-0000  SL-L3L-004(AX-P3660-G8)
    1600-0001-0200-0000  OP-ULTG(AX-P3660-F3)
>
```

Display items

Table 15-3: Information displayed by the show license command

Item	Displayed information	Displayed detailed information
Available:	Abbreviated software license and optional license names that are activated	—
Serial Number	Serial numbers of the software license and optional licenses that are set	—
Licensed software	Abbreviated software license and optional license names that have been set in the Switch (with the model name in parentheses)	"unknown(-----)" is displayed when the software name is unknown.

Impact on communication

None

Response messages

Table 15-4: List of response messages for the show license command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

None

erase license

Erases the specified optional license. Note that this command cannot delete the software license.

Syntax

```
erase license [switch <switch no.>] <serial no.>
```

Input mode

Administrator mode

Parameters

switch <switch no.>

Executes the command on the member switch whose switch number is specified.

This parameter can be specified only on the master switch when the stack is configured. For the specifiable range of values, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

The command is executed on the local device.

<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.

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command <switch no.> erase license <serial no.>
```

Example

Figure 15-1: 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

Response messages

Table 15-5: List of response messages for the erase license command

Message	Description
Can't erase software license.	The command cannot delete the software license.
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Invalid serial number <serial no.>	The optional license of the specified serial number does not exist. <serial no.>: Serial number
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

The deleted license key is no longer valid when the device is restarted.

16 Power Saving Functions

show power-control schedule

Displays the current status of the power-saving schedule and the dates and times the power-saving schedule has been enabled.

Syntax

```
show power-control schedule [<yymmdd>] [count <count>]
```

Input mode

User mode and administrator mode

Parameters

<yymmdd>

> The scheduled date and time is displayed from midnight of the day specified here. The specifiable range of values is from January 1, 2000 to January 17, 2038.

> yy

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

>> For example, 00 means the year 2000.

> mm

>> Specify the month in the range from 01 to 12.

> dd

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

> Behavior when this parameter is omitted:

> The scheduled date and time from the time of command execution is displayed.

count <count>

> Scheduled dates and times equivalent to the number of specified schedules are displayed. The specifiable range of schedules is from 1 to 50.

> Behavior when this parameter is omitted:

>> The scheduled dates and times for 10 schedules are displayed.

Behavior when all parameters are omitted:

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

Operation when a stack configuration is used

This command is not supported.

Example

Displays the current status of the power-saving schedule and the dates and times the power-saving schedule has been enabled.

Figure 16-1: Result of executing the show power-control schedule command

```
> show power-control schedule XX0401 count 5
Date 20XX/04/01(Thu) 18:36:57 UTC
Current Schedule Status : Disable
Schedule Power Control Date:
```

```
 20XX/04/01(Thu) 20:00 UTC  -  20XX/04/02(Fri) 06:00 UTC
 20XX/04/02(Fri) 20:00 UTC  -  20XX/04/05(Mon) 06:00 UTC
 20XX/04/05(Mon) 20:00 UTC  -  20XX/04/06(Tue) 06:00 UTC
 20XX/04/06(Tue) 20:00 UTC  -  20XX/04/07(Wed) 06:00 UTC
 20XX/04/07(Wed) 20:00 UTC  -  20XX/04/08(Thu) 06:00 UTC
>
```

Display items

Table 16-1: Information displayed by the show power-control schedule command

Item	Displayed information	Displayed detailed information
Current Schedule Status	Power-saving schedule status	Enable: Power saving is in effect as scheduled. Enable (force disabled): Although it is in the scheduled time range for saving power now, the scheduled power saving is disabled. Disable: Normal power control is in effect. Disable (force disabled): Although it is in the normal time range now, the scheduled power saving has been disabled. (The power saving is disabled even though it is in the scheduled time range.)
Schedule Power Control Date	Date and time that the power-saving schedule will be enabled.	Date and time that the power-saving schedule will be enabled. <date and time power-saving schedule started> - <date and time power-saving schedule ended>

Impact on communication

None

Response messages

Table 16-2: List of response messages for the show power-control schedule command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

Notes

None

show power

Shows the maximum power consumption information of the device.

Syntax

```
show power
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show power
```

Example

Figure 16-2: Result of executing the show power command

```
>show power
Date 20XX/09/21 12:00:00 UTC
H/W        Maximum Wattage
Chassis          130.00 W
>
```

Display items

Table 16-3: 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

Response messages

Table 16-4: List of response messages for the show power command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

- The power consumption information displayed by this command is equal to the result value of the command execution.

clear power

Clears the information about the power consumption of the device.

Syntax

```
clear power
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} clear power
```

Example

Figure 16-3: Result of executing the clear power command

```
> clear power
>
```

Display items

None

Impact on communication

None

Response messages

Table 16-5: List of response messages for the clear power command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

Even if you use this command to clear the information about the power consumption, the value of the MIB information obtained by using SNMP is not cleared to zero.

set power-control schedule

Specifies whether or not to apply a power-saving schedule in a scheduled time range of the power-saving schedule. The setting of this command is valid until the time range moves from the scheduled one to the normal. Note that if this command is executed during the normal time range, the setting will be enabled in the next scheduled time range.

Syntax

```
set power-control schedule {enable | disable}
```

Input mode

User mode and administrator mode

Parameters

{enable | disable}

    enable

        Enables power-saving schedules.

    disable

        Disables power-saving schedules. If this command is set during the normal time range, the schedule-disabled mode takes effect in the next scheduled time range.

Operation when a stack configuration is used

This command is not supported.

Example

Disables power-saving schedules.

Figure 16-4: Result of executing the set power-control schedule command

```
> set power-control schedule disable
>
```

Display items

None

Impact on communication

None

Response messages

Table 16-6: List of response messages for the set power-control schedule command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

Notes

None

17 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 [switch <switch no.>] [<kind>] [<command classification>] [count <count>]
```

Input mode

User mode and administrator mode

Parameters

switch <switch no.>

> Executes the command on the member switch whose switch number is specified.

> This parameter can be specified only on the master switch when the stack is configured. For the specifiable range of values, see "Specifiable values for parameters".

> Behavior when this parameter is omitted:

> > The command is executed on the local device.

<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.

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show logging [<kind>] [<command classification>] [count <count>]
```

Example

- Display the operation log entries for the device.

```
> show logging
```

Figure 17-1: Displaying operation logs

```
> show logging
Date 20XX/12/25 14:14:18 UTC
System Information
    AX3660S-48T4XW, OS-L3M Ver. 12.0 (Build:xx)
Logging Information
KEY 12/24 12:37:30 user1:ping 192.111.214.10
    :
    :
    :
>
```

- Display the reference log entries for the device.

```
> show logging reference
```

Figure 17-2: Displaying reference logs

```
> show logging reference
Date 20XX/12/25 14:14:18 UTC
System Information
    AX3660S-48T4XW, OS-L3M Ver. 12.0 (Build:xx)
Logging Information
E3 SOFTWARE 01900250 1001:000000000000
12/23 14:12:10    12/23 14:12:10    1
    :
    :
    :
>
```

Display items

None

Impact on communication

None

Response messages

Table 17-1: List of response messages for the show logging command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
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. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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 [switch <switch no.>] [<kind>]
```

Input mode

User mode and administrator mode

Parameters

switch <switch no.>

Executes the command on the member switch whose switch number is specified.

This parameter can be specified only on the master switch when the stack is configured. For the specifiable range of values, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

The command is executed on the local device.

<kind>

reference

Specifies the reference log.

Behavior when this parameter is omitted:

Specifies the operation log.

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} clear logging [<kind>]
```

Example

Figure 17-3: Erasing operation logs

```
> clear logging
```

Figure 17-4: Erasing reference logs

```
> clear logging reference
```

Display items

None

Impact on communication

None

Response messages

Table 17-2: List of response messages for the clear logging command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
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. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show logging console
```

Example

Figure 17-5: Enabling the display of operation messages on the screen
```
> show logging console
  System message mode : Display all
```

Figure 17-6: Suppressing the display of operation messages at event level E6 or lower
```
> show logging console
  System message mode : E6
```

Display items

None

Impact on communication

None

Response messages

Table 17-3: List of response messages for the show logging console command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration.

Message	Description
	\<switch no.\>: Switch number

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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all}
set logging console { disable <event level> | enable }
```

Example

Figure 17-7: Enabling operation messages to be displayed on the screen

```
> set logging console enable
```

Figure 17-8: Suppressing the display of operation messages at event level E5 or lower

```
> set logging console disable E5
```

Display items

None

Impact on communication

None

Response messages

Table 17-4: List of response messages for the set logging console command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

None

18 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 18-1: Informed request information
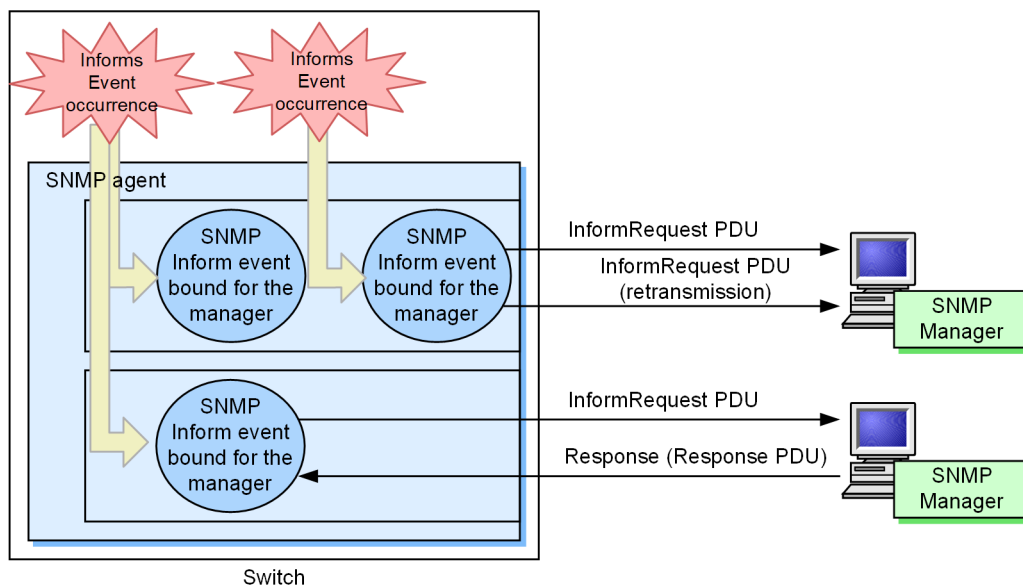
Syntax

```
show snmp
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

Example

Figure 18-2: 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 : 53
    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            : 49
    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           retries:26
        response:2          pending:1          failed:5          dropped:0
    Host: 192.168.0.4
        sent   :3           retries:15
        response:0          pending:0          failed:3          dropped:0
    Host: 2001:db8::10
        sent   :1           retries:0
        response:1          pending:0          failed:0          dropped:0
```

Display items

Table 18-1: 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).	—

Item	Meaning	Displayed detailed information
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
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 no-Error.	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).	—

Item	Meaning	Displayed detailed information
Bad values errors	Indicates the snmpOutBadValues value (total number of sent PDUs whose error status is bad-Value).	—
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
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
VRF [SL-L3A]	Indicates the VRF ID.	Value set by the vrf 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 inform events that are held and the maximum number of inform events that can be held. If the SNMP manager does not respond, an inform event is held.	<current>: Number of inform events 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
VRF [SL-L3A]	Indicates the VRF ID.	Value set by the vrf parameter of the "snmp-server host" configuration command
sent	Indicates the number of inform events bound for the SNMP manager that sent InformRequest PDUs.	0 to 4294967295
retries	Indicates the number of resent InformRequest PDUs.	0 to 4294967295

Item	Meaning	Displayed detailed information
response	Indicates the number of responses from the SNMP manager to inform events bound for the SNMP manager.	0 to 4294967295
pending	Indicates the number of inform events bound for the SNMP manager that is waiting for a response from another SNMP manager.	0 to 21000
failed	Indicates the number of times sending of an inform event 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 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

Impact on communication

None

Response messages

Table 18-2: List of response messages for the show snmp command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to SNMP program.	Communication with the SNMP program failed. Re-execute the command.

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

Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

Example

Figure 18-3: 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 18-3: 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
VRF [SL-L3A]	VRF ID of the SNMP manager	Value set by the vrf <vrf id> 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

Response messages

Table 18-4: List of response messages for the show snmp pending command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to SNMP program.	Communication with the SNMP program failed. Re-execute the command.
no entries.	There are no inform events bound for the SNMP manager.

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.

Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

Example

Figure 18-4: 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

Response messages

Table 18-5: List of response messages for the snmp lookup command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
No match found for <MIB object name>	The applicable <MIB object name> cannot be found by using this command.

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.

Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

Example

Figure 18-5: Example of executing the snmp get command

```
> snmp get sysDescr.0

Name: sysDescr.0
Value: ALAXALA AX3660S AX-3660-48T4XW [AX3660S-48T4XW] Switching software Ver. 12.0 [OS-L3M]
> snmp get 1.3.6.1.2.1.1.1.0

Name: sysDescr.0
Value: ALAXALA AX3660S AX-3660-48T4XW [AX3660S-48T4XW] Switching software Ver. 12.0 [OS-L3M]
```

Display items

Table 18-6: 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

Response messages

Table 18-7: List of response messages for the snmp get command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot translate variable class: <MIB Object Name>	The object name <MIB Object Name> is invalid.
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 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.
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.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

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.

Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

Example

Figure 18-6: 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 18-8: 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

Response messages

Table 18-9: List of response messages for the snmp getnext command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot translate variable class: <MIB Object Name>	The object name <MIB Object Name> is invalid.
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 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.
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.

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.

Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

Example

Figure 18-7: 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.10
Value: MGMT0

Name: ifDescr.100
Value: GigabitEther 1/0/1
```

Display items

Table 18-10: 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

Response messages

Table 18-11: List of response messages for the snmp walk command

Message	Description
\<SNMP agent IP address\>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot translate variable class: \<MIB Object Name\>	The object name \<MIB Object Name\> is invalid.
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 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.
receive error.	A receive error occurred.

Message	Description
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.

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 getif

Searches management information of the interfaces group and then displays the MIB information.

Syntax

```
snmp getif
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

Example

Figure 18-8: Example of executing the snmp getif command

```
> snmp getif
    # Type       PhysAddr       Adm Opr    InOctets  OutOctets   InPkts   OutPkts
    1 loopback 0000.0000.0000 up  up        18426      18575      290       292
    3 l2vlan   0012.e23e.b0bf up  up            0          0        0         0
   10 Ethernet 0012.e23e.b0bf up  up        24591       3417      377        52
  100 Ethernet 0012.e23e.b0c1 up  dwn         601        854        6         7
```

Display items

Table 18-12: Information displayed when the snmp getif command is executed

Item	Meaning	Displayed detailed information
#	Indicates the ifIndex number.	—
Type	Indicates the interface type (ifType).	other (A type other than the following types)
		Ethernet
		loopback (local loopback)
		l2vlan
		LA
PhysAddr	Indicates the physical address of an interface (ifPhysAddress).	—
Adm	Indicates the interface status of the configuration (ifAdminStatus).	up (enabled)
		down (disabled)

Item	Meaning	Displayed detailed information
Opr	Indicates the current interface status (ifOperStatus).	up (enabled)
		down (disabled)
		test (being tested)
InOctets	Indicates the number of octets received on an interface (ifInOctets).	—
OutOctets	Indicates the number of octets sent from an interface (ifOutOctets).	—
InPkts	Indicates the number of packets received on an interface (ifInUcastPkts + ifInNUcastPkts).	—
OutPkts	Indicates the number of packets sent from an interface (ifOutUcastPkts + ifOutNUcastPkts).	—

Impact on communication

None

Response messages

Table 18-13: List of response messages for the snmp getif command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
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.
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.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

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 getroute

Shows the IP routing table (ipRouteTable).

Syntax

```
snmp getroute
```

Input mode

User mode and administrator mode

Parameters

None

Searches for ipRouteTable management information and displays routing information.

Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

Example

Figure 18-9: Example of executing the snmp getroute command

```
> snmp getroute
Index  Destination     NextHop         Metric1   Type      Proto        Age
    0  127.0.0.0       0.0.0.0               0   other     local       4940
    1  127.0.0.1       127.0.0.1             0   direct    local       4942
  100  10.1.1.0        10.1.1.1              0   direct    local        720
  100  10.1.1.1        10.1.1.1              0   direct    local        720
>
```

Display items

Table 18-14: Information displayed when the snmp getroute command is executed

Item	Meaning	Displayed detailed information
Index	Indicates the interface number of the interface used to reach the next hop on this route (ipRouteIfIndex).	—
Destination	Indicates the destination IP address on this route (ipRouteDest).	—
NextHop	Indicates the IP address of the next hop for the destination of this route (ipRouteNextHop).	—
Metric1	Indicates the primary routing metric for this route (ipRouteMetric1).	—
Type	Indicate the type of this route (ipRouteType).	direct (direct route)
		indirect (indirect route)
		invalid (invalid route)
		other (others)

Item	Meaning	Displayed detailed information
Proto	Indicates the routing protocol (ipRouteProto).	rip (RIP)
		ospf (OSPF)
		bgp (bgp)
		local (static routing)
		netmgmt (static routing)
		other (others)
Age	Indicates the number of seconds elapsed after this route was last updated or confirmed (ipRouteAge).	—

Impact on communication

None

Response messages

Table 18-15: List of response messages for the snmp getroute command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
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.
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.
No routing information available.	There were no routing table entries.

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.

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 the ipRouteTable MIB information , and a timeout might occur. If that happens, use the "snmp getnext" command to acquire the ipRouteTable information.

3. If the "snmp-server community" configuration command is not set, the No response message appears and the MIB cannot be acquired.

snmp getarp

Shows the IP address translation table (ipNetToMediaTable).

Syntax

```
snmp getarp
```

Input mode

User mode and administrator mode

Parameters

None

Searches for ipNetToMediaTable management information and displays ARP information.

Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

Example

Figure 18-10: Example of executing the snmp getarp command

```
> snmp getarp
 Index     Network Address     Physical Address    Type
    4      12.1.1.99           0012.e2c0.d162   static
>
```

Display items

Table 18-16: Information displayed when the snmp getarp command is executed

Item	Meaning	Displayed detailed information
Index	Indicates the interface number of the interface that has this ARP information (ipNetToMediaIfIndex).	—
Network Address	Indicates the IP address corresponding to the physical address (ipNetToMediaNetAddress).	—
Physical Address	Indicates the physical address (ipNetToMediaPhysAddress).	—
Type	Indicates the type of mapping (ipNetToMediaType).	other (mapping other than the following types)
		invalid (invalid mapping)
		dynamic (dynamic mapping)
		static (static mapping)

Impact on communication

None

Response messages

Table 18-17: List of response messages for the snmp getarp command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
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.
No ARP information available.	There were no ARP table entries.
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.
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.

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 the ipNetToMediaTable MIB information, and a timeout might occur. If that happens, use the "snmp getnext" command to acquire the ipNetToMediaTable information.

3. If the "snmp-server community" configuration command is not set, the No response message appears and the MIB cannot be acquired.

snmp getforward

Displays ipForwardTable and axsVrfIpForwardTable (IP forwarding tables).

Syntax

```
snmp getforward
```

Input mode

User mode and administrator mode

Parameters

None

> Searches for ipForwardTable and axsVrfIpForwardTable management information and displays forwarding information.

Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

Example

Figure 18-11: Example of executing the snmp getforward command

```
> snmp getforward
Index  Destination      NextHop         Metric1 Type    Proto    Age NH-AS
 2202  0.0.0.0/0        192.168.0.1           0 remote  netmgmt  855 0
    0  127.0.0.0/8      0.0.0.0               0 other   local    974 0
    1  127.0.0.1/32     127.0.0.1             0 local   local    974 0
 2202  192.168.0.0/24   192.168.0.34          0 local   local    855 0
 2202  192.168.0.34/32  192.168.0.34          0 local   local    855 0

VRF 3
Index  Destination      NextHop         Metric1 Type    Proto    Age NH-AS
 2210  10.10.10.0/24    10.10.10.1            0 local   local    855 0

VRF 4
Index  Destination      NextHop         Metric1 Type    Proto    Age NH-AS
 2211  20.1.1.0/24      20.1.1.1              0 local   local    855 0
 2212  20.20.20.0/24    20.20.20.1            0 local   local    855 0
```

Display items

Table 18-18: Information displayed when the snmp getforward command is executed

Item	Meaning	Displayed detailed information
Index	Indicates the identifier of the local interface connected to the next hop on this route (ipForwardIfIndex).	—
Destination	Indicates the destination address of this route (ipForwardDest) and the mask for logical conjunction with the destination (ipForwardMask) displayed in mask length.	—
NextHop	Indicates the address of the next system on the route (ipForwardNextHop).	—
Metric1	Indicates the metric for this route (ipForwardMetric1).	—

Item	Meaning	Displayed detailed information
Type	Indicates the type of the route (ipForwardType).	local (local)
		remote (remote)
		invalid (invalid)
		other (others)
Proto	Indicates the protocol that learned this route (ipForwardProto).	rip (RIP)
		ospf (OSPF)
		bgp (BGP)
		local (static routing)
		netmgmt (static routing)
		other (others)
Age	Indicates the time (in seconds) elapsed since this route was learned or updated (ipForwardAge).	—
NH-AS	Indicates the autonomous system number of the next hop (ipForwardNextHopAS).	—

Table 18-19: Information displayed when the snmp getforward command is executed (VRF unit) [SL-L3A]

Item	Meaning	Displayed detailed information
VRF	Indicates the VRF index (axsVrfIpFwVRFIndex).	—
Index	Indicates the identifier of the local interface connected to the next hop on this route (axsVrfIpFwIfIndex).	—
Destination	Indicates the destination address of this route (axsVrfIpFwDest) and the mask for ANDing with the destination (axsVrfIpFwMask), displayed as a mask length.	—
NextHop	Indicates the address of the next system on this route (axsVrfIpFwNextHop).	—
Metric1	Indicates the metric for this route (axsVrfIpFwMetric1).	—
Type	Indicates the type of the route (axsVrfIpFwType).	local (local)
		remote (remote)
		invalid (invalid)
		other (others)
Proto	Indicates the protocol that learned this route (axsVrfIpFwProto).	rip (RIP)
		ospf (OSPF)

Item	Meaning	Displayed detailed information
		bgp (BGP)
		local (static routing)
		netmgmt (static routing)
		other (others)
Age	Indicates the time (in seconds) elapsed since this route was learned or updated (axsVrfIpFwAge).	—
NH-AS	Indicates the autonomous system number of the next hop (axsVrfIpFwNextHopAS).	—

Impact on communication

None

Response messages

Table 18-20: List of response messages for the snmp getforward command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
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.
No forwarding information available.	There were no forwarding table entries.
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
No VRF forwarding information available.	There were no VRF forwarding table entries.
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.

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 the ipForwardTable MIB information, and a timeout might occur. If that happens, use the "snmp getnext" command to acquire the ipForwardTable 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.

Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

Example

Figure 18-12: Example of executing the snmp rget command

```
> snmp rget version 2 192.168.11.35 public sysObjectID.0

Name: sysObjectID.0
Value: ax3660s
```

Display items

Table 18-21: 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

Response messages

Table 18-22: List of response messages for the snmp rget command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot translate variable class: <MIB Object Name>	The object name <MIB Object Name> is invalid.
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 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.
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.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

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.

Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

Example

Figure 18-13: 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 18-23: 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

Response messages

Table 18-24: List of response messages for the snmp rgetnext command

Message	Description
\<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot translate variable class: \<MIB Object Name>	The object name \<MIB Object Name> is invalid.
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 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.
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.

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.

Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

Example

Figure 18-14: 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 18-25: 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

Response messages

Table 18-26: List of response messages for the snmp rwalk command

Message	Description
\<SNMP agent IP address\>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot translate variable class: \<MIB Object Name\>	The object name \<MIB Object Name\> is invalid.
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 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.
receive error.	A receive error occurred.

Message	Description
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.

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 rgetroute

Shows the IP routing table (ipRouteTable) of the specified remote device.

Syntax

```
snmp rgetroute <ip address> <community>
```

Input mode

User mode and administrator mode

Parameters

This command remotely accesses an SNMP agent and displays routing information from the ipRouteTable management information.

<ip address>

Specifies the IP address of the device which is remotely accessed.

<community>

Specifies the community name of the remote device.

Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

Example

Figure 18-15: Example of executing the snmp rgetroute command

```
> snmp rgetroute  20.1.30.101  public
No response - retrying...
          - retrying...
          - try again.

> snmp rgetroute 20.1.30.101 public
Index    Destination      NextHop      Metric1 Type     Proto        Age
    2    20.0.0.0         20.1.1.1           0 direct   local        180
    2    20.1.1.0         20.1.1.1           0 direct   local        720
```

Display items

Table 18-27: Information displayed when the snmp rgetroute command is executed

Item	Meaning	Displayed detailed information
Index	Indicates the interface number of the interface used to reach the next hop on this route (ipRouteIfIndex).	—
Destination	Indicates the destination IP address on this route (ipRouteDest).	—
NextHop	Indicates the IP address of the next hop for the destination of this route (ipRouteNextHop).	—
Metric1	Indicates the primary routing metric for this route (ipRouteMetric1).	—

Item	Meaning	Displayed detailed information
Type	Indicate the type of this route (ipRouteType).	direct (direct route)
		indirect (indirect route)
		invalid (invalid route)
		other (others)
Proto	Indicates the routing protocol (ipRouteProto).	rip (RIP)
		ospf (OSPF)
		bgp (bgp)
		local (static routing)
		netmgmt (static routing)
		other (others)
Age	Indicates the number of seconds elapsed after this route was last updated or confirmed (ipRouteAge).	—

Impact on communication

None

Response messages

Table 18-28: List of response messages for the snmp rgetroute command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
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.

Message	Description
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.
No routing information available.	There were no routing table entries.
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.

Notes

1. If there are too many interfaces on the target device, it takes time to search for the ipRouteTable MIB information, and a timeout might occur. If that happens, use the "snmp rgetnext" command to acquire the ipRouteTable information.

snmp rgetarp

Shows the IP address translation table (ipNetToMediaTable) of the specified remote device.

Syntax

```
snmp rgetarp <ip address> <community>
```

Input mode

User mode and administrator mode

Parameters

This command remotely accesses an SNMP agent and displays ARP information from the ipNetToMediaTable management information.

<ip address>

Specifies the IP address of the device which is remotely accessed.

<community>

Specifies the community name of the remote device.

Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

Example

Figure 18-16: Example of executing the snmp rgetarp command

```
> snmp rgetarp  20.1.30.101  public
Index    Network Address    Physical Address    Type
    4    12.1.1.99          0012.e258.8860      static
    1    112.1.1.99         0012.e258.8870      static
```

Display items

Table 18-29: Information displayed when the snmp rgetarp command is executed

Item	Meaning	Displayed detailed information
Index	Indicates the interface number of the interface that has this ARP information (ipNetToMediaIfIndex).	—
Network Address	Indicates the IP address corresponding to the physical address (ipNetToMediaNetAddress).	—
Physical Address	Indicates the physical address (ipNetToMediaPhysAddress).	—
Type	Indicates the type of mapping (ipNetToMediaType).	other (mapping other than the following types)
		invalid (invalid mapping)
		dynamic (dynamic mapping)

Item	Meaning	Displayed detailed information
		static (static mapping)

Impact on communication

None

Response messages

Table 18-30: List of response messages for the snmp rgetarp command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
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.
No ARP information available.	There were no ARP table entries.
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.
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.

Notes

If there are too many interfaces on the target device, it takes time to search for the ipNetToMediaTable MIB

information, and a timeout might occur. If that happens, use the "snmp rgetnext" command to acquire the ipNetToMediaTable information.

19 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.

Operation when a stack configuration is used

The command can be executed only on the master switch.

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.

Response messages

Table 19-1: List of response messages for the python command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
The command cannot be executed because you are in user mode.	This command cannot be executed in user mode.
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.

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.

Operation when a stack configuration is used

The command can be executed only on the master switch.

Example

Figure 19-1: 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

Response messages

Table 19-2: List of response messages for the stop python command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
The command cannot be executed because you are in user mode.	This command cannot be executed in user mode.
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

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".

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} pyflakes <file name>
```

Example

Figure 19-2: Checking the syntax of a script file (sample.py) created according to the Python version 3 syntax

```
> pyflakes ./sample.py
>
```

Figure 19-3: 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

Response messages

Table 19-3: List of response messages for the pyflakes command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
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. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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. In a stack configuration, the file is synchronized with the one in the same directory on the backup switch.

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> | sync | diff}
```

Input mode

Administrator mode

Parameters

{<file name> | sync | diff}

Specifies a script file, or specifies an operation targeted for script files.

<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.

sync

Synchronizes all installed script files with those on other member switches as the files on the master switch are the originals. Script files that are not installed in the master switch are deleted from other member switches. If the contents of two files do not match, they are overwritten by the contents of the file on the master switch.

diff

Compares the number of installed script files and the contents of the script files installed in the master switch and other member switches, and then displays whether there are any differences between them. Nothing is displayed if there is no member switch to be compared or if everything matches.

Operation when a stack configuration is used

The script files installed in the master switch are automatically synchronized to those in the other member switches. The sync and diff parameters are available.

Example

Figure 19-4: Installing a script file (testscript.py) in the current directory in the Switch

```
# install script testscript.py
#
```

Figure 19-5: Synchronizing installed script files

```
# install script sync
Do you want to synchronize all script files? (y/n): y
#
```

Figure 19-6: Checking differences between script files

```
# install script diff
Some script files differ.
#
```

Display items

None

Impact on communication

None

Response messages

Table 19-4: List of response messages for the install script command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Permission denied. (file name = <file name>)	No read permission for the specified script file exists. <file name>: Script file name
Some script files differ.	There are some differences between installed script files. Execute the "install script sync" command to synchronize them.
The command cannot be executed because stack is not active.	The command cannot be executed because a stack is not configured.
The command cannot be executed because the software versions do not match.	The command cannot be executed due to software version mismatch.
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 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.

Message	Description
The specified script file does not exist. (file name = <file name>)	The specified script file does not exist. <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.

Notes

1. An already installed script file cannot be overwritten. If you want to change the script file, delete and then reinstall it.

2. When a stack is configured, synchronization of script files might take a long time.

3. If the version of the software in the master switch does not match that of the software in other member switches in a stack configuration, the command with the sync or diff parameter specified cannot be executed.

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.

Operation when a stack configuration is used

The script files deleted from the master switch are synchronously and automatically deleted from the other member switches.

Example

Figure 19-7: 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

Response messages

Table 19-5: List of response messages for the uninstall script command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
The command cannot be executed because you are in user mode.	This command cannot be executed in user mode.
The specified script file is not installed. (file name = <file name>)	The specified script file is not installed. <file name>: Script file name

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} show script installed-file [<file name>]
```

Example

Figure 19-8: 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 19-9: 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 19-6: 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
name		File name
size		File size
MD5		MD5 hash value

Impact on communication

None

Response messages

Table 19-7: List of response messages for the show script installed-file command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
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. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number
The specified script file is not installed. (file name = <file name>)	The specified script file is not installed. <file name>: Script file name

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

Operation when a stack configuration is used

The command can display information only for the master switch.

Example

Figure 19-10: 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 19-8: 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.	

Item	Displayed information	Displayed detailed information
command line args	Command-line argument	Command-line arguments specified when the applicable script is started
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

Response messages

Table 19-9: List of response messages for the show script running-state command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} show event manager history {applet | script}
```

Example 1

Figure 19-11: 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 19-10: 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	—

Item	Displayed information	Displayed detailed information
type	Event type	timer: Timer monitoring sysmsg: Operation message monitoring

Example 2

Figure 19-12: 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 19-11: 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

Response messages

Table 19-12: List of response messages for the show event manager history command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

None

show event manager monitor

Shows monitoring event information.

Syntax

```
show event manager monitor {applet [name <applet name>] | script [pid <pid>]} [type {timer | sy
smsg}] [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.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example

Figure 19-13: 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 19-14: Displaying the information of monitoring events registered using the applet whose applet name is monitor2

```
> show event manager monitor applet name monitor2
Date 20XX/10/25 12:15:15 UTC
applet name                   type         start time                 detection
----------------------------- ------------ -------------------------- ----------
monitor2                      sysmsg       20XX/10/24 12:04:08 UTC             1
>
```

Figure 19-15: 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 19-16: 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 19-17: Display the information of monitoring events registered using the script with its process ID of 12345

```
> show event manager monitor script pid 12345
Date 20XX/10/25 12:25:10 UTC
1 event(sysmsg:1)
  PID name                event ID type         start time                 detection
----- ------------------- ---------- ------------ -------------------------- ----------
12345 test2.py            33554433 sysmsg       20XX/10/24 15:10:01 UTC             1
>
```

Figure 19-18: Displaying the information of monitoring events of operation messages, registered using scripts

```
> show event manager monitor script type sysmsg
Date 20XX/10/25 12:25:10 UTC
2 event
  PID name                  event ID type      start time                 detection
----- ------------------- ---------- ----------- -------------------------- ----------
 2543 test1.py                33554432 sysmsg      20XX/10/24 13:12:56 UTC             0
12345 test2.py                33554433 sysmsg      20XX/10/24 15:10:01 UTC             1
>
```

Figure 19-19: 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 19-13: 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	—

Item	Displayed information	Displayed detailed information
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 19-14: 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	—
	switch status	Switch status	Master: Operation messages from the master switch are monitored. Backup: Operation messages from the backup switch are monitored.

Event type	Item	Displayed information	Displayed detailed information
	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

Response messages

Table 19-15: List of response messages for the show event manager monitor command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
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.

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} clear event manager [{applet | script}] [{statistics | history}]
```

Example

Figure 19-20: Clearing the statistics held by the event management program

```
> clear event manager statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 19-16: List of response messages for the clear event manager command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
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. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} restart script-manager [-f] [core-file]
```

Example

Figure 19-21: 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

Response messages

Table 19-17: List of response messages for the restart script-manager command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
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. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

1. If the core 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/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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} restart event-manager [-f] [core-file]
```

Example

Figure 19-22: 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

Response messages

Table 19-18: List of response messages for the restart event-manager command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
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. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

1. If the core 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/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

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} dump script-user-program
```

Example

Figure 19-23: Outputting standard errors output by resident and event startup scripts to a file

```
> dump script-user-program
>
```

Display items

None

Impact on communication

None

Response messages

Table 19-19: List of response messages for the dump script-user-program command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
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. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number

Message	Description
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} dump script-manager
```

Example

Figure 19-24: Outputting control information of the script management program to a file

```
> dump script-manager
>
```

Display items

None

Impact on communication

None

Response messages

Table 19-20: List of response messages for the dump script-manager command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
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. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number

Message	Description
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} dump event-manager
```

Example

Figure 19-25: Outputting the control information of the event management program to a file

```
> dump event-manager
>
```

Display items

None

Impact on communication

None

Response messages

Table 19-21: List of response messages for the dump event-manager command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
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. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number

Message	Description
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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

20 Python Extended 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 20-1: 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 20-2: 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 20-3: 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 20-4: 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 20-5: 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 20-6: 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,
               switch_status = 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. The specifiable values are from 1 to 2.

The default value of this argument is eventmonitor.DEFAULT. If eventmonitor.DEFAULT is specified, all switch numbers are monitored.

switch_status

Specifies the switch status of operation messages to be monitored:

- eventmonitor.M: Standalone or master
- eventmonitor.B: Backup

The default value of this argument is eventmonitor.DEFAULT. If eventmonitor.DEFAULT is specified, all switch statuses 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 20-7: 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, switch_status, 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:yyyyyyyyyyy ttt...ttt
 1               2 3 4   5         6               7        8    9            10
```

   1. message_type
   2. switch_no
   3. switch_status

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 20-8: 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 20-9: 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 20-10: 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 20-11: 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 20-13: Data structure of the variable-length section in a trigger operation message".

Exception

Table 20-12: 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 20-13: 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_STA-TUS	Switch status • eventmonitor.I: Initial status • eventmonitor.M: Standalone or master • eventmonitor.B: Backup

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_FUNC-TION	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 20-15: Detailed applet information".

Exception

Table 20-14: 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 20-15: 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 20-16: Detailed monitoring condition information (timer monitoring)".
	For operation message monitoring:
	   See "Table 20-17: 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 20-18: Event cause information (operation message monitoring)".

Table 20-16: 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 20-17: 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.I: Initial status • eventmonitor.M: Standalone or master • eventmonitor.B: Backup If this value of tuple type is not specified as a monitoring condition, eventmonitor.DEFAULT is stored.

Tuple type (access value)	Description
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.
eventmonitor.SYSMSG_MSG_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_MSG_TYPE_DET	Detailed message type information 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 20-18: 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_SWITCH_STATUS	Switch status • eventmonitor.M: Standalone or master • eventmonitor.B: Backup
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.

Tuple type (access value)	Description
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.SYSMSG_TIME	Output time of the operation message "<month>/<day> <hour>:<minute>:<second>"

21 Ethernet

show interfaces

Shows Ethernet information.

Syntax

```
show interfaces {gigabitethernet | tengigabitethernet | fortygigabitethernet | hundredgigabitet
hernet} <switch no.>/<nif no.>/<port no.> [detail]
```

Input mode

User mode and administrator mode

Parameters

{gigabitethernet | tengigabitethernet | fortygigabitethernet | hundredgigabitethernet}

> gigabitethernet

>> Specifies an Ethernet interface with the maximum line speed of 1 Gbit/s.

> tengigabitethernet

>> Specifies an Ethernet interface with the maximum line speed of 10 Gbit/s.

> fortygigabitethernet

>> Specifies an Ethernet interface with the maximum line speed of 40 Gbit/s.

> hundredgigabitethernet

>> Specifies an Ethernet interface with the maximum line speed of 100 Gbit/s.

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

> Specifies the switch number, NIF number, and port number. For the specifiable range of values, see "Specifiable values for parameters".

detail

> Specifies that detailed statistics be displayed.

> Behavior when this parameter is omitted:

>> Detailed information is not displayed.

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command <switch no.> show interfaces {gigabitethernet | tengigabitethernet | fortygigabi
tethernet | hundredgigabitethernet} <switch no.>/<nif no.>/<port no.> [detail]
```

Example

The following figure shows an example of executing the command with the 10BASE-T/100BASE-TX/1000BASE-T port specified.

Figure 21-1: 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
        TPID:8100
        Frame size:1518 Octets  retry:0  Interface name:geth1/0/1
        description:test lab area network
        MAC address movement detect:0
        <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
        Single collision    :       0 Excessive deferral  :        0
        Multiple collisions :       0 Excessive collisions :       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 Error frames        :        0
        <Line fault counter>
        Polarity changed    :       0 MDI cross over changed :     0
        Link down           :       0
        Link down in operational state               :        0
        In limit over                                :        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 21-2: 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
        TPID:8100
        Frame size:1518 Octets  retry:0  Interface name:geth1/0/1
        description:test lab area network
        MAC address movement detect:0
        <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
        64 packets          :       1 64 packets          :       13
        65-127 packets      :     271 65-127 packets      :      271
        128-255 packets     :       0 128-255 packets     :        1
        256-511 packets     :       0 256-511 packets     :        1
        512-1023 packets    :       0 512-1023 packets    :        0
        1024-1518 packets   :       0 1024-1518 packets   :        0
                                      :
                                      :
>
```

The following figure shows an example of executing the command with an SFP+/SFP shared port that enabled SFP+ specified.

Figure 21-3: Example of executing the command (on an SFP+/SFP shared port with SFP+
enabled)

```
> show interfaces tengigabitethernet 1/0/25
Date 20XX/01/14 12:41:55 UTC
NIF0: -
Port25: 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:1518 Octets  retry:0  Interface name:tengeth1/0/25
        MAC address movement detect:0
        <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
        <In line error counter>
        CRC errors                                :               0
        Fragments                                 :               0
        Jabber                                    :               0
        Symbol errors                             :               0
        Short frames                              :               0
        Long frames                               :               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
        In limit over                                    :         0
>
```

Display items

Table 21-1: 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).

Item	Displayed information	
	Detailed information	**Meaning**
	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. • The port has been deactivated by port resetting of GSRP. • 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 the move monitoring function for MAC address learning. • The port has been deactivated by port resetting of uplink redundancy.
	disable	Operation was stopped by using the "shut-down" or "schedule-power-control shut-down" configuration command.
<line type>	See "Table 21-2: List of line types".	
<MAC address>	MAC address of the applicable port	
<type of transceiver>	SFP	SFP or SFP-T
	SFP+	SFP+
	QSFP+	QSFP+
	QSFP28	QSFP28
	—	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 21-2: List of line types

Displayed item[#]	Displayed information
10BASE-T full	10BASE-T full duplex
100BASE-TX full	100BASE-TX full duplex
1000BASE-T full	1000BASE-T full duplex
10GBASE-T full	10GBASE-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
1000BASE-BX40-U full	1000BASE-BX-U (40km) full duplex
1000BASE-LHB full	1000BASE-LHB full duplex
10GBASE-SR	10GBASE-SR
10GBASE-LR	10GBASE-LR
10GBASE-ER	10GBASE-ER
10GBASE-ZR	10GBASE-ZR
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)
40GBASE-SR4 full	40GBASE-SR4
40GBASE-LR4 full	40GBASE-LR4
40GBASE-CU35CM full	40GBASE-CR4 (35cm)
40GBASE-CU1M full	40GBASE-CR4 (1m)
40GBASE-CU3M full	40GBASE-CR4 (3m)
40GBASE-CU5M full	40GBASE-CR4 (5m)
100GBASE-SR4 full	100GBASE-SR4
100GBASE-CWDM4 full	100GBASE-CWDM4
100GBASE-LR4 full	100GBASE-LR4

Displayed item[#]	Displayed information
100GBASE-4WDM full	100GBASE-4WDM-40
100GBASE-CU35CM full	100GBASE-CR4 (35cm)
100GBASE-CU1M full	100GBASE-CR4 (1m)
(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 or abbreviation 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 21-3: 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.	
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.	

Item	Displayed information	
	Detailed information	**Meaning**
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.
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 starting from the MAC header and ending with the DATA and PAD fields. "-" is displayed for a stack port.	
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.	
MAC address movement detect	Number of times moves for MAC address learning were detected	

#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 21-4: List of statistical items

Item	Displayed information
\<Out octets/packets counter\>	Send statistics
\<In octets/packets counter\>	Receive statistics
Octets	The number of octets 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 (including error packets)
Unicast packets	Number of unicast packets
Multicast packets	Number of multicast packets
Broadcast packets	Number of broadcast packets
Pause packets	Number of pause packets
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.
1024-1518 packets	The number of packets whose frame length is from 1024 to 1518 octets.
\<Out line error counter\>	Send error statistics (This item is displayed only for 10BASE-T/100BASE-TX/1000BASE-T ports and 100BASE-TX/1000BASE-T/10GBASE-T ports.)
Late collision	The number of collisions detected after the 512-bit time has elapsed
Single collision	The number of transmissions that were successful after one collision
Multiple collisions	The number of transmissions that were successful after two or more collisions
Defer indication	The number of times the initial transmission was delayed because the transmit line was busy
Excessive deferral	The number of times an excessive delay occurred
Excessive collisions	The number of transfer failures due to excessive collisions (16 collisions)
Error frames	The total number of frames discarded due to errors (total value of the following items: Late collision, Excessive deferral, Excessive collisions)
\<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[#] (This item is displayed only for 10BASE-T/100BASE-TX/1000BASE-T ports and 100BASE-TX/1000BASE-T/10GBASE-T ports.)
Fragments	The number of times a short frame (whose length was shorter than 64 octets) was received and an FCS error or an Alignment error occurred[#]

Item	Displayed information
Jabber	The number of times a long frame (whose length exceeded the max frame length) was received and an FCS error or an Alignment error occurred Fixed value of 0 (This item is included in Long frames.)
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
Error frames	The total number of frames discarded due to errors (total value of the following items: Short frames, Fragments, CRC errors, Long frames, Symbol errors)
\<Line fault counter\>	Failure statistics (For 10BASE-T/100BASE-TX/1000BASE-T ports and 100BASE-TX/1000BASE-T/10GBASE-T ports)
Polarity changed	The number of times the polarity of the send or receive pin of a twisted pair cable was changed
MDI cross over changed	The number of times 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)
In limit over	The number of frames discarded due to exceeded receiving capacity
\<Line fault counter\>	Failure statistics (For SFP+/SFP shared ports, QSFP+ ports , and QSFP28/QSFP+ 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)
In limit over	The number of frames discarded due to exceeded receiving capacity

#: The Alignment and Fragments items show the same value.

Impact on communication

None

Response messages

Table 21-5: List of response messages for the show interfaces command

Message	Description
\<switch no.>/\<nif no.>/\<port no.> is not fortygigabitethernet.	The interface of the specified port is not fortygigabitethernet. 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 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 hundredgigabitethernet.	The interface of the specified port is not hundredgigabitethernet. 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
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- \<port no.>.	The port number is outside the valid range. Make sure the specified parameter is correct. \<port no.>: Port number
No such Switch \<switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. \<switch no.>: Switch number
Switch \<switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. \<switch no.>: Switch number

Notes

1. All display items are cleared when:

   - The device starts up.
   - The "restart vlan" command is executed.
   - A device hardware failure occurs.

- A failure occurs in the network interface management program (nimd).

2. In AX3660S-24T4X, AX3660S-24T4XW, and AX3660S-48T4XW, if the software license or optional license does not support 10G uplink, inserting an SFP + transceiver changes the transceiver status to not support.

3. In AX3660S-16S4XW and AX3660S-24X4QW, if the optional license does not support expanding the number of ports, inserting a transceiver into a port enabled by the optional license changes the transceiver status to not support.

4. If the stack function is disabled in a model that has a stack-dedicated port, the 40GBASE-R port is not displayed.

5. In AX3660S-48XT4QW, if the line speed of the QSFP28/QSFP+ shared port is not enabled at 100 Gbit/s with the "system interface hundredgigabitethernet" configuration command, inserting a QSFP28 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
- Number of times moves for MAC address learning were detected

Syntax

```
clear counters
clear counters {gigabitethernet | tengigabitethernet | fortygigabitethernet | hundredgigabiteth
ernet} <switch no.>/<nif no.>/<port no.>
```

Input mode

User mode and administrator mode

Parameters

{gigabitethernet | tengigabitethernet | fortygigabitethernet | hundredgigabitethernet}

    gigabitethernet

        Specifies an Ethernet interface with the maximum line speed of 1 Gbit/s.

    tengigabitethernet

        Specifies an Ethernet interface with the maximum line speed of 10 Gbit/s.

    fortygigabitethernet

        Specifies an Ethernet interface with the maximum line speed of 40 Gbit/s.

    hundredgigabitethernet

        Specifies an Ethernet interface with the maximum line speed of 100 Gbit/s.

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

    Specifies the switch number, NIF number, and port number. For the specifiable range of values, see "Specifiable values for parameters".

Behavior when all parameters are omitted:

    The statistics counters of all Ethernet interfaces are cleared to zero.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch. You can also execute the command with the switch number of the member switch specified.

You can also use the "remote command" command.

```
remote command all clear counters
remote command <switch no.> clear counters [{gigabitethernet | tengigabitethernet | fortygigabi
tethernet | hundredgigabitethernet} <switch no.>/<nif no.>/<port no.>]
```

Example and display items

None

Impact on communication

None

Response messages

Table 21-6: List of response messages for the clear counters (Ethernet) command

Message	Description
\<switch no.\>/\<nif no.\>/\<port no.\> is not fortygigabitethernet.	The interface of the specified port is not fortygigabitethernet. 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 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 hundredgigabitethernet.	The interface of the specified port is not hundredgigabitethernet. 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
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- \<port no.\>.	The port number is outside the valid range. Make sure the specified parameter is correct. \<port no.\>: Port number
No such Switch \<switch no.\>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. \<switch no.\>: Switch number
Switch \<switch no.\> was deleted from stack.	The member switch was deleted from the stack configuration. \<switch no.\>: Switch number

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:
  - The "restart vlan" command is executed.
  - 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 }]
```

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" or "schedule-power-control 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.

Behavior when all parameters are omitted:

> The information for all implemented Ethernet ports is listed.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch. You can also execute the command with the switch number of the member switch specified.

You can also use the "remote command" command.

```
remote command all show port
remote command all show port protocol
remote command all show port statistics [{ up | down }] [discard]
remote command all show port transceiver [detail]
remote command all show port vlan [{ access | trunk | protocol | mac | tunnel }]
remote command <switch no.> show port [<port list>]
remote command <switch no.> show port protocol [<port list>]
remote command <switch no.> show port statistics [<port list>] [{ up | down }] [discard]
remote command <switch no.> show port transceiver [<port list>] [detail]
remote command <switch no.> show port vlan [<port list>] [{ access | trunk | protocol | mac | t
unnel }]
```

Example 1

Figure 21-4: Example of listing the link information for ports

```
> show port
Date 20XX/01/14 10:56:37 UTC
Port Counts: 52
Port  Name          Status  Speed        Duplex     FCtl FrLen ChGr/Status
 0/ 1 tengeth1/0/1   up      10GBASE-T    full(auto) off  1518  1/up
 0/ 2 tengeth1/0/2   inact   1000BASE-T   full       off  1518  -/-
 0/ 3 tengeth1/0/3   down    -            -          -    -     -/-
          :
          :
          :
 0/40 tengeth1/0/40  up      1000BASE-T   full(auto) off  1518  1/up
 0/43 tengeth1/0/43  down    -            -          -    -     -/-
 0/44 tengeth1/0/44  down    -            -          -    -     -/-
 0/45 tengeth1/0/45  up      10GBASE-SR   full       off  1518  -/-
 0/46 tengeth1/0/46  up      10GBASE-SR   full       off  1518  -/-
 0/47 tengeth1/0/47  down    -            -          -    -     -/-
 0/48 tengeth1/0/48  up      10GBASE-SR   full       off  1518  -/-
 0/49 hndgeth1/0/49  up      100GBASE-LR4 full       off  1518  32/up
 0/50 hndgeth1/0/50  up      100GBASE-LR4 full       off  1518  32/up
 0/51 hndgeth1/0/51  down    -            -          -    -     -/-
 0/52 hndgeth1/0/52  up      100GBASE-LR4 full       off  1518  32/up
>
```

Display items in Example 1

Table 21-7: Description of displayed items in the link information list for ports

Item	Meaning	Displayed detailed information
Port Counts	Number of target ports	—
Port	Port	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 • Port resetting of GSRP • 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 the move monitoring function for MAC address learning. • The port has been deactivated by port resetting of uplink redundancy. dis: Operation was stopped by using the "shutdown" or "schedule-power-control shutdown" configuration command.

Item	Meaning	Displayed detailed information
Speed	Line speed	Displays the connection interface or abbreviation. 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 1000BASE-LHB: 1000BASE-LHB 10GBASE-T: 10GBASE-T 10GBASE-SR: 10GBASE-SR 10GBASE-LR: 10GBASE-LR 10GBASE-ER: 10GBASE-ER 10GBASE-ZR: 10GBASE-ZR 10GBASE-CU30CM: 10GBASE-CU (30cm) 10GBASE-CU1M: 10GBASE-CU (1m) 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 40GBASE-SR4: 40GBASE-SR4 40GBASE-LR4: 40GBASE-LR4 40GBASE-CU35CM: 40GBASE-CR4 (35cm) 40GBASE-CU1M: 40GBASE-CR4 (1m) 40GBASE-CU3M: 40GBASE-CR4 (3m) 40GBASE-CU5M: 40GBASE-CR4 (5m) 100GBASE-SR4: 100GBASE-SR4 100GBASE-CWDM4: 100GBASE-CWDM4 100GBASE-LR4: 100GBASE-LR4 100GBASE-4WDM: 100GBASE-4WDM-40 100GBASE-CU35CM: 100GBASE-CR4 (35cm) 100GBASE-CU1M: 100GBASE-CR4 (1m) -: The line speed is unknown (If auto-negotiation is enabled for a 10BASE-T/100BASE-TX/1000BASE-T/10GBASE-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) -: The line speed is unknown (If auto-negotiation is enabled for a 10BASE-T/100BASE-TX/1000BASE-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.

Item	Meaning	Displayed detailed information
FrLen	Maximum frame length	Displays the maximum frame length of the port in octets. -: Status is neither up nor test, or a stack port is used.
ChGr /Status	Channel group and status	The channel group to which the port belongs and the status. Channel group number: 1 to 48 (In a stack configuration, the number is between 1 and 96.) 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. In a stack configuration, "-" is displayed as the status of the backup switch.

Example 2

Figure 21-5: Example of listing the protocol information for ports

```
> show port protocol
Date 20XX/01/14 10:56:37 UTC
Port Counts: 52
Port  Name           Type        VLAN STP   QoS Filter MACTbl   Ext.
 0/ 1 tengeth1/0/1   Protocl      100   0     0      0      0    - - - - - -
 0/ 2 tengeth1/0/2   Mac         1024   0   100    100      7    - - - - - -
 0/ 3 tengeth1/0/3   Trunk        256   0     0      0      0    - - - - - -
 0/ 4 tengeth1/0/4   Protocol      16   0     1      1      0    - - - - - -
              :
              :
              :
 0/49 hndgeth1/0/49  Access         1   0     0      0      0    - - - - - -
 0/50 hndgeth1/0/50  Access         1   0     0      0      0    - - - - - -
 0/51 hndgeth1/0/51  Access         1   0     0      0      0    - - - - - -
 0/52 hndgeth1/0/52  Access         1   0     0      0      0    - - - - - -
>
```

Display items in Example 2

Table 21-8: Displayed items for the protocol information list for ports

Item	Meaning	Displayed detailed information
Port Counts	Number of target ports	—
Port	Port	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 Stack: Stack 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)

Item	Meaning	Displayed detailed information
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. O: Indicates that OADP 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 21-6: 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: 52
Port  Name          Status T/R  All packets   Multicast   Broadcast    Discard
 0/ 1 geth1/0/1     up     Tx         36060       36012          48          0
                           Rx   267868905982 67868905982           0          0
 0/ 2 geth1/0/2     inact  Tx             0           0           0          0
                           Rx             0           0           0          0
 0/ 3 geth1/0/3     down   Tx             0           0           0          0
                           Rx             0           0           0          0
 0/ 4 geth1/0/4     down   Tx             0           0           0          0
                           Rx             0           0           0          0
 0/ 5 geth1/0/5     down   Tx             0           0           0          0
                           Rx             0           0           0          0
              :
              :
              :
 0/47 tengeth1/0/47 down   Tx             0           0           0          0
                           Rx             0           0           0          0
 0/48 tengeth1/0/48 up     Tx          5679           0          10          0
                           Rx          5158           0          11          0
 0/49 hndgeth1/0/49 up     Tx   41601114258 32945109231           1          0
                           Rx    6352088724       15118           8          0
 0/50 hndgeth1/0/50 up     Tx  230169902708 25895910148      557807          0
                           Rx   34671538289       66885     1487508          0
 0/51 hndgeth1/0/51 down   Tx             0           0           0          0
                           Rx             0           0           0          0
 0/52 hndgeth1/0/52 up     Tx   42422843302 41973185821         160          0
                           Rx    5839856540        5593       42399          0
>
```

Display items in Example 3

Table 21-9: 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	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 • Port resetting of GSRP • 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 the move monitoring function for MAC address learning. • The port has been deactivated by port resetting of uplink redundancy. dis: Operation was stopped by using the "shutdown" or "schedule-power-control 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	
Discard	Number of discarded packets	

Example 4

Figure 21-7: Example of listing the detailed transceiver information (if the transceiver type is SFP or SFP+)

```
> show port transceiver 1/0/47-48 detail
Date 20XX/01/14 10:56:38 UTC
Port Counts: 2
Port: 0/47 Status:notconnect  Type:-  Speed:-
        Vendor name:-              Vendor SN :-
        Vendor PN  :-             Vendor rev:-
        Tx power   :-             Rx power  :-
        Temperature:-
        Voltage    :-
```

```
          Tx bias   :-
Port: 0/48 Status:connect  Type:SFP+  Speed:10GBASE-SR
          Vendor name:xxxxxxxxxxxxxxxx     Vendor SN :xxxxxxxxxxxxxxxx
          Vendor PN  :xxxxxxxxxxxxxxxx     Vendor rev:xxxx
          Tx power   :-2.0dBm             Rx power  :-2.4dBm
          Temperature:40 degrees C
          Voltage    :3.22V
          Tx bias    :23mA
>
```

Display items in Example 4

Table 21-10: 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	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 or abbreviation. 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 1000BASE-LHB: 1000BASE-LHB 10GBASE-SR: 10GBASE-SR 10GBASE-LR: 10GBASE-LR 10GBASE-ER: 10GBASE-ER 10GBASE-ZR: 10GBASE-ZR 10GBASE-CU30CM: 10GBASE-CU (30cm) 10GBASE-CU1M: 10GBASE-CU (1m) 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]

Item	Meaning	Displayed detailed information
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, #5]
Rx power	Receiving optical power	Displays the receiving optical power in dBm.[#1, #2, #3, #4, #5]
Temperature	Temperature	Displays the temperature in degrees Celsius.[#1, #2, #4, #5, #6]
Voltage	Voltage	Displays the voltage in volts.[#1, #2, #4, #5, #7]
Tx bias	Bias current	Displays the bias current in mA.[#1, #2, #4, #5, #8]

#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.

#5: A hyphen (-) is displayed if an SFP-T and direct attach cable is used.

#6: If the temperature is out of range of -128 to 128 degrees Celsius, a hyphen (-) is displayed.

#7: If the voltage is out of range from 0.00 to 6.55 V, a hyphen (-) is displayed.

#8: If the bias current is out of range from 0 to 131 mA, a hyphen (-) is displayed.

Example 5

Figure 21-8: Example of listing detailed transceiver information (when the transceiver type is QSFP+ or QSFP28)

```
> show port transceiver 1/0/49-52 detail
Date 20XX/10/06 12:00:00 UTC
Port Counts: 4
Port: 0/49 Status:connect  Type:QSFP+  Speed:40GBASE-SR4
          Vendor name:xxxxxxxxxxxxxxxx      Vendor SN :xxxxxxxxxxxxxxxx
          Vendor PN  :xxxxxxxxxxxxxxxx      Vendor rev:xxxx
          Tx1 power  :-4.7dBm               Rx1 power :-40.0dBm
          Tx2 power  :-4.7dBm               Rx2 power :-40.0dBm
          Tx3 power  :-4.7dBm               Rx3 power :-40.0dBm
          Tx4 power  :-4.7dBm               Rx4 power :-40.0dBm
          Temperature:40 degrees C
          Voltage    :3.22V
          Tx1 bias   :23mA
          Tx2 bias   :23mA
          Tx3 bias   :23mA
          Tx4 bias   :23mA
Port: 0/50 Status:notconnect  Type:-  Speed:-
          Vendor name:-                     Vendor SN :-
          Vendor PN  :-                     Vendor rev:-
          Tx1 power  :-                     Rx1 power :-
          Tx2 power  :-                     Rx2 power :-
          Tx3 power  :-                     Rx3 power :-
          Tx4 power  :-                     Rx4 power :-
          Temperature:-
          Voltage    :-
          Tx1 bias   :-
```

```
           Tx2 bias   :-
           Tx3 bias   :-
           Tx4 bias   :-
Port: 0/51 Status:notconnect   Type:-  Speed:-
           Vendor name:-                  Vendor SN :-
           Vendor PN  :-                  Vendor rev:-
           Tx1 power  :-                  Rx1 power :-
           Tx2 power  :-                  Rx2 power :-
           Tx3 power  :-                  Rx3 power :-
           Tx4 power  :-                  Rx4 power :-
           Temperature:-
           Voltage    :-
           Tx1 bias   :-
           Tx2 bias   :-
           Tx3 bias   :-
           Tx4 bias   :-
Port: 0/52 Status:connect  Type:QSFP28  Speed:100GBASE-LR4
           Vendor name:xxxxxxxxxxxxxxxx    Vendor SN :xxxxxxxxxxxxxxxx
           Vendor PN  :xxxxxxxxxxxxxxxx    Vendor rev:xxxx
           Tx1 power  :-4.7dBm             Rx1 power :-40.0dBm
           Tx2 power  :-4.7dBm             Rx2 power :-40.0dBm
           Tx3 power  :-4.7dBm             Rx3 power :-40.0dBm
           Tx4 power  :-4.7dBm             Rx4 power :-40.0dBm
           Temperature:40 degrees C
           Voltage    :3.22V
           Tx1 bias   :23mA
           Tx2 bias   :23mA
           Tx3 bias   :23mA
           Tx4 bias   :23mA
>
```

Display items in Example 5

Table 21-11: Display items of the transceiver information list (when the transceiver type is QSFP+ or QSFP28)

Item	Meaning	Displayed detailed information
Port Counts	Number of target ports	—
Port	Port	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	QSFP+: QSFP+ QSFP28: QSFP28 -: The type of the transceiver is unknown (- is displayed if the transceiver status is notconnect).
Speed	Line speed	Displays the connection interface or abbreviation. 40GBASE-SR4: 40GBASE-SR4 40GBASE-LR4: 40GBASE-LR4 40GBASE-CU35CM: 40GBASE-CR4 (35cm) 40GBASE-CU1M: 40GBASE-CR4 (1m) 40GBASE-CU3M: 40GBASE-CR4 (3m) 40GBASE-CU5M: 40GBASE-CR4 (5m) 100GBASE-SR4: 100GBASE-SR4

Item	Meaning	Displayed detailed information
		100GBASE-CWDM4: 100GBASE-CWDM4 100GBASE-LR4: 100GBASE-LR4 100GBASE-4WDM: 100GBASE-4WDM-40 100GBASE-CU35CM: 100GBASE-CR4 (35cm) 100GBASE-CU1M: 100GBASE-CR4 (1m) -: 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]
Tx1 power	Lane 1 sending optical power	Displays the sending optical power of Lane 1 in dBm.[#1, #2, #3, #4, #5]
Rx1 power	Lane 1 receiving optical power	Displays the receiving optical power of Lane 1 in dBm.[#1, #2, #3, #4, #5]
Tx2 power	Lane 2 sending optical power	Displays the sending optical power of Lane 2 in dBm.[#1, #2, #3, #4, #5]
Rx2 power	Lane 2 receiving optical power	Displays the receiving optical power of Lane 2 in dBm.[#1, #2, #3, #4, #5]
Tx3 power	Lane 3 sending optical power	Displays the sending optical power of Lane 3 in dBm.[#1, #2, #3, #4, #5]
Rx3 power	Lane 3 receiving optical power	Displays the receiving optical power of Lane 3 in dBm.[#1, #2, #3, #4, #5]
Tx4 power	Lane 4 sending optical power	Displays the sending optical power of Lane 4 in dBm.[#1, #2, #3, #4, #5]
Rx4 power	Lane 4 receiving optical power	Displays the receiving optical power of Lane 4 in dBm.[#1, #2, #3, #4, #5]
Temperature	Temperature	Displays the temperature in degrees Celsius.[#1, #2, #4, #5, #6]
Voltage	Voltage	Displays the voltage in volts.[#1, #2, #4, #5, #7]
Tx1 bias	Lane 1 bias current	Displays the bias current in mA.[#1, #2, #4, #5, #8]
Tx2 bias	Lane 2 bias current	Displays the bias current in mA.[#1, #2, #4, #5, #8]
Tx3 bias	Lane 3 bias current	Displays the bias current in mA.[#1, #2, #4, #5, #8]
Tx4 bias	Lane 4 bias current	Displays the bias current in mA.[#1, #2, #4, #5, #8]

#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.

#5: A hyphen (-) is displayed if an SFP-T and direct attach cable is used.

#6: If the temperature is out of range of -128 to 128 degrees Celsius, a hyphen (-) is displayed.

#7: If the voltage is out of range from 0.00 to 6.55 V, a hyphen (-) is displayed.

#8: If the bias current is out of range from 0 to 131 mA, a hyphen (-) is displayed.

Example 6

Figure 21-9: Example of listing VLAN information for ports (standalone configuration)

```
> show port vlan
Date 20XX/01/15 14:15:00
Port Counts: 52
Port  Name            Status Type      VLAN
 0/ 1 tengeth1/0/1    up     Protocl   100  (Global IP Network VLAN)
 0/ 2 tengeth1/0/2    inact  Mac       1024
      :
      :
      :
 0/49 hndgeth1/0/49   up     Trunk     32
 0/50 hndgeth1/0/50   up     Stack     32
 0/51 hndgeth1/0/51   down   Access    1    (DefaultVLAN)
 0/52 hndgeth1/0/52   up     Trunk     32
>
```

Figure 21-10: 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
 0/ 3 geth1/0/3       up     Trunk     1-4094
 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 6

Table 21-12: Display items of the VLAN information list for ports

Item	Meaning	Displayed detailed information
Switch	Switch number. The switch status is displayed in parentheses.	Switch number Master: In the stack configuration (Master) Backup: In the stack configuration (Backup)
Port counts	Number of target ports	—
Port	Port 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.

Item	Meaning	Displayed detailed information
		• The standby link function of link aggregation • The BPDU guard function of the Spanning Tree Protocol • Port resetting of GSRP • 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 the move monitoring function for MAC address learning. • The port has been deactivated by port resetting of uplink redundancy. dis: Operation was stopped by using the "shutdown" or "schedule-power-control shutdown" configuration command.
Type	Port type	Access: Access port Trunk: Trunk port Protocol: Protocol VLAN port Mac: MAC VLAN port Tunnel: Tunneling port Stack: Stack 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.

Impact on communication

None

Response messages

Table 21-13: List of response messages for the show port command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Manager.	Communication with the L2Manager program failed. Re-execute the command. If this message is output frequently, execute the "restart vlan" command to restart the L2Manager program.
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.

Message	Description
Connection failed to OADP.	Communication with the OADP program failed. Re-execute the command. If the failure occurs frequently, use the "re-start oadp" command to restart the OADP 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.
No operational Port.	There are no available ports. Make sure the specified parameter is correct.
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

1. The displayed number of discarded packets is the total of the values for the items listed in the following table.

Table 21-14: Statistical items used to calculate the number of discarded packets

Port	Statistical item	
	Sending	**Receiving**
Ethernet	Late collision Excessive collisions Excessive deferral	CRC errors Alignment Fragments Symbol errors Short frames Long frames

2. The statistic counter is cleared when:

   - The device starts up.
   - The "clear counters" command is executed.
   - The "restart vlan" command is executed.
   - A device hardware failure occurs.
   - A failure occurs in the network interface management program (nimd).

3. If the "no switchport" configuration command is set for a port, the target port information is not displayed even if the protocol and VLAN parameters are specified in this command.

4. If the stack function is disabled in a model that has a stack-dedicated port, the 40GBASE-R port is not displayed.

5. In AX3660S-24T4X, AX3660S-24T4XW, and AX3660S-48T4XW, if the software license or optional

license does not support 10G uplink, inserting an SFP + transceiver changes the transceiver status to not support.

6. In AX3660S-16S4XW and AX3660S-24X4QW, if the optional license does not support expanding the number of ports, inserting a transceiver into a port enabled by the optional license changes the transceiver status to not support.

7. In AX3660S-48XT4QW, if the line speed of the QSFP28/QSFP+ shared port is not enabled at 100 Gbit/s with the "system interface hundredgigabitethernet" configuration command, inserting a QSFP28 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 {gigabitethernet | tengigabitethernet | fortygigabitethernet | hundredgigabitethernet}
<switch no.>/<nif no.>/<port no.>
```

Input mode

User mode and administrator mode

Parameters

{gigabitethernet | tengigabitethernet | fortygigabitethernet | hundredgigabitethernet}

    gigabitethernet

        Specifies an Ethernet interface with the maximum line speed of 1 Gbit/s.

    tengigabitethernet

        Specifies an Ethernet interface with the maximum line speed of 10 Gbit/s.

    fortygigabitethernet

        Specifies an Ethernet interface with the maximum line speed of 40 Gbit/s.

    hundredgigabitethernet

        Specifies an Ethernet interface with the maximum line speed of 100 Gbit/s.

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

    Specifies the switch number, NIF number, and port number. For the specifiable range of values, see "Specifiable values for parameters".

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command <switch no.> activate {gigabitethernet | tengigabitethernet | fortygigabitethern
et | hundredgigabitethernet} <switch no.>/<nif no.>/<port no.>
```

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.

Response messages

Table 21-15: List of response messages for the activate command

Message	Description
<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 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. <switch no.>: Switch number <nif no.>: NIF number <port no.>: Port number
<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. <switch no.>: Switch number <nif no.>: NIF number <port no.>: Port number
<switch no.>/<nif no.>/<port no.> is not fortygigabitethernet.	The interface of the specified port is not fortygigabitethernet. 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 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 hundredgigabitethernet.	The interface of the specified port is not hundredgigabitethernet. 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
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The port number is outside the valid range. Make sure the specified parameter is correct. <port no.>: Port number
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 such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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 {gigabitethernet | tengigabitethernet | fortygigabitethernet | hundredgigabitetherne
t} <switch no.>/<nif no.>/<port no.>
```

Input mode

User mode and administrator mode

Parameters

{gigabitethernet | tengigabitethernet | fortygigabitethernet | hundredgigabitethernet}

    gigabitethernet

        Specifies an Ethernet interface with the maximum line speed of 1 Gbit/s.

    tengigabitethernet

        Specifies an Ethernet interface with the maximum line speed of 10 Gbit/s.

    fortygigabitethernet

        Specifies an Ethernet interface with the maximum line speed of 40 Gbit/s.

    hundredgigabitethernet

        Specifies an Ethernet interface with the maximum line speed of 100 Gbit/s.

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

    Specifies the switch number, NIF number, and port number. For the specifiable range of values, see "Specifiable values for parameters".

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command <switch no.> inactivate {gigabitethernet | tengigabitethernet | fortygigabitethe
rnet | hundredgigabitethernet} <switch no.>/<nif no.>/<port no.>
```

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.

Response messages

Table 21-16: List of response messages for the inactivate command

Message	Description
<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 disabled.	The specified port is in disable status due to the configuration. 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 failed.	The specified port is not in active status. 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 fortygigabitethernet.	The interface of the specified port is not fortygigabitethernet. 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 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 hundredgigabitethernet.	The interface of the specified port is not hundredgigabitethernet. 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
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The port number is outside the valid range. Make sure the specified parameter is correct. <port no.>: Port number

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. (For details about canceling a line test, see "no test interfaces".)
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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 gigabitethernet <nif no.>/<port no.> {internal | connector}
     [auto_negotiation {10base-t | 100base-tx | 1000base-t}]
     [interval <interval time>] [pattern <test pattern no.>]
     [length <data length>]
test interfaces tengigabitethernet <nif no.>/<port no.> {internal | connector}
     [auto_negotiation {10base-t | 100base-tx | 1000base-t | 10Gbase-t}]
     [interval <interval time>] [pattern <test pattern no.>]
     [length <data length>]
test interfaces fortygigabitethernet <nif no.>/<port no.> {internal | connector}
     [interval <interval time>] [pattern <test pattern no.>]
     [length <data length>]
test interfaces hundredgigabitethernet <nif no.>/<port no.> {internal | connector}
     [interval <interval time>] [pattern <test pattern no.>]
     [length <data length>]
```

Input mode

User mode and administrator mode

Parameters

gigabitethernet

Specifies an Ethernet interface with the maximum line speed of 1 Gbit/s.

tengigabitethernet

Specifies an Ethernet interface with the maximum line speed of 10 Gbit/s.

fortygigabitethernet

Specifies an Ethernet interface with the maximum line speed of 40 Gbit/s.

hundredgigabitethernet

Specifies an Ethernet interface with the maximum line speed of 100 Gbit/s.

<nif no.>/<port no.>

Specifies the NIF number and the port number. For the specifiable range of values, see "Specifiable values for parameters".

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}

Specifies the segment standard that will be used for a line test conducted when "auto" is specified in the

445

"speed" configuration command.

Note that this parameter can be specified only when "auto" is specified in the "speed" command. It can be specified when the line type is as follows:

- 100BASE-TX/1000BASE-T/10GBASE-T port
- When SFP-T is used on an SFP port

Behavior when this parameter is omitted:

The command assumes that 100base-tx is specified.

auto_negotiation {10base-t | 100base-tx | 1000base-t | 10Gbase-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. It can be specified when the line type is as follows:

- 100BASE-TX/1000BASE-T/10GBASE-T port
- When SFP-T is used on an SFP+/SFP shared port

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 21-17: 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.

Operation when a stack configuration is used

This command is not supported.

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 21-11: Starting a line test

```
> test interfaces  gigabitethernet 0/2 internal interval 5 pattern 1 length 100
```

Display items

None

Impact on communication

None

Response messages

Table 21-18: List of response messages for the test interfaces command

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 fortygigabitethernet.	The interface of the specified port is not fortygigabitethernet. 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 hundredgigabitethernet.	The interface of the specified port is not hundredgigabitethernet. 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
Can't execute this commad in all switches configured stack.	In a stack configuration, the command cannot be executed.

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The port number is outside the valid range. Make sure the specified parameter is correct. \<port no.>: Port number
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 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.

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, 1000BASE-LHB, 10GBASE-ER, or 10GBASE-ZR port, an optical attenuator is required. For details about optical attenuation, see the following table.

Table 21-19: Optical attenuation

Line type	Attenuation value (dB)
1000BASE-LH	5 to 22
1000BASE-LHB	17 to 36
10GBASE-ER	5 to 11
10GBASE-ZR	15 to 24

- 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 used in the SFP port or SFP+/SFP shared port.

- The loop connector loopback test cannot be conducted on a 100BASE-TX/1000BASE-T/10GBASE-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 gigabitethernet <nif no.>/<port no.>
no test interfaces tengigabitethernet <nif no.>/<port no.>
no test interfaces fortygigabitethernet <nif no.>/<port no.>
no test interfaces hundredgigabitethernet <nif no.>/<port no.>
```

Input mode

User mode and administrator mode

Parameters

gigabitethernet

Specifies an Ethernet interface with the maximum line speed of 1 Gbit/s.

tengigabitethernet

Specifies an Ethernet interface with the maximum line speed of 10 Gbit/s.

fortygigabitethernet

Specifies an Ethernet interface with the maximum line speed of 40 Gbit/s.

hundredgigabitethernet

Specifies an Ethernet interface with the maximum line speed of 100 Gbit/s.

<nif no.>/<port no.>

Specifies the NIF number and the port number. For the specifiable range of values, see "Specifiable values for parameters".

Operation when a stack configuration is used

This command is not supported.

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 21-12: 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 21-20: Items displayed as a line test result

Item	Meaning	Presumed cause	Measures
Interface type	Line type (which displays the connection interface or abbreviation) • 10BASE-T • 100BASE-TX • 1000BASE-T • 1000BASE-LX • 1000BASE-SX • 1000BASE-LH • 1000BASE-BX10-D • 1000BASE-BX10-U • 1000BASE-BX40-D • 1000BASE-BX40-U • 1000BASE-LHB • 10GBASE-T • 10GBASE-SR • 10GBASE-LR • 10GBASE-ER • 10GBASE-ZR • 10GBASE-CU30CM • 10GBASE-CU1M • 10GBASE-CU3M • 10GBASE-CU5M • 10GBASE-BR10-D • 10GBASE-BR10-U • 10GBASE-BR40-D • 10GBASE-BR40-U • 40GBASE-SR4 • 40GBASE-LR4 • 40GBASE-CU35CM • 40GBASE-CU1M • 40GBASE-CU3M • 40GBASE-CU5M • 100GBASE-SR4 • 100GBASE-CWDM4 • 100GBASE-LR4 • 100GBASE-4WDM[1] • 100GBASE-CU35CM • 100GBASE-CU1M • ----[2]	—	—
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.

Item	Meaning	Presumed cause	Measures
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[3]	Line failure	Replace the device.
In alignment	The number of times the frame length was invalid and an error was detected by the FCS check[3]	Line failure	Replace the device.
In monitor time out	Timeout for the reception monitoring timer	Line failure	For a loop connector loopback test, verify that a loopback connector is correctly connected to the port.[4]
In line error	Number of receive line failures that occurred	Line failure	For a loop connector loopback test, verify that a loopback 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: It is displayed in abbreviated form. The following table shows what connection interface the abbreviation refers to.

Table 21-21: Association between the abbreviation and the connection interface

Abbreviated name	Connection interface
100GBASE-4WDM	100GBASE-4WDM-40

#2: 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.

#3: The frame length indicates the length starting from the MAC header and ending with the FCS field. For details about frame formats, see "Configuration Guide Vol. 1, 20.2.2 Frame format".

#4: 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

Response messages

Table 21-22: List of response messages for the no test interfaces command

Message	Description
<nif no.>/<port no.> is not fortygigabitethernet.	The interface of the specified port is not fortygigabitethernet. 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 hundredgigabitethernet.	The interface of the specified port is not hundredgigabitethernet. 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
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The port number is outside the valid range. 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
Test not executing.	No line test has been conducted. Make sure the specified parameter is correct.

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.

- The loop connector loopback test cannot be conducted on a 100BASE-TX/1000BASE-T/10GBASE-T port. If the test is conducted, the Send-NG value will increase.

show network-clock

Shows the behavior status of Sync-E.

Syntax

```
show network-clock synchronization
```

Input mode

User mode and administrator mode

Parameters

synchronization

Shows the behavior status of Sync-E.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show network-clock synchronizaion
```

Example

Figure 21-13: Example of displaying the Sync-E information

```
> show network-clock synchronization
Date 20XX/07/26 11:56:46 UTC
Current input source
Priority  : 1
Port      : 1/0/1
Status    : Sync

Source status
Pri Port   Link Clock
    1 1/0/1  Up   Lock
    2 1/0/2  Up   Lock
>
```

Display items

Table 21-23: Display items for the Sync-E information

Item	Meaning	Displayed detailed information
Current input source	Information on the clock currently working	—
Priority	Priority	Number: Priority -: Working through internal clock signals
Port	Receiving port number for external clock signals	XX: Receiving port number Internal: Working through internal clock signals

Item	Meaning	Displayed detailed information
Status	Clock behavior status	Sync: Working through external clock signals, with proper Sync-E synchronization Freerun: Working through internal clock signals
Source status	External clock reception information	Displayed when the external clock reception port information is configured with the "network-clock" configuration command.
Pri	Priority	—
Port	Receiving port number for external clock signals	—
Link	Link status of the receiving port	Up: Link-up status Down: Link-down status
Clock	Reception status of external clock signals	Lock: Receiving external clock signals Lock (preempt-delay XX sec): Receiving external clock signals, with auto-switchback suppressed. When switchbacking is suppressed, it displays the time required to perform a switchback action. Unlock (Out of Frequency): External clock frequency accuracy error detected Unlock (Loss of Signal): No external clock signals received

Impact on communication

None

Response messages

Table 21-24: List of response messages for the show network-clock command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

Notes

None

22 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.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example 1

The following shows an example of displaying information about link aggregation.

Figure 22-1: 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
  Multi Speed  :Off        Load Balance:src-dst-port
  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:11   Mode:LACP
 CH Status   :Down     Elapsed Time:-
 Multi Speed :Off      Load Balance:src-dst-port
 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:21   Mode:Static
 CH Status   :Disabled  Elapsed Time:-
 Multi Speed :Off      Load Balance:src-dst-port
 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:22   Mode:Static
 CH Status   :Up       Elapsed Time:160.11:45:10
 Multi Speed :Off      Load Balance:src-dst-port
 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
>
```

The following shows an example of displaying the link aggregation information for a specific channel group number.

Figure 22-2: Displaying the link aggregation information for a specific channel group number

```
>show channel-group 21-30
Date 20XX/12/10 12:00:00 UTC
channel-group Counts:2
 ChGr:21   Mode:Static
 CH Status   :Disabled  Elapsed Time:-
 Multi Speed :Off      Load Balance:src-dst-port
 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:22   Mode:Static
 CH Status   :Up       Elapsed Time:160.11:45:10
 Multi Speed :Off      Load Balance:src-dst-port
 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 22-1: 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.
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 de-tached ports	0 or 7 (7 is displayed as the initial value.) "-" is displayed when link aggregation mode is not set.
Load Balance	Distribution method	dst-ip: The load is distributed according to the destination IP addresses. dst-mac: The load is distributed according to the destination MAC addresses. dst-port: The load is distributed according to the destination port numbers. src-dst-ip: The load is distributed according to the source and destination IP addresses. src-dst-mac: The load is distributed according to the source and destination MAC addresses. src-dst-port: The load is distributed according to the source and destination port numbers. src-ip: The load is distributed according to the source IP addresses. src-mac: The load is distributed according to the source MAC addresses. src-port: The load is distributed according to the source port numbers.

Item	Meaning	Displayed detailed information
Multi Speed	Mixed-speed mode	Off: Does not permit a channel group to consist of ports with different transmission speeds. On: Permits a channel group to consist of ports with different transmission speeds.
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
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

Item	Meaning	Displayed detailed information
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 22-3: 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)             :1,22
Down(1)           :11
Disabled(1)       :21
>
```

Display items in Example 2

Table 22-2: 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 22-4: 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
  Multi Speed  :Off       Load Balance:src-dst-port
  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:11   Mode:LACP
  CH Status    :Down     Elapsed Time:-
  Multi Speed  :Off      Load Balance:src-dst-port
  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:21   Mode:Static
  CH Status    :Disabled  Elapsed Time:-
  Multi Speed  :Off       Load Balance:src-dst-port
  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:22   Mode:Static
  CH Status    :Up        Elapsed Time:160.11:45:10
  Multi Speed  :Off       Load Balance:src-dst-port
  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
>
```

The following shows an example of displaying the detailed link aggregation information for a specific channel group number.

Figure 22-5: Displaying the detailed link aggregation information for a specific channel group number

```
>show channel-group 10-21 detail
Date 20XX/12/10 12:00:00 UTC
channel-group Counts:2
ChGr:11   Mode:LACP
 CH Status    :Down      Elapsed Time:-
 Multi Speed  :Off       Load Balance:src-dst-port
 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:21   Mode:Static
 CH Status    :Disabled  Elapsed Time:-
 Multi speed  :Off       Load Balance:src-dst-port
 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
>
```

Display items in Example 3

Table 22-3: 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 link-not-down mode, sending is impossible but receiving is possible.)
		Disabled: Link aggregation is disabled.

Item	Meaning	Displayed detailed information
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	dst-ip: The load is distributed according to the destination IP addresses. dst-mac: The load is distributed according to the destination MAC addresses. dst-port: The load is distributed according to the destination port numbers. src-dst-ip: The load is distributed according to the source and destination IP addresses. src-dst-mac: The load is distributed according to the source and destination MAC addresses. src-dst-port: The load is distributed according to the source and destination port numbers. src-ip: The load is distributed according to the source IP addresses. src-mac: The load is distributed according to the source MAC addresses. src-port: The load is distributed according to the source port numbers.
Multi Speed	Mixed-speed mode	Off: Does not permit a channel group to consist of ports with different transmission speeds. On: Permits a channel group to consist of ports with different transmission speeds.
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.

Item	Meaning	Displayed detailed information
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.

Item	Meaning	Displayed detailed information
		LACPDU Expired: The valid time period of the LACPDU received from the connected port expired.
		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
		10G: 10 Gbit/s
		40G: 40 Gbit/s
		100G: 100 Gbit/s
		-: The line speed is unknown.
Duplex	Duplex mode	Full: Full 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. An asterisk (*) is added when the device is waiting for receiving a LACPDU after the master switch is switched over. (* Active)
		Passive: An LACPDU is sent after an LACPDU is received. An asterisk (*) is added when the device is waiting for receiving a LACPDU after the master switch is switched over. (* Passive)
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.

Item	Meaning	Displayed detailed information
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 is Unmatched Partner Key.
Unmatched Partner System ID	Partner system ID that is unmatched	This item is displayed only when Status is Down and Reason is 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

Response messages

Table 22-4: List of response messages for the show channel-group command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Manager.	Communication with the L2 Manager program failed. Re-execute the command. If this message is output frequently, execute the "restart vlan" command to restart the L2 Manager program.
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.
Specified channel-group is not configured.	The channel group has not been configured. Check the configuration.

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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show channel-group statistics
```

When the lacp parameter is specified, the command can display the information only for the master switch.

Example 1

The following shows an example of displaying statistics on sent and received data packets for link aggregation (by port).

Figure 22-6: 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:11(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:21(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:22(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
>
```

The following shows an example of displaying statistics on sent and received data packets for a specific channel group number (by port).

Figure 22-7: Displaying the statistics on sent and received data packets for a specific channel group number

```
>show channel-group statistics 22-30
Date 20XX/07/14 12:00:00 UTC
channel-group counts:1
ChGr:22(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 22-5: 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. The status of the channel group is displayed only for the master switch.
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
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 21-14: 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 22-8: 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
>
```

The following shows an example of displaying statistics for sent and received LACPDUs for a specific channel group number.

Figure 22-9: Displaying the statistics for sent and received LACPDUs for a specific channel group number

```
>show channel-group statistics lacp 10-20
Date 20XX/07/14 12:00:00 UTC
channel-group counts:1
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 22-6: 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
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	—

Item	Meaning	Displayed detailed information
RxMarkerPDUs	Number of received marker PDUs	—
RxDiscards	Number of discarded received PDUs	Number of LACPDUs discarded due to parameter errors

Impact on communication

None

Response messages

Table 22-7: List of response messages for the show channel-group statistics command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Manager.	Communication with the network interface management program failed. Re-execute the command. If this message is output frequently, execute the "restart vlan" command to restart the network interface management program.
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.
Specified channel-group is not configured.	The channel group has not been configured. Check the configuration.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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.

Operation when a stack configuration is used

The command can clear information only from the master switch.

Example

Figure 22-10: Clearing the statistics on sent and received LACPDUs for link aggregation

```
>clear channel-group statistics lacp
>
```

Figure 22-11: Clearing the statistics on sent and received LACPDUs for a specific channel group number in a link aggregation

```
>clear channel-group statistics lacp 11
>
```

Display items

None

Impact on communication

None

Response messages

Table 22-8: List of response messages for the clear channel-group statistics lacp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.

Message	Description
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.
Specified channel-group is not configured.	The channel group has not been configured. Check the configuration.

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 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 link aggregation program is restarted.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} restart link-aggregation [-f] [core-file]
```

Example

Figure 22-12: Restarting the link aggregation program

```
> restart link-aggregation
Link Aggregation restart OK? (y/n):y
>
```

Figure 22-13: 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.

Response messages

Table 22-9: List of response messages for the restart link-aggregation command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
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.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} dump protocols link-aggregation
```

Example

Figure 22-14: Taking a link aggregation dump

```
> dump protocols link-aggregation
>
```

Impact on communication

None

Response messages

Table 22-10: List of response messages for the dump protocols link-aggregation command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
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.
Specified channel-group is not configured.	The channel group has not been configured. Check the configuration.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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.

23 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 and the number of detected moves for MAC address learning for each port.

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.

Operation when a stack configuration is used

The information in the MAC address table of the master switch is automatically synchronized with that of the other member switches.

If the learning-counter parameter is specified, execute the command on all member switches that belong to the stack on the master switch. You can also execute the command with the switch number of the member switch specified.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show mac-address-table learning-counter [ port <port list>
] [channel-group-number <channel group list>]
```

Example 1

Figure 23-1: 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 23-1: Display items for the information in the MAC address table

Item	Meaning	Displayed detailed information
MAC address	MAC address	—
VLAN	VLAN ID	-: When Vxlan is displayed in Type
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 or registered via IEEE 802.1X Dot1x: Entry registered via IEEE 802.1X Wa: Entry registered via the Web authentication function Macauth: Entry registered via the MAC-based authentication function Vxlan: Entries learned by VNI for VXLAN
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 Blank: When Vxlan is displayed in Type

Example 2

Figure 23-2: 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      Movement Detect
1/0/1            3                    0
1/0/2         1000                 1000
1/0/3            0                    0
1/0/4           50                    0
1/0/5           45                    0
1/0/6            0                    0
1/0/7           22                   50
1/0/8            0                    0
1/0/9            0                    0
1/0/10           0                    0
>
```

Figure 23-3: 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 23-2: 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
Count	Number of learned entries in the current MAC address table	—
Movement Detect	Number of times moves for MAC address learning were detected	—
Maximum	Maximum number of addresses that can be learned in the MAC address table	"-" is displayed at all times.

Impact on communication

None

Response messages

Table 23-3: List of response messages for the show mac-address-table command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Mac Manager.	Communication with the L2 Mac Manager program failed. Re-execute the command. If this message is output frequently, execute the "restart vlan" command to restart the L2 Mac Manager program.
Connection failed to L2 Manager.	Communication with the L2Manager program failed. Re-execute the command. If this message is output frequently, execute the "restart vlan" command to restart the L2Manager 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.
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.

Message	Description
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Specified VLAN is not configured.	The specified VLAN has not been configured. Make sure the specified parameter is correct, and then try again.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

1. Entries learned by the IGMP snooping function or MLD snooping function are not displayed by this command when the IP multicast routing function is used together.

2. If the VXLAN function is enabled, entries learned through VNIs are displayed. For MAC address table information about VXLAN, see the "show vxlan mac-address-table" command.

3. The number of times moves for MAC address learning were detected is cleared to 0 by using the "clear counters" command. It is not cleared to zero by the "clear mac-address-table" command.

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.

Operation when a stack configuration is used

The clearing of the information in the MAC address table of the master switch is automatically synchronized

with the other member switches.

Example

Figure 23-4: 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 23-5: 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

For L2 forwarding, frames are flooded until learning is completed again. Execute this command at a time when flooding will have a minimal impact.

For L3 forwarding, communication might temporarily be interrupted.

Response messages

Table 23-4: List of response messages for the clear mac-address-table command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
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 Manager.	Communication with the L2Manager program failed. Re-execute the command. If this message is output frequently, execute the "restart vlan" command to restart the L2Manager program.
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.

Notes

1. If the VXLAN function is enabled, entries learned through VNIs are also cleared according to the parameters. However, some entries are not cleared depending on the specified parameters.

   - When you specify a parameter that takes a VLAN ID for clearing, the command do not clear entries learned through VNIs mapped to the VLAN IDs set by the "encapsulation dot1q" configuration command.
   - When you specify a parameter that takes a port for clearing, the command do not clear entries learned through VXLAN Network ports.
   - When you specify a VLAN ID or a VLAN ID and MAC address in the parameter for clearing, with the "vxlan vlan-mapping mode" configuration command not set, all entries are not cleared.

For details about how to clear entries by specifying a VNI, see the "clear vxlan mac-address-table" command.

2. The number of times moves for MAC address learning were detected, which is displayed when the learning-counter parameter is specified in the "show mac -address-table" command, is not cleared to zero.

24 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.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example 1

The following figure shows an example of displaying the summary information about all configured VLANs.

Figure 24-1: 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 24-1: 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 24-2: 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:
 LLDP Forwarding:       UDLD 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:
 GSRP ID:      GSRP VLAN group:    L3:
 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 24-3: 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:
  LLDP Forwarding:       UDLD 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
  AXRP Virtual-Link-VLAN
  GSRP ID:      GSRP VLAN group:    L3:
  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 24-4: 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:
  LLDP Forwarding:       UDLD Forwarding:
  Router Interface Name:VLAN0003
  VRF:3
  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:
  GSRP ID:      GSRP VLAN group:    L3:
  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 24-2: 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
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.
LLDP Forwarding	LLDP forwarding	Blank: No IP address has been set. On: The LLDP forwarding function is being used.
UDLD Forwarding	UDLD forwarding	Blank: No IP address has been set. On: The UDLD forwarding function is being used.
Router Interface Name	Interface name	Displays the name of the interface assigned to the VLAN.
VRF [SL-L3A]	VRF ID	This item is displayed only when VRF is assigned to the VLAN interface.
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. VLAN: The MAC address of each VLAN is used.

Item	Meaning	Displayed detailed information
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.)
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.
AXRP Virtual-Link-VLAN	The VLAN is a virtual link VLAN for the Ring Protocol function.	This item is displayed when the VLAN is assigned to the virtual link VLAN for the Ring Protocol function.
GSRP ID	GSRP ID	Blank: The setting for this item does not exist. Alternatively, no VLAN group is assigned when the function limiting GSRP control to VLANs in VLAN groups is used.
GSRP VLAN group	GSRP VLAN group ID	Blank: The setting for this item does not exist. Alternatively, no VLAN group is assigned when the function limiting GSRP control to VLANs in VLAN groups is used. --: No VLAN group has been assigned.
L3	Layer 3 redundancy switching function	Blank: The setting for this item does not exist. Alternatively, no VLAN group is assigned when the function limiting GSRP control to VLANs in VLAN groups is used. On: The layer 3 redundancy switching function is being used.
Virtual MAC Address	Virtual MAC address	The virtual MAC address used for the layer 3 redundancy switching function is displayed.
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 24-3: 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

Item	Meaning	Displayed detailed information
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 24-4: 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 32 (1 to 52 if a stack configuration is used). 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. 　(GSRP): Data forwarding has been stopped by GSRP. 　(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
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 24-5: 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)
     GSRP GSRP ID:VLAN Group ID(M:Master/B:Backup)
     S:IGMP/MLD snooping  T:Tag Translation
     4:IPv4 address configured  6:IPv6 address configured
>
```

Figure 24-6: Example of displaying the VLAN information in list format (when GSRP is used)

```
> show vlan list
Date 20XX/11/15 17:01:40 UTC
VLAN counts:2
Number of VLAN ports:8
ID  Status  Fwd/Up /Cfg Name         Type  Protocol       Ext.  IP
   1 Up        2/ 2/  2 VLAN0001      Port  GSRP 100:  1(M) - - - 4
   3 Down      0/ 2/  6 VLAN0003      Port  GSRP 100:  2(B) - - T 4/6
     AXRP (C:Control-VLAN)
     GSRP GSRP ID:VLAN Group ID(M:Master/B:Backup)
     S:IGMP/MLD snooping  T:Tag Translation
     4:IPv4 address configured  6:IPv6 address configured
>
```

Figure 24-7: 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)
     GSRP GSRP ID:VLAN Group ID(M:Master/B:Backup)
     S:IGMP/MLD snooping  T:Tag Translation
     4:IPv4 address configured  6:IPv6 address configured
>
```

Figure 24-8: 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)
     GSRP GSRP ID:VLAN Group ID(M:Master/B:Backup)
     S:IGMP/MLD snooping  T:Tag Translation
     4:IPv4 address configured  6:IPv6 address configured
>
```

Display items in Example 3

Table 24-5: Display items for the VLAN information in list format

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.)

Item	Meaning	Displayed detailed information
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, GSRP information, Ring Protocol information	For STP:
		  STP <type>:<protocol>
		  <type>: Single, PVST+, or MSTP
		  <protocol>: 802.1D, 802.1w, or 802.1s
		For GSRP:
		  GSRP <GSRP ID>:<VLAN Group ID> (M/B) (If no VLAN group is assigned when the function limiting GSRP control to VLANs in VLAN groups is enabled, a hyphen (-) is displayed, and the subsequent items are not displayed.)
		• <GSRP ID>: GSRP group ID
		• <VLAN Group ID>: VLAN group ID (If no VLAN group is assigned, a hyphen (-) is displayed.)
		• (M): Master
		• (B): Backup
		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.

Item	Meaning	Displayed detailed information
		-: 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 24-9: 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 24-6: 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

Response messages

Table 24-7: List of response messages for the show vlan command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to GSRP.	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.

Message	Description
Connection failed to L2 Manager.	Communication with the L2Manager program failed. Re-execute the command. If this message is output frequently, execute the "restart vlan" command to restart the L2Manager program.
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.
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 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.

Notes

1. Be careful if the "switchport mac" configuration command with the vlan parameter specified has not been executed for MAC ports that are placed in dynamic VLAN mode for Web authentication or MAC-based authentication. If this happens, the "show vlan" command displays the VLAN information for the terminals that have been authorized and unauthorized in all MAC VLANs that are set.

2. When a port receives frames from a terminal that has not yet been authenticated, the port learns the MAC address of the terminal. However, the port can send frames only to authenticated terminals.

3. If the "vxlan-vni" configuration command is set for a VLAN, the VLAN will be in disable status. [SL-L3A]

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.

Operation when a stack configuration is used

This command is not supported.

Example

The following figures show examples of displaying the information related to MAC VLANs from the information for all configured VLANs.

Figure 24-10: 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 (dot1x)
VLAN ID:200     MAC Counts:1
   0012.e200.1111 (dot1x)
>
```

Figure 24-11: 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 (dot1x)    0012.e200.0004 (dot1x)
VLAN ID:200    MAC Counts:1
 0012.e200.1111 (dot1x)
>
```

Figure 24-12: 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 (dot1x)
>
```

Display items

Table 24-8: 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

Response messages

Table 24-9: List of response messages for the show vlan mac-vlan command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Mac Manager.	Communication with the L2 Mac Manager program failed. Re-execute the command. If this message is output frequently, execute the "restart vlan" command to restart the L2 Mac Manager 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 VLAN.	There are no available VLANs. Make sure the specified parameter is correct, and then try again.

Notes

None

restart vlan

Restarts the VLAN program.

Syntax

```
restart vlan [switch <switch no.>] [mac-manager] [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

switch <switch no.>

> Executes the command on the member switch whose switch number is specified.

> This parameter can be specified only on the master switch when the stack is configured. For the specifiable range of values, see "Specifiable values for parameters".

> Behavior when this parameter is omitted:

>> The command is executed on the local device.

mac-manager

> Restarts the MAC management program, which runs when MAC VLAN is set, that runs with the VLAN program.

> Behavior when this parameter is omitted:

>> The VLAN program is restarted. If the MAC management program is running, it is also restarted.

-f

> Restarts the VLAN program without outputting a restart confirmation message.

> Behavior when this parameter is omitted:

>> A confirmation message is displayed.

core-file

> Outputs the VLAN program's core files when the VLAN 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 VLAN program is restarted.

Operation when a stack configuration is used

Execute the command from the master switch, with the switch number of the member switch that belongs to the stack specified.

You can also use the "remote command" command.

```
remote command <switch no.> restart vlan [mac-manager] [-f] [core-file]
```

Example

Figure 24-13: Restarting the VLAN program

```
> restart vlan
VLAN Program restart OK? (y/n): y
>
```

Figure 24-14: Restarting the VLAN program (with the mac-manager parameter specified)

```
> restart vlan mac-manager
L2 Mac Manager restart OK? (y/n): y
>
```

Figure 24-15: Restarting the VLAN program (with the -f parameter specified)

```
> restart vlan -f
>
```

Display items

None

Impact on communication

All Ethernet interfaces are re-initialized, and the ports that make up the VLAN temporarily become unable to send or receive data.

In addition, if this command is executed for a member switch where the stack function is activated, the member switch restarts. During the restart, communication is temporarily suspended.

Response messages

Table 24-10: List of response messages for the restart vlan command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
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. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

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

  Storage directory: /usr/var/core/

  Core file: nimd.core and L2MacManager.core

  If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

- Because all Ethernet interfaces are re-initialized, statistics are cleared.

- If this command is executed immediately after the "restart unicast" command is executed, the IPv4 or IPv6 route table might be unstable for a few minutes. After you execute the "restart unicast" command, wait at least five minutes, and then execute the "restart vlan" command.

- If this command is executed for a member switch where the stack function is activated, the member switch restarts.

dump protocols vlan

Dumps detailed event trace information and control table information collected by the VLAN 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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} dump protocols vlan
```

Example

Figure 24-16: Taking a VLAN dump

```
> dump protocols vlan
>
```

Display items

None

Impact on communication

None

Response messages

Table 24-11: List of response messages for the dump protocols vlan command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. Re-execute the command.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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.

25 VXLAN

[SL-L3A]

show vxlan

Displays information about VXLAN interfaces.

Syntax

```
show vxlan [interface <vtep id>]
```

Input mode

User mode and administrator mode

Parameters

interface <vtep id>

>Displays VXLAN interface information for the specified VTEP ID.

>For <vtep id>, specify a VTEP ID set by the "interface vxlan" configuration command.

>Behavior when this parameter is omitted:

>>All VXLAN interface information is displayed.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example

Figure 25-1: Displaying the VXLAN interface information

```
> show vxlan
Date 20XX/06/10 10:26:00 UTC
VLAN mapping mode: Standard
VXLAN PMTU: 9216
      Port: 1/0/10
VTEP ID: 1
  Flooding mode      : unicast
  Source IP          : 192.168.1.1
  Destination IP(1)  : 192.168.4.1
  VNI(20)            : 1-10,201-210
VTEP ID: 10
  Flooding mode      : unicast
  Source IP          : 192.168.10.1
  Destination IP(1)  : 192.168.10.4
  VNI(10)            : 101-110
>
```

Display items

Table 25-1: Display items for the VXLAN interface information

Item	Meaning	Displayed detailed information
VLAN mapping mode	Capacity limit when VLAN mapping is enabled	Standard: Not extended Extended: Extended
VXLAN PMTU	PMTU value set for the VXLAN	—
Port	VXLAN PMTU-enabled port	This item is not displayed if VXLAN PMTU has not been set.

Item	Meaning	Displayed detailed information
VTEP ID	VTEP ID	—
Flooding mode	Flooding mode	unicast: Unicast mode (fixed)
Source IP	Source IPv4 address	Displays the source IPv4 address of the VXLAN tunnel. Blank: No IP address has been set.
Destination IP	Destination IPv4 address	Displays the destination IPv4 address of the VXLAN tunnel. The value in parentheses indicates the number of destination IPv4 addresses configured. Blank: No IP address has been set.
VNI	VNI	The value in parentheses indicates the number of VNIs configured. Blank: No IP address has been set.

Impact on communication

None

Response messages

Table 25-2: List of response messages for the show vxlan command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to vxlan program.	Communication with the VXLAN program failed. Re-execute the command. If this message is output frequently, execute the "restart overlay" command to restart the VXLAN program.
Vxlan is not configured.	The VXLAN function is not configured. Check the configuration.

Notes

None

show vxlan vni

Shows VNI information.

Syntax

```
show vxlan vni [<vni list>]
```

Input mode

User mode and administrator mode

Parameters

\<vni list\>

Displays VNI information for the specified VNIs in list format.

For details about how to specify \<vni list\>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

All VNI information is displayed.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example

Figure 25-2: Displaying the VNI information

```
> show vxlan vni
Date 20XX/11/12 14:15:00 UTC
VTEP ID: 1
  VNI: 1          Status: enable
                  Learning: On
    VLAN: 10     Port: 1/0/1,5
  VNI: 10100      Status: enable
                  Learning: Off
    Port    VLAN
    1/0/3   100,Untagged
    1/0/6   100-105,200
    CH:2    2001-2200,4000
  VNI: 16671234  Status: disable
VTEP ID: 20
  VNI: 2          Status: enable
                  Learning: Off
    VLAN: 20     Port: 1/0/2,6
                  CH  : 1,14
>
```

Display items

Table 25-3: Display items for the VNI information

Item	Meaning	Displayed detailed information
VTEP ID	VTEP ID	—
VNI	VNI	If multiple VNIs are registered, they are displayed starting with the smallest number.

Item	Meaning	Displayed detailed information
Status	VNI status	enable: The VNI is enabled as a VXLAN Access port. disable: The VNI is not enabled as a VXLAN Access port.
Learning	Status of MAC address learning	On: MAC address learning is enabled. Off: MAC address learning is disabled.

VLAN	VLAN belonging to the VNI	When a VNI is configured on a VLAN basis:
		    The VLAN is displayed.
		When a VNI is configured on a subinterface basis:
		    A VLAN list and Untagged are displayed.

Port	VXLAN Access port	When a VNI is configured on a VLAN basis:
		    A port list is displayed.
		When a VNI is configured on a subinterface basis:
		    A port number for which the subinterface is configured is displayed.

CH	VXLAN Access channel group	When a VNI is configured on a VLAN basis:
		    A channel group list is displayed. This item is not displayed if the channel group has not been set.
		When a VNI is configured on a subinterface basis:
		    A channel group number for which the subinterface is configured is displayed. This item is not displayed if the channel group has not been set.

Impact on communication

None

Response messages

Table 25-4: List of response messages for the show vxlan vni command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to vxlan program.	Communication with the VXLAN program failed. Re-execute the command. If this message is output frequently, execute the "restart overlay" command to restart the VXLAN program.
Specified vni is not configured.	The specified VNI has not been configured.
Vxlan is not configured.	The VXLAN function is not configured. Check the configuration.

Notes

None

show vxlan peers

Shows VTEP peer information.

Syntax

```
show vxlan peers [interface <vtep id>] [destination-ip <ip address>]
```

Input mode

User mode and administrator mode

Parameters

interface <vtep id>

> Displays the VTEP peer information for the specified VTEP ID.
>
> For <vtep id>, specify a VTEP ID set by the "interface vxlan" configuration command.
>
> Behavior when this parameter is omitted:
>
> > The VTEP peer information about all VTEP IDs is displayed.

destination-ip <ip address>

> Displays the VTEP peer information about the destination IPv4 address of the specified VXLAN tunnel.
>
> For <ip address>, specify the destination IPv4 address set by the "destination-ip" configuration command.
>
> Behavior when this parameter is omitted:
>
> > The VTEP peer information for all destination IPv4 addresses is displayed.

Behavior when all parameters are omitted:

> All VTEP peer information is displayed.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example

Figure 25-3: Displaying the VTEP peer information

```
> show vxlan peers
Date 20XX/10/29 11:33:50 UTC
VTEP ID: 1   Source IP: 192.168.1.1
  Destination IP   Status   Nexthop          VRF
  192.168.30.1     Up       192.168.10.1     global
  192.30.1.21      Down     -                -
  192.168.110.1    Up       192.168.100.1    10
VTEP ID: 2   Source IP: 192.168.2.1
  Destination IP   Status   Nexthop          VRF
  192.168.50.1     Up       192.168.20.1     20
>
```

Notes

> For a multipath route, only the Status, Nexthop, and VRF are displayed for the second and subsequent paths.

Display items

Table 25-5: Display items of the VTEP peer information

Item	Meaning	Displayed detailed information
VTEP ID	VTEP ID	—
Source IP	Source IPv4 address	Displays the source IPv4 address of the VXLAN tunnel. Blank: No IP address has been set.
Destination IP	Destination IPv4 address	Displays the destination IPv4 address of the VXLAN tunnel. This item is not displayed if it is not set or if the route is a multipathed route.
Status	Peer status	Displays the configuration status of the VXLAN tunnel. Up: The VXLAN tunnel has been configured. Down: The VXLAN tunnel has not been configured.
Nexthop	Next hop of the destination IPv4 address	-: The next hop of the destination IPv4 address is not resolved.
VRF	VRF ID	Displays the VRF number. global: Global network -: Status is in Down state

Impact on communication

None

Response messages

Table 25-6: List of response messages for the show vxlan peers command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to vxlan program.	Communication with the VXLAN program failed. Re-execute the command. If this message is output frequently, execute the "restart overlay" command to restart the VXLAN program.
Specified destination-ip is not configured.	The specified destination IPv4 address has not been configured.
Specified vxlan interface is not configured.	The specified VXLAN interface has not been configured.
Vxlan is not configured.	The VXLAN function is not configured. Check the configuration.

Notes

None

show vxlan mac-address-table

Shows VXLAN MAC address table information.

Syntax

```
show vxlan mac-address-table [<mac>] [vni <vni list>] [port <port-list>] [channel-group-number
<channel group list>]
show vxlan mac-address-table [<mac>] [vni <vni list>] [destination-ip <ip address>]
show vxlan mac-address-table learning-counter [vni <vni list>]
```

Input mode

User mode and administrator mode

Parameters

\<mac>

　Displays the information in the VXLAN MAC address table for the specified MAC address.

vni \<vni list>

　Displays the information in the VXLAN MAC address table for the VNIs specified in list format.

　For details about how to specify \<vni list>, see "Specifiable values for parameters".

port \<port list>

　Displays the information in the VXLAN 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 VXLAN 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".

destination-ip \<ip address>

　Displays the VXLAN MAC address table information about the destination IPv4 address of the specified VXLAN tunnel. For \<ip address>, specify the destination IPv4 address set by the "destination-ip" configuration command.

learning-counter [vni \<vni list>]

　Displays the number of learned addresses in the MAC address table for each VNI. For details about how to specify \<vni list>, see "Specifiable values for parameters". If \<vni list> is omitted, the number of learned addresses for all VNIs 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 VXLAN MAC address table information learned on the VNIs is displayed.

Operation when a stack configuration is used

The information in the VXLAN MAC address table of the master switch is automatically synchronized with that of the other member switches.

To execute this command with the learning-counter parameter specified for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} show vxlan mac-address-table learning-counter [vni <vni lis
t>]
```

Example 1

Figure 25-4: Displaying all the VXLAN MAC address table information.

```
> show vxlan mac-address-table
Date 20XX/06/07 20:27:38 UTC
MAC address          VNI  Type     Port     VLAN  Connect
0012.e20f.10d9         1  Dynamic  Access   2001  1/0/17
0012.e20f.10da         1  Dynamic  Network     -  192.168.4.1
0012.e20f.10db         -  Dynamic  -           -  -
>
```

Display items in Example 1

Table 25-7: Display items for the information in the VXLAN MAC address table

Item	Meaning	Displayed detailed information
MAC address	MAC address	—
VNI	VNI	VNI number: 1 to 16777215 -: Learning information is being updated.
Type	Type of MAC address table entry	Dynamic: Entry registered dynamically
Port	Type of VXLAN port	Access: VXLAN Access port Network: VXLAN Network port -: Learning information is being updated.
VLAN	VLAN ID	"-" is displayed in the following cases: • VXLAN Access port with the subinterface VLAN as Untagged • VXLAN Network port
Connect	Port or destination IPv4 address	VXLAN Access port: Port list (switch number/NIF number/port number) VXLAN Network Port: Destination IPv4 address in the VXLAN tunnel -: VNI or Port information is updating learning information.

Example 2

Figure 25-5: Displaying the learning status of the VXLAN MAC address table

```
> show vxlan mac-address-table learning-counter
Date 20XX/12/10 20:00:57 UTC
VNI counts: 4
     VNI  Count
       1      3
     100   1000
     200      0
16671234     90
       -      1
>
```

Display items in Example 2

Table 25-8: Display items for the learning status of the VXLAN MAC address table

Item	Meaning	Displayed detailed information
VNI counts	Number of applicable VNIs	—
VNI	VNI	VNI number: 1 to 16777215 -: Learning information is being up-dated.
Count	Number of current learned entries in the MAC address table through VNI learning	—

Impact on communication

None

Response messages

Table 25-9: List of response messages for the show vxlan mac-address-table command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to vxlan program.	Communication with the VXLAN program failed. Re-execute the command. If this message is output frequently, execute the "restart overlay" command to restart the VXLAN program.
No mac-address-table entry for vni.	There is no information learned on VNIs in the MAC address table.
No operational Port.	There is no port on which this command can be executed. Make sure the specified parameter is correct, and then try again.
No operational vni.	There is no VNI on which this command can be executed. Make sure the specified parameter is correct, and then try again.
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Vxlan is not configured.	The VXLAN function is not configured. Check the configuration.

Notes

1. To display entries in a MAC address table that are not learned on VNIs, execute the "show mac-address-table" command.

clear vxlan mac-address-table

Clears VXLAN MAC address table information.

Syntax

```
clear vxlan mac-address-table [vni <vni list>] [-f]
```

Input mode

User mode and administrator mode

Parameters

vni <vni list>

> Specifies a list of VNIs for which you want to clear the information in the VXLAN MAC address table that have been learned.
>
> For details about how to specify <vni list>, see "Specifiable values for parameters".
>
> Behavior when this parameter is omitted:
>
> > The information in the VXLAN MAC address table learned for all VNIs is cleared.

-f

> Clears the information in the VXLAN MAC address table without displaying a confirmation message.
>
> Behavior when this parameter is omitted:
>
> > A confirmation message is displayed.

Behavior when all parameters are omitted:

> The information in the VXLAN MAC address table learned for all VNIs is cleared.

Operation when a stack configuration is used

The clearing of the information in the VXLAN MAC address table of the master switch is automatically synchronized with the other member switches.

Example

Figure 25-6: Clearing the information in the VXLAN MAC address table when VNIs are specified

```
> clear vxlan mac-address-table vni 10,20
mac-address-table clear OK? (y/n): y
>
```

Figure 25-7: Clearing the information in the VXLAN MAC address table without the confirmation message

```
> clear vxlan mac-address-table vni 10,20 -f
>
```

Display items

None

Impact on communication

Communication through a VXLAN tunnel may temporarily be suspended until MAC addresses are learned for VNIs again.

Response messages

Table 25-10: List of response messages for the clear vxlan mac-address-table command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
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 vxlan program.	Communication with the VXLAN program failed. Re-execute the command. If this message is output frequently, execute the "restart overlay" command to restart the VXLAN program.
No operational vni.	There is no VNI on which this command can be executed.
Vxlan is not configured.	The VXLAN function is not configured. Check the configuration.

Notes

1. To clear entries in a MAC address table that are not learned on VNIs, execute the "clear mac -address-table" command.

show vxlan statistics

Displays VXLAN statistics.

Syntax

```
show vxlan statistics {vni <vni list> | destination-ip <ip address>}
```

Input mode

User mode and administrator mode

Parameters

vni <vni list>

Displays VXLAN statistics for the specified VNI in list format.

For details about how to specify <vni list>, see "Specifiable values for parameters".

destination-ip <ip address>

Displays the VXLAN statistics about the destination IPv4 address of the specified VXLAN tunnel. For <ip address>, specify the destination IPv4 address set by the "destination-ip" configuration command.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show vxlan statistics {vni <vni list> | destination-ip <ip
address>}
```

Example 1

Figure 25-8: Displaying the VXLAN statistics for each VNI

```
>show vxlan statistics vni 16777000-16777215
Date 20XX/11/12 14:15:00 UTC
VTEP ID: 1  VNI: 16777000
          Packets              Octets
  Encap  1073741823        137438953471
  Decap           1                 128
  AcsAcs           0                   0
VTEP ID: 1  VNI: 16777001
          Packets              Octets
  Encap           0                   0
  Decap           0                   0
  AcsAcs           0                   0
VTEP ID: 2  VNI: 16777002
          Packets              Octets
  Encap         125              135871
  Decap         215              287455
  AcsAcs           0                   0
                  :
                  :
```

Display items in Example 1

Table 25-11: Display items of the VXLAN statistics for each VNI

Item	Meaning	Displayed detailed information
VTEP ID	VTEP ID	—
VNI	VNI list	VNIs that are included in the specified tunnel
Packets	Number of packets	—
Octets	The number of octets	Calculation of octet values is based on the range from the MAC header to the FCS field over the frame length.
Encap	Statistics on packets encapsulated in VXLAN frames	Statistics on VXLAN frames received from VXLAN Access ports and sent to VXLAN Network ports
Decap	Statistics on packets decapsulated from VXLAN frames	Statistics on VXLAN frames received from VXLAN Network ports and sent to VXLAN Access ports
AcsAcs	Statistics on packets forwarded between VXLAN Access ports	—

Example 2

Figure 25-9: Displaying the VXLAN statistics for each tunnel

```
>show vxlan statistics destination-ip 192.168.1.1
Date 20XX/11/12 14:15:00 UTC
VTEP ID: 1  Destination IP: 192.168.1.1
  VNI(216): 16777000-16777215
          Packets                Octets
  Encap   1073741823         137438953471
  Decap           1                  128
>
```

Display items in Example 2

Table 25-12: Display items of the VXLAN statistics for each tunnel

Item	Meaning	Displayed detailed information
VTEP ID	VTEP ID	—
Destination IP	Destination IPv4 address	—
VNI (n)	VNI list	n: Number of VNIs VNIs that are included in the specified tunnel
Packets	Number of packets	—
Octets	The number of octets	Calculation of octet values is based on the range from the MAC header to the FCS field over the frame length.
Encap	Statistics on packets encapsulated in VXLAN frames	Statistics on VXLAN frames received from VXLAN Access ports and sent to VXLAN Network ports
Decap	Statistics on packets decapsulated from VXLAN frames	Statistics on VXLAN frames received from VXLAN Network ports and sent to VXLAN Access ports

Impact on communication

None

Response messages

Table 25-13: List of response messages for the show vxlan statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to vxlan program.	Communication with the VXLAN program failed. Re-execute the command. If this message is output frequently, execute the "restart overlay" command to restart the VXLAN program.
No operational vni.	There is no VNI on which this command can be executed.
Specified destination-ip is not configured.	The specified destination IPv4 address has not been configured.
Vxlan is not configured.	The VXLAN function is not configured. Check the configuration.

Notes

1. The table below shows the triggers for counting the VXLAN statistics.

   Note that if this command is executed continuously, it may take several seconds for statistics on the screen to be updated.

   Table 25-14: Count triggers for the VXLAN statistics

Statistics type	Sampled when
VNI-based entry (Encap)	Packets are sent. (When they are sent from a VXLAN Network port.)
VNI-based entry (Decap)	Packets are received. (When they are received at a VXLAN Network port.)
VNI-based entry (AcsAcs)	Packets are sent. (When they are sent from a VXLAN Access port while the VNI belongs to the VTEP.)
Tunnel-based entry (Encap)	Packets are sent. (When they are sent from a VXLAN Network port.)
Tunnel-based entry (Decap)	Packets are received. (When they are received at a VXLAN Network port.)

2. If the VXLAN function is used in a stack configuration, VXLAN statistics are counted only in member switches that have the count triggers.

clear vxlan statistics

Clears VXLAN statistics.

Syntax

```
clear vxlan statistics [vni <vni>] [destination-ip <ip address>]
```

Input mode

User mode and administrator mode

Parameters

vni <vni>

>　Clears VXLAN statistics for the specified VNI.
>
>　The range of values the <vni> option accepts is from 1 to 16777215.
>
>　Behavior when this parameter is omitted:
>
>>　The VXLAN statistics for all VNIs are cleared.

destination-ip <ip address>

>　Clears the VXLAN statistics about the destination IPv4 address of the specified VXLAN tunnel. For <ip address>, specify the destination IPv4 address set by the "destination-ip" configuration command.
>
>　Behavior when this parameter is omitted:
>
>>　The VXLAN statistics for all destination IPv4 addresses are cleared.

Behavior when all parameters are omitted:

>　All VXLAN statistics are cleared.

Operation when a stack configuration is used

The VXLAN statistics are automatically synchronized from the master switch to the other member switches. You can also execute the command with the switch number of the member switch specified.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} clear vxlan statistics
```

Example

Figure 25-10: Clearing the VXLAN statistics
```
> clear vxlan statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 25-15: List of response messages for the clear vxlan statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to vxlan program.	Communication with the VXLAN program failed. Re-execute the command. If this message is output frequently, execute the "restart overlay" command to restart the VXLAN program.
No operational vni.	There is no VNI on which this command can be executed.
Specified destination-ip is not configured.	The specified destination IPv4 address has not been configured.
Specified VNI and destination-ip is not config-ured.	The specified VNI and destination IPv4 address have not been configured.
Vxlan is not configured.	The VXLAN function is not configured. Check the configura-tion.

Notes

None

restart overlay

Restarts the overlay (VXLAN) program.

Syntax

```
restart overlay [-f] [core-flie]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the overlay (VXLAN) program without displaying a 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 confirmation message is output, the overlay (VXLAN) program is restarted.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} restart overlay [-f] [core-file]
```

Example

Figure 25-11: Restarting the overlay (VXLAN) program

```
> restart overlay
overlay program restart OK? (y/n): y
>
```

Figure 25-12: Restarting the overlay (VXLAN) program without the confirmation message

```
> restart overlay -f
>
```

Display items

None

Impact on communication

Ports for which a VXLAN is enabled temporarily become unable to send or receive data.

Response messages

Table 25-16: List of response messages for the restart overlay command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Vxlan doesn't seem to be running.	The VXLAN program is not running. Check the configuration.

Notes

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

   - Storage directory: /usr/var/core/

   - Core file: vxland.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 overlay

Dumps detailed event trace information and control table information collected by the overlay (VXLAN) program to a file.

Syntax

```
dump protocols overlay
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} dump protocols overlay
```

Example

Figure 25-13: Taking an overlay (VXLAN) dump

```
> dump protocols overlay
```

Display items

None

Impact on communication

None

Response messages

Table 25-17: List of response messages for the dump protocols overlay command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Vxlan is not configured.	The VXLAN function is not configured. Check the configuration.

Notes

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

   - Storage directory: /usr/var/vxlan/

   - File: vxland_dump.gz

   If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

26 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>] [virtual-link <link id>]]
[ 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".

virtual-link <link id>

> Displays Spanning Tree information for the specified virtual link ID. Specifiable values for the virtual link ID are in the range from 1 to 250.

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.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example 1

Figure 26-1: 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 26-1: 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	—
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. If a virtual link is used, the port list for the virtual link and the virtual link ID 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, channel group number, or virtual link ID	The port number, channel group number, or virtual link ID 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. If a virtual link is used, this means that at least one virtual link port is in Up status.

Item	Meaning	Displayed detailed information
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. If a virtual link is used, this means that all virtual link ports are 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.
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 26-2: 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:32)
 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:32    Up   Status:Forwarding  Role:Root        LoopGuard
>
```

Display items in Example 2

Table 26-2: 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
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. If a virtual link is used, the port list for the virtual link and the virtual link ID 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, channel group number, or virtual link ID	The port number, channel group number, or virtual link ID of the port for which information is displayed

Item	Meaning	Displayed detailed information
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. If a virtual link is used, this means that at least one virtual link port 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. If a virtual link is used, this means that all virtual link ports are 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.
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 26-3: 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:32)
  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:32    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:32    Up   Status:Forwarding  Role:Master      Boundary
>
```

Display items in Example 3

Table 26-3: 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
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

Item	Meaning	Displayed detailed 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. If a virtual link is used, the port list for the virtual link and the virtual link ID 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.
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	The MAC address of the Switch.

Item	Meaning	Displayed detailed information
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. If a virtual link is used, the port list for the virtual link and the virtual link ID 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.
<switch no.>/<nif no.>/<port no.>	Port number, channel group number, or virtual link ID	The port numbers, channel group numbers, or virtual link IDs of the ports for which information is displayed

Item	Meaning	Displayed detailed information
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. If a virtual link is used, this means that at least one virtual link port 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. If a virtual link is used, this means that all virtual link ports are 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 26-4: 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 26-4: 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 BP-DUs	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.

Item	Meaning	Displayed detailed information
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. If a virtual link is used, the port list for the virtual link and the virtual link ID are displayed. A hyphen (-) is displayed if the Switch is the root bridge.
Max Age	Maximum valid time of BP-DUs 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, channel group number, or virtual link ID	The port number, channel group number, or virtual link ID 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. If a virtual link is used, this means that at least one virtual link port 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. If a virtual link is used, this means that all virtual link ports are 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.

Item	Meaning	Displayed detailed information
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 5

Figure 26-5: 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:32)
    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:32 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 26-5: 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
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. If a virtual link is used, the port list for the virtual link and the virtual link ID are displayed. A hyphen (-) is displayed if the Switch is the root bridge.

Item	Meaning	Displayed detailed information
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, channel group number, or virtual link ID	The port number, channel group number, or virtual link ID 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. If a virtual link is used, this means that at least one virtual link port 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. If a virtual link is used, this means that all virtual link ports are 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: 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.

Item	Meaning	Displayed detailed information
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.
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

Item	Meaning	Displayed detailed information
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 BP-DUs	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 26-6: 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:32)
 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:32  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:32  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 26-6: 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. If a virtual link is used, the port list for the virtual link and the virtual link ID 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

Item	Meaning	Displayed detailed information
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).
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.

Item	Meaning	Displayed detailed 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 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 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. If a virtual link is used, the port list for the virtual link and the virtual link ID 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.

Item	Meaning	Displayed detailed information
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.
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, channel group number, or virtual link ID	The port numbers, channel group numbers, or virtual link IDs of the ports 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. If a virtual link is used, this means that at least one virtual link port 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. If a virtual link is used, this means that all virtual link ports are 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.

Item	Meaning	Displayed detailed information
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.
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.

Item	Meaning	Displayed detailed information
		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
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\>

Item	Meaning	Displayed detailed information
		\<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

Response messages

Table 26-7: List of response messages for the show spanning-tree command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Spanning Tree program.	Communication with the Spanning Tree program failed.
No corresponding port information.	No port and channel group information exists as Spanning Tree information.
Spanning Tree is not configured.	The spanning Tree Protocol has not been configured. Check the configuration.
Specified Spanning Tree is not configured.	The specified Spanning Tree Protocol has not been configured. Check the configuration.

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>] [virtual-link <
link id>]]
```

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".

virtual-link <link id>

> Displays Spanning Tree statistics for the specified virtual link ID. Specifiable values for the virtual link ID are in the range from 1 to 250.

Behavior when all parameters are omitted:

> Displays statistics about Single Spanning Tree, PVST+, and Multiple Spanning Tree.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example 1

Figure 26-7: 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 26-8: 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 26-8: 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	—
VL	Virtual link ID	—
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. If a virtual link is used, this means that at least one virtual link port 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. If a virtual link is used, this means that all virtual link ports are in Down status.
Forward Transit Times	Number of transitions to the forwarding status	—
TxBPDUs	Number of sent BPDUs	—

Item	Meaning	Displayed detailed information
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 26-9: 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:32      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:32      Up
       TxBPDUs              :        2  RxBPDUs          :         15
       Forward Transit Times:        2  Discard Message:         0
       Exceeded Hop         :        0
>
```

Display items in Example 2

Table 26-9: Display Items of the Multiple Spanning Tree statistics

Item	Meaning	Displayed detailed information
MST Instance ID	Instance ID of the applicable MST instance	—
Topology ChangeTimes	Number of topology changes detected	—
Port	Port number	—
ChGr	Channel group number	—
VL	Virtual link ID	—
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. If a virtual link is used, this means that at least one virtual link port 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. If a virtual link is used, this means that all virtual link ports are 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)

Item	Meaning	Displayed detailed information
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.
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

Response messages

Table 26-10: List of response messages for the show spanning-tree statistics command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Spanning Tree program.	Communication with the Spanning Tree program 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.

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>] [virtual-link
<link id>]]
```

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".

virtual-link <link id>

> Clears statistics about the Spanning Tree Protocols for the specified virtual link ID. Specifiable values for the virtual link ID are in the range from 1 to 250.

Behavior when all parameters are omitted:

> Statistics about all Spanning Tree Protocols are cleared.

Operation when a stack configuration is used

The command can clear information only from the master switch.

Example

Figure 26-10: Clearing all the Spanning Tree statistics

```
> clear spanning-tree statistics
>
```

Figure 26-11: Clearing the Single Spanning Tree statistics

```
> clear spanning-tree statistics single
>
```

Figure 26-12: Clearing the Multiple Spanning Tree statistics

```
>clear spanning-tree statistics mst
>
```

Display items

None

Impact on communication

None

Response messages

Table 26-11: List of response messages for the clear spanning-tree statistics command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Spanning Tree program.	Communication with the Spanning Tree program failed.

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.

Operation when a stack configuration is used

The command can be executed only on the master switch.

Example

The following figure shows an example of forcing recovery of STP-compatible mode for Spanning Tree Protocols.

Figure 26-13: Forcibly recovering the STP-compatible mode for Spanning Tree Protocols

```
> clear spanning-tree detected-protocol
```

>

Display items

None

Impact on communication

None

Response messages

Table 26-12: List of response messages for the clear spanning-tree detected-protocol command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Spanning Tree program.	Communication with the Spanning Tree program failed.

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.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example 1

The following shows an example of displaying the number of VLANs handled by PVST+.

Figure 26-14: 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 26-13: 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 26-15: 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 26-14: 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 26-16: 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 26-15: 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

Response messages

Table 26-16: List of response messages for the show spanning-tree port-count command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Spanning Tree program.	Communication with the Spanning Tree program failed.
Spanning Tree is not configured.	The spanning Tree Protocol has not been configured. Check the configuration.
Specified Spanning Tree is not configured.	The specified Spanning Tree Protocol has not been configured. Check the configuration.

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} restart spanning-tree [-f] [core-file]
```

Example

Figure 26-17: 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 temporarily become unable to send or receive data.

Response messages

Table 26-17: List of response messages for the restart spanning-tree command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Spanning Tree program failed to be restarted.	The command could not restart the Spanning Tree program. Re-execute the command.

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

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} dump protocols spanning-tree
```

Example

Figure 26-18: Example of taking a Spanning Tree dump

```
> dump protocols spanning-tree
>
```

Display items

None

Impact on communication

None

Response messages

Table 26-18: List of response messages for the dump protocols spanning-tree command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

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.

27 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.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example 1

The following figures show examples of displaying the summary information about the Ring Protocol.

Figure 27-1: Example of displaying the summary information about the Ring Protocol

```
> show axrp
Date 20XX/01/26 12:00:00 UTC

Total Ring Counts:4

Ring ID:1
 Name:RING#1
 Oper State:enable          Mode:Master     Attribute:-
 MAC Clear Mode:system

 VLAN Group ID  Ring Port  Role/State             Ring Port  Role/State
 1              1/0/1      primary/forwarding     1/0/2      secondary/blocking
 2              1/0/1      secondary/blocking     1/0/2      primary/forwarding

Ring ID:2
 Name:RING#2
 Oper State:enable          Mode:Transit    Attribute:-
 MAC Clear Mode:system

 VLAN Group ID  Ring Port  Role/State             Ring Port  Role/State
 1              1(ChGr)    -/forwarding           2(ChGr)    -/forwarding
 2              1(ChGr)    -/forwarding           2(ChGr)    -/forwarding

Ring ID:3
```

```
Name:
Oper State:disable        Mode:-          Attribute : -
MAC Clear Mode:-

VLAN Group ID  Ring Port  Role/State              Ring Port  Role/State
1              -          -/-                     -          -/-
2              -          -/-                     -          -/-

Ring ID:4
 Name:RING#4
 Oper State:enable        Mode:Transit    Attribute:rift-ring-edge(1)
 MAC Clear Mode:-
 Shared Edge Port:1/0/3

 VLAN Group ID  Ring Port  Role/State              Ring Port  Role/State
 1              1/0/3      -/-                     1/0/4      -/forwarding
 2              1/0/3      -/-                     1/0/4      -/forwarding
>
```

Figure 27-2: Example of displaying the summary information about the Ring Protocol when a ring ID is specified

```
> show axrp 1
Date 20XX/01/26 12:00:00 UTC

Total Ring Counts:1

Ring ID:1
 Name:RING#1
 Oper State:enable        Mode:Master     Attribute:-
 MAC Clear Mode:system

 VLAN Group ID  Ring Port  Role/State          Ring Port  Role/State
 1              1/0/1      primary/forwarding  2/0/2      secondary/blocking
 2              1/0/1      secondary/blocking  2/0/2      primary/forwarding
>
```

Display items in Example 1

Table 27-1: Displayed items of the summary information about the Ring Protocol

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	Master: Master node Transit: Transit node
Attribute	In a multi-ring configuration, the attribute of the Switch in a shared link non-monitoring ring	rift-ring: Master node in a shared link non-monitoring ring rift-ring-edge (1): Terminal node having an edge node ID of 1 in a shared link non-monitoring ring (both master and transit nodes can have this attribute)

Item	Meaning	Displayed information
		rift-ring-edge (2): Terminal node having an edge node ID of 2 in a shared link non-monitoring ring (both master and transit nodes can have this attribute) -: 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 Edge Port	Port number on the shared-link side of the terminal node in a shared link non-monitoring ring	Physical port number (switch number/NIF number/port number) or channel group number (ChGr) Note: This item is displayed only for the terminal nodes in a shared link non-monitoring ring. However, if "Not Operating" or a hyphen (-) is displayed for "Oper State", the value that has been set is displayed regardless of the node type.
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) Note: This item is displayed only for transit nodes on a shared link. However, if "Not Operating" or a hyphen (-) is displayed for "Oper State", the value that has been set is displayed regardless of the node type.
VLAN Group ID	Data transfer VLAN group ID	1 to 2
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	primary: Primary port secondary: Secondary port Note: A hyphen (-) is displayed for nodes other than the master node on which the Ring Protocol function is enabled.
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.

Example 2

The following figure shows an example of displaying the detailed Ring Protocol information.

Figure 27-3: Example of displaying the detailed Ring Protocol information

```
> show axrp detail
Date 20XX/03/10 12:00:00 UTC

Total Ring Counts:4

Ring ID:1
 Name:RING#1
 Oper State:enable          Mode:Master      Attribute:-
 MAC Clear Mode:system
 Control VLAN ID:5          Ring State:normal
 Health Check Interval  (msec):1000
 Health Check Hold Time (msec):3000
 Preempt Delay Time      (sec):-
 Flush Request Counts:3
 Flush Request Transmit VLAN ID:12
```

```
 Forwarding Shift Time (sec):10

 VLAN Group ID:1
  VLAN ID:6-10,12
  Ring Port:1/0/1        Role:primary      State:forwarding
  Ring Port:1/0/2        Role:secondary    State:blocking

 VLAN Group ID:2
  VLAN ID:16-20,22
  Ring Port:1/0/1        Role:secondary    State:blocking
  Ring Port:1/0/2        Role:primary      State:forwarding

 Last Transition Time:20XX/10/05 10:00:00
 Fault Counts    Recovery Counts   Total Flush Request Counts
 1              1                 12

Multi Fault Detection State:normal
 Mode:monitoring    Backup Ring ID:4
 Control VLAN ID:100
 Multi Fault Detection Interval  (msec):1000
 Multi Fault Detection Hold Time (msec):3000

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

Ring ID:3
 Name:
 Oper State:disable        Mode:-         Attribute : -
 MAC Clear Mode:-
 Control VLAN ID:-

 VLAN Group ID:1
  VLAN ID:-
  Ring Port:-          Role:-          State:-
  Ring Port:-          Role:-          State:-

 VLAN Group ID:2
  VLAN ID:-
  Ring Port:-          Role:-          State:-
  Ring Port:-          Role:-          State:-

Ring ID:4
 Name:RING#4
 Oper State:enable         Mode:Transit    Attribute:rift-ring-edge(1)
 MAC Clear Mode:-
 Shared Edge Port:1/0/3
 Control VLAN ID:45
 Health Check Interval  (msec):1000
 Forwarding Shift Time (sec):10
 Last Forwarding:flush request receive

 VLAN Group ID:1
  VLAN ID:46-50,52
  Ring Port:1/0/3      Role:-          State:-
  Ring Port:1/0/4      Role:-          State:forwarding

 VLAN Group ID:2
  VLAN ID:56-60,62
  Ring Port:1/0/3      Role:-          State:-
  Ring Port:1/0/4      Role:-          State:forwarding
>
```

Display items in Example 2

Table 27-2: 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	Master: Master node Transit: Transit node
Attribute	In a multi-ring configuration, the attribute of the Switch in a shared link non-monitoring ring	rift-ring: Master node in a shared link non-monitoring ring rift-ring-edge (1): Terminal node having an edge node ID of 1 in a shared link non-monitoring ring (both master and transit nodes can have this attribute) rift-ring-edge (2): Terminal node having an edge node ID of 2 in a shared link non-monitoring ring (both master and transit nodes can have this attribute) -: 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 Edge Port	Port number on the shared-link side of the terminal node in a shared link non-monitoring ring	Physical port number (switch number/NIF number/port number) or channel group number (ChGr) Note: This item is displayed only for the terminal nodes in a shared link non-monitoring ring. However, if "Not Operating" or a hyphen (-) is displayed for "Oper State", the value that has been set is displayed regardless of the node type.
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) Note: This item is displayed only for transit nodes on a shared link. However, if "Not Operating" or a hyphen (-) is displayed for "Oper State", the value that has been set is displayed regardless of the node type.
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) (This item is displayed only for transit nodes.)

Item	Meaning	Displayed information
Ring State	Status of the ring	normal: Normal fault: A failure has occurred. preempt delay: Path switchback suppression is enabled. monitoring recovery: Recovery is being monitored. Note: This item is displayed only for the master node. However, if the Ring Protocol function is not enabled, a hyphen (-) is displayed.
Health Check Interval	Value of the health-check frame sending interval timer	200 to 60000 (milliseconds) 5 to 60000 (milliseconds) [SL-L3A] Note: This item is displayed for the master node and terminal nodes in a shared link non-monitoring ring.
Health Check Hold Time	Time period during which a health-check frame is not received but the judgment that a failure occurred is suppressed	500 to 300000 (milliseconds) 15 to 300000 (milliseconds) [SL-L3A] (This item is displayed only for the master node.)
Preempt Delay Time	Time required to complete a switchback action when path switchback suppression is enabled.	1 to 3600 (seconds), or infinity. If path switchback suppression is disabled, a hyphen (-) is displayed. Note: This item is displayed only for the master node. However, this item is not displayed if no value has been set.
Flush Request Counts	Number of times a flush control frame was sent	1 to 10 (This item is displayed only for the master node.)
Flush Request Transmit VLAN ID	When a failure occurs in a ring or the failure is corrected, the ID of the VLAN from which neighboring-ring flush control frames are to be sent to the devices in the neighboring ring	1 to 4094 (This item is displayed only for the master node.)
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. (This item is displayed only for transit nodes.)
VLAN Group ID	Data transfer VLAN group ID	1 to 2
Ring Port	Ring port number	Physical port number (switch number/NIF number/port number) or channel group number (ChGr)
VLAN ID	Data transfer VLAN ID	1 to 4094
Role	The role of the ring port	primary: Primary port secondary: Secondary port Note: A hyphen (-) is displayed for nodes other than the master node on which the Ring Protocol function is enabled.

Item	Meaning	Displayed information
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.
Last Transition Time	Time that the failure or recovery monitoring status changed last	yyyy/mm/dd hh:mm:ss UTC: Year, month, day, hour, minute, second, and time zone (This item is displayed only for the master node.)
Fault Counts	Number of times a failure was detected (statistics)	0 to 4294967295 (This item is displayed only for the master node.)
Recovery Counts	Number of times recovery was detected (statistics)	0 to 4294967295 (This item is displayed only for the master node.)
Total Flush Request Counts	Total number of times a flush control frame was sent (statistics)	0 to 4294967295 (This item is displayed only for the master node.)
Multi Fault Detection State	Multi-fault monitoring is enabled	normal: Normal fault: Multiple faults have occurred. (This item is displayed if the multi-fault monitoring function is enabled. If a hyphen (-) is displayed, it means that either multi-fault monitoring has not yet started when the monitoring mode is monitoring or that the monitoring mode is transport.)
Mode	Multi-fault monitoring mode	monitoring: monitor-enable transport: transport-only (This item is displayed if the multi-fault monitoring function is enabled. - is displayed when the monitoring mode is not set.)
Backup Ring ID	Backup ring ID	1 to 65535 (This item is displayed only when the monitoring mode is monitoring.)
Control VLAN ID	ID of the VLAN used for multi-fault monitoring	2 to 4094 (This item is displayed if the multi-fault monitoring VLAN is set.) - is displayed when this item is not set.)
Multi Fault Detection Interval	Value of the timer for the multi-fault monitoring frame sending interval	500 to 60000 (milliseconds) (This item is displayed only when the monitoring mode is monitoring.)
Multi Fault Detection Hold Time	Time period during which a multi-fault monitoring frame is not received but the judgment that multiple faults occurred is suppressed	1000 to 300000 (milliseconds) (This item is displayed only when the monitoring mode is monitoring.)

Impact on communication

None

Response messages

Table 27-3: List of response messages for the show axrp command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
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.
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.
Specified Ring ID is not configured:<ring id>.	The specified ring ID has not been configured. <ring id>: Ring ID

Notes

The counter values for statistics do not increment when the upper limit is reached.

In a stack configuration, the statistics is cleared when the master switch is switched over. Also, it may take some time before the Ring State and State items show their respective states correctly after the switching.

clear axrp

Clears Ring Protocol statistics.

Syntax

```
clear axrp [<ring id list>]
```

Input mode

User mode and administrator mode

Parameters

\<ring id list>

Specify a list of ring IDs for which you want to clear all Ring Protocol statistics. 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.

Behavior when all parameters are omitted:

All Ring Protocol statistics are cleared.

Operation when a stack configuration is used

The command can clear information only from the master switch.

Example

Figure 27-4: Example of clearing all the Ring Protocol statistics

```
> clear axrp
>
```

Figure 27-5: Example of clearing all the Ring Protocol statistics with a ring ID specified

```
> clear axrp 1
>
```

Display items

None

Impact on communication

None

Response messages

Table 27-4: List of response messages for the clear axrp command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
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.
Specified Ring ID is not configured:<ring id>.	The specified ring ID has not been configured. <ring id>: Ring ID

Notes

- Even if statistics are cleared, the value for the MIB information obtained by using SNMP is not cleared.

- If the configuration is deleted or added, the target statistics are cleared to zero.

clear axrp preempt-delay

Clears the path switchback suppression status for the master node.

Syntax

```
clear axrp preempt-delay <ring id> [-f]
```

Input mode

User mode and administrator mode

Parameters

<ring id>

Specify the ID of the ring whose path switchback suppression status you want to clear.

The specifiable values are from 1 to 65535.

-f

Clears the path switchback suppression status without outputting any messages.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Operation when a stack configuration is used

The path switchback suppression status for the master node can be cleared by the master switch only.

Example

Figure 27-6: Example of executing the clear axrp preempt-delay command

```
>clear axrp preempt-delay 1
Fault recovery process restore OK? (y/n) :y
>
```

Figure 27-7: Example of executing the clear axrp preempt-delay command (with the -f parameter specified)

```
>clear axrp preempt-delay 1 -f
>
```

Display items

None

Impact on communication

If this command is executed on a ring for which path switchback suppression is enabled, the suppression is disabled and path switchbacking is performed. At this time, the VLANs that belong to the VLAN group for the ring become unable to receive frames temporarily.

Response messages

Table 27-5: List of response messages for the clear axrp preempt-delay command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
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.
Ring Protocol is not configured.	The Ring Protocol has not been configured. Check the configuration.
Specified Ring ID is not configured:<ring id>.	The specified ring ID has not been configured. <ring id>: Ring ID
Specified Ring ID is not preempt delay state:<ring id>	Path switchback suppression is not enabled for the specified ring. <ring id>: Ring ID

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} restart axrp [-f] [core-file]
```

Example

Figure 27-8: Example of restarting the Ring Protocol program

```
> restart axrp
axrp program restart OK? (y/n):y
>
```

Figure 27-9: 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.

Response messages

Table 27-6: List of response messages for the restart axrp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Ring Protocol doesn't seem to be running.	The Ring Protocol program is not running. Check the configuration.
Ring Protocol program failed to be restarted.	This command could not restart the Ring Protocol program. Re-execute the command.

Notes

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

Storage directory: /usr/var/core/

Core file (standalone): axrpd_rapid.core

Core file (stack): 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

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} dump protocols axrp
```

Example

The following figure shows an example of taking a Ring Protocol dump.

Figure 27-10: Example of taking a Ring Protocol dump

```
> dump protocols axrp
>
```

Display items

None

Impact on communication

None

Response messages

Table 27-7: List of response messages for the dump protocols axrp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

Message	Description
Ring Protocol doesn't seem to be running.	The Ring Protocol program is not running. Check the configuration.

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.

28 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)

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>]
```

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". However, range specification with an asterisk (*) is not possible.

    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.

Operation when a stack configuration is used

When both IPv4 multicast and IGMP snooping are used together, commands can be executed only on the master switch.

Example 1

Figure 28-1: Displaying the IGMP snooping information

```
> show igmp-snooping
Date 20XX/04/10 15:20:00 UTC
VLAN counts: 2
VLAN: 100
  VRF: 2
  Querier: enable
  IP address          : 192.168.11.20
    IGMP querying system: 192.168.11.20
    Querier version: V3
    Query interval : 125
  IP address(secondary) : 192.168.20.10
    IGMP querying system: 192.168.20.5
    Querier version: V3
    Query interval : 60
  IP address(secondary) : 192.168.30.10
    IGMP querying system: 192.168.30.10
    Querier version: V2
    Query interval : 125
  IP address(secondary) : 192.168.40.10
    IGMP querying system: 192.168.40.5
    Querier version: V2
    Query interval : -
  IPv4 Multicast routing: On
  Fast-leave: On
  Port(5): 1/0/1-5
  Mrouter-port: 1/0/1,3
  Group counts: 3
VLAN: 200
  Querier: disable
  IP address          :
    IGMP querying system:
    Querier version: V2
    Query interval : 125
  IPv4 Multicast routing: Off
  Fast-leave: Off
  Port(4): 1/0/6-9
  Mrouter-port: 1/0/6
  Group counts: 0
>

> show igmp-snooping 100
Date 20XX/04/10 15:21:00 UTC
VLAN: 100
  VRF: 2
  Querier: enable
  IP address          : 192.168.11.20
    IGMP querying system: 192.168.11.20
    Querier version: V3
    Query interval : 125
  IP address(secondary) : 192.168.20.10
    IGMP querying system: 192.168.20.5
    Querier version: V3
    Query interval : 60
  IP address(secondary) : 192.168.30.10
    IGMP querying system: 192.168.30.10
    Querier version: V2
    Query interval : 125
  IP address(secondary) : 192.168.40.10
    IGMP querying system: 192.168.40.5
    Querier version: V2
    Query interval : -
  IPv4 Multicast routing: On
  Fast-leave: Off
  Port(5): 1/0/1-5
  Mrouter-port: 1/0/1,3
  Group counts: 3
>
```

Display items in Example 1

Table 28-1: 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	—
VRF [SL-L3A]	VRF ID	This item is displayed only when VRF is assigned to the VLAN interface.
Querier	Whether the querier function has been set	enable: The function has been set. disable: The function has not been set.
IP address	IP address	Blank: No IP address has been set.
IP address(secondary)	Secondary IP address	This item is displayed only when the secondary IP address is configured.
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
Query interval	Sending interval for IGMP Query messages (seconds)	Sending interval for IGMP Query messages in the applicable network - is displayed when Querier version is V2 and this device is not a querier.
IPv4 Multicast routing	Whether IPv4 multicast routing has been set for the VLAN	On: Multicast routing has been set. Off: Multicast routing has not been set.
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
Mrouter-port	Multicast router ports	—
Group counts	Number of multicast groups in the VLAN	—

Example 2

Figure 28-2: 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  IPv4 Multicast routing: Off
  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  IPv4 Multicast routing: On
  Group Address     MAC Address         Version      Mode
```

```
  239.168.10.5     0100.5e28.0a05     -           -
    Port-list:1/0/4,6
  239.192.20.6     0100.5e40.1406     -           -
    Port-list:1/0/2-4
>
> show igmp-snooping group 100
Date 20XX/01/15 15:20:00 UTC
VLAN counts: 1
VLAN: 100  Group counts: 3  IPv4 Multicast routing: Off
  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     V1,V2,V3    EXCLUDE
    Port-list:1/0/1-2
  239.192.1.1      0100.5e40.0101     V1,V2       -
    Port-list:1/0/1
>

> show igmp-snooping group 224.10.10.10
Date 20XX/01/15 15:20:00 UTC
VLAN counts: 2
VLAN: 100  Group counts: 1  IPv4 Multicast routing: Off
  Group Address    MAC Address        Version     Mode
  224.10.10.10     0100.5e0a.0a0a     V2          -
    Port-list:1/0/1-3
VLAN: 300  Group counts: 1  IPv4 Multicast routing: On
  Group Address    MAC Address        Version     Mode
  224.10.10.10     0100.5e0a.0a0a     -           -
    Port-list:1/0/4,6
>
> show igmp-snooping group 224.10.10.10 100
Date 20XX/01/15 15:20:00 UTC
VLAN counts: 1
VLAN: 100  Group counts: 1  IPv4 Multicast routing: Off
  Group Address    MAC Address        Version     Mode
  224.10.10.10     0100.5e0a.0a0a     V2          -
    Port-list:1/0/1-3
>
```

Display items in Example 2

Table 28-2: 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	—
IPv4 Multicast routing	Whether IPv4 multicast routing has been set for the VLAN	On: Multicast routing has been set. Off: Multicast routing has not been set.
Group Address	Subscription group addresses	—
MAC Address	Learned MAC addresses	—

Item	Meaning	Displayed detailed information
Version	IGMP version information	V1: IGMP Version 1 V2: IGMP Version 2 V3: IGMP Version 3 If IPv4 Multicast routing is On, a hyphen (-) is displayed. In this case, to check the IGMP version information, use the "show ip igmp group" command. 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.
Mode	Group mode	INCLUDE: INCLUDE mode EXCLUDE: EXCLUDE mode If the IGMP version information does not include V3 or if IPv4 Multicast routing is On, "-" is displayed. If IPv4 Multicast routing is On, to check the group mode, use the "show ip igmp group" command. 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 28-3: 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 28-3: 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	—

Item	Meaning	Displayed detailed information
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 28-4: 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 28-4: 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	—

Item	Meaning	Displayed detailed information
Report(V3)	IGMP Version 3 Report message	—
Leave	Leave message	—
Error	Error packet	—

Impact on communication

None

Response messages

Table 28-5: List of response messages for the show igmp-snooping command

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 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
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
No operational Port.	The ports specified in \<port list> did not include active ones.
No operational VLAN.	There are no available VLANs.
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

Notes

None

clear igmp-snooping

Clears IGMP snooping information.

Syntax

```
clear igmp-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 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.

-f

Clears statistics without displaying a clear confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Operation when a stack configuration is used

When both IPv4 multicast and IGMP snooping are used together, commands can be executed only on the master switch.

Example

None

Display items

None

Impact on communication

Note that when the "clear igmp-snooping all" or "clear igmp-snooping group" command is executed, multicast communication temporarily stops.

Response messages

Table 28-6: List of response messages for the clear igmp-snooping command

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
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
No operational VLAN.	There are no available VLANs.

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

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, use of <switch no.> and range specification with an asterisk (*) are not possible.

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.

Operation when a stack configuration is used

This command is not supported.

Example 1

Figure 28-5: Displaying the MLD snooping information

```
> show mld-snooping
Date 20XX/04/10 15:20:00 UTC
VLAN counts: 2
VLAN: 100
  VRF: 2
  IP Address: fe80::b1  Querier: enable
  MLD querying system: fe80::b1
  Querier version: V2
  IPv6 Multicast routing: On
  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
  IPv6 Multicast routing: Off
  Port(4): 0/6-9
  Mrouter-port: 0/6
  Group counts: 0
>

> show mld-snooping 100
Date 20XX/04/10 15:21:00 UTC
VLAN: 100
  IP Address: fe80::b1  Querier: enable
  MLD querying system: fe80::b1
  Querier version: V2
  IPv6 Multicast routing: On
  Port(5):  0/1-5
  Mrouter-port: 0/1,0/3
  Group counts: 3
>
```

Display items in Example 1

Table 28-7: 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	—
VRF [SL-L3A]	VRF ID	This item is displayed only when VRF is assigned to the VLAN interface.
IP Address	IP address	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
IPv6 Multicast routing	Whether IPv6 multicast routing has been set for the VLAN	On: Multicast routing has been set. Off: Multicast routing has not been set.

Item	Meaning	Displayed detailed information
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 28-6: 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  IPv6 Multicast routing: Off
  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 IPv6 Multicast routing: On
  Group Address     MAC Address         Version      Mode
  ff35::3           3333:0000:0003      -            -
    Port-list:0/4,0/6
>
> show mld-snooping group 100
Date 20XX/01/15 15:20:00 UTC
VLAN counts: 1
VLAN: 100  Group counts: 2  IPv6 Multicast routing: Off
  Group Address     MAC Address         Version      Mode
  ff35::1           3333:0000:0001      V1,V2        EXCLUDE
    Port-list:0/1-3
  ff35::2           3333:0000:0002      V2           EXCLUDE
    Port-list:0/1-2

> show mld-snooping group ff35::1
Date 20XX/01/15 15:20:00 UTC
VLAN counts: 2
VLAN: 100  Group counts: 1  IPv6 Multicast routing: Off
  Group Address     MAC Address         Version      Mode
  ff35::1           3333:0000:0001      V1           -
    Port-list:0/1-3
VLAN: 300  Group counts: 1  IPv6 Multicast routing: On
  Group Address     MAC Address         Version      Mode
  ff35::1           3333:0000:0001      -            -
    Port-list:0/4,0/6
>
> show mld-snooping group ff35::1 100
Date 20XX/01/15 15:20:00 UTC
VLAN counts: 1
VLAN: 100  Group counts: 1  IPv6 Multicast routing: Off
  Group Address     MAC Address         Version      Mode
  ff35::1           3333:0000:0001      V1,V2        EXCLUDE
    Port-list:0/1-3
```

Display items in Example 2

Table 28-8: 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.

Item	Meaning	Displayed detailed information
VLAN counts	Number of VLANs on which MLD snooping is enabled	—
VLAN	VLAN information	—
Group counts	Number of subscription multicast groups in the VLAN	—
IPv6 Multicast routing	Whether IPv6 multicast routing has been set for the VLAN	On: Multicast routing has been set. Off: Multicast routing has not been set.
Group Address	Subscription group addresses	—
MAC Address	Learned MAC addresses	—
Version	MLD version information	V1: MLD Version 1 V2: MLD Version 2 If IPv6 Multicast routing is On, a hyphen (-) is displayed. In this case, to check the MLD version information, use the "show ipv6 mld group" command. 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 If the MLD version information is V1 or if IPv6 Multicast routing is On, "-" is displayed. If IPv6 Multicast routing is On, to check the group mode, use the "show ipv6 mld group" command. 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 28-7: 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 28-9: 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 28-8: 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 28-10: 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

Response messages

Table 28-11: List of response messages for the show mld-snooping command

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 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>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.
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

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.

Operation when a stack configuration is used

This command is not supported.

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.

Response messages

Table 28-12: List of response messages for the clear mld-snooping command

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 re-started, and then re-execute the command. \<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 VLAN.	There are no available VLANs.

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

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} restart snooping [-f] [core-file]
```

Example

None

Display items

None

Impact on communication

After the snooping program has been restarted, multicast communication stops until multicast groups are learned again.

Response messages

Table 28-13: List of response messages for the restart snooping command

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
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 failed to terminate.	The "restart snooping" command could not restart the IGMP snooping/MLD snooping program. Re-execute the command.
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.

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

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} dump protocols snooping
```

Example

None

Impact on communication

None

Response messages

Table 28-14: List of response messages for the dump protocols snooping command

Message	Description
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

Message	Description
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.

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.

29 Filters

show access-filter

Displays the filter conditions applied on the Ethernet interface or VLAN interface by the access group com-
mands (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 ac-
cess list.

Syntax

```
show access-filter
show access-filter <switch no.>/<nif no.>/<port no.>
            [ { <access list number> | <access list name> } ]
            [ { in | out | in-mirror | out-mirror } ]
show access-filter interface vlan <vlan id>
            [ { <access list number> | <access list name> } ]
            [ { in | out | in-mirror | out-mirror } ]
```

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-mirror | out-mirror }

   in: Inbound (Specifies the receiving side of the filter)

   out: Outbound (Specifies the sending side of the filter)

   in-mirror: Inbound (Specifies the receiving side of policy-based mirroring)

   out-mirror: Outbound (Specifies the sending side of policy-based mirroring)

   The command with this parameter displays statistics on the receiving side or the sending side of the fil-
   ter, or of policy-based mirroring, for the specified interface.

Behavior when this parameter is omitted:

Statistics for the receiving side and the sending side of the specified interface are displayed.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch. You can also execute the command with the switch number of the member switch specified.

You can also use the "remote command" command.

```
remote command { <switch no.> | all } show access-filter
remote command <switch no.> show access-filter <switch no.>/<nif no.>/<port no.> [ { <access li
st number> | <access list name> } ] [ { in | out | in-mirror | out-mirror } ]
remote command { <switch no.> | all } show access-filter interface vlan <vlan id> [ { <access l
ist number> | <access list name> } ] [ { in | out | in-mirror | out-mirror } ]
```

Example

Figure 29-1: 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 29-2: 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 29-3: 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 29-4: Result of displaying the IPv6 access list

```
> show access-filter 1/0/15 telnet-server
Date 20XX/07/14 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 29-5: 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 29-6: 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 29-7: 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

Display items of statistics for the access list applied to an interface by using an access group command are described below.

```
> show access-filter 1/0/7 12
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/7 in              <-------------------- Interface Information
Standard IP access-list: 12    <-------------------- Access list ID
     remark "permit only host pc"      <----------- Access list information
     10 permit host 10.10.10.1         <--------- Access list information
        matched packets      :  74699826      <---- Statistics
     20 permit host 10.10.10.254        <--------- Access list information
        matched packets      :    264176      <---- Statistics
     implicitly denied packets:    2698        <---- Statistics
>
```

Table 29-1: Statistical items for the access list

Item	Displayed information	
	Detailed information	**Meaning**
Interface in-formation	Using Port:<switch no.>/<nif no.>/<port no.> in	Information about an Ethernet interface to which an access list has been applied on the in-bound 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 out-bound side
	Using Port:<switch no.>/<nif no.>/<port no.> in-mirror	Information about an Ethernet interface to which an access list has been applied on the in-bound side of policy-based mirroring
	Using Port:<switch no.>/<nif no.>/<port no.> out-mirror	Information about an Ethernet interface to which an access list has been applied on the out-bound side of policy-based mirroring
	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
	Using Interface:vlan <vlan id> in-mirror	Information about a VLAN interface to which an access list has been applied on the inbound side of policy-based mirroring
	Using Interface:vlan <vlan id> out-mirror	Information about a VLAN interface to which an access list has been applied on the outbound side of policy-based mirroring
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

| Item | Displayed information | |
	Detailed information	Meaning
	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 Vol. 1, 25. 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

Response messages

Table 29-2: List of response messages for the show access-filter command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. 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
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.
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

1. To check the route information for policy-based routing, execute the "show ip cache policy" command. [SL-L3A]

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 | in-mirror | out-mirror } ]
clear access-filter interface vlan <vlan id>
             [ { <access list number> | <access list name> } ]
             [ { in | out | in-mirror | out-mirror } ]
```

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-mirror | out-mirror }

> > in: Inbound (Specifies the receiving side of the filter)
> >
> > out: Outbound (Specifies the sending side of the filter)
> >
> > in-mirror: Inbound (Specifies the receiving side of policy-based mirroring)
> >
> > out-mirror: Outbound (Specifies the sending side of policy-based mirroring)
> >
> > The command with this parameter clears statistics on the receiving side or the sending side of the filter, or of policy-based mirroring, for the specified interface, 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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch. You can also execute the command with the switch number of the member switch specified.

You can also use the "remote command" command.

```
remote command { <switch no.> | all } clear access-filter
remote command <switch no.> clear access-filter <switch no.>/<nif no.>/<port no.> [ { <access l
ist number> | <access list name> } ] [ { in | out | in-mirror | out-mirror } ]
remote command { <switch no.> | all } clear access-filter interface vlan <vlan id> [ { <access
list number> | <access list name> } ] [ { in | out | in-mirror | out-mirror } ]
```

Example

Figure 29-8: 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

Response messages

Table 29-3: List of response messages for the clear access-filter command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. 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
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.

Message	Description
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

1. If this command is executed, the MIB information of the axsAccessFilterStats group is also cleared to zero.

30 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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch. You can also execute the command with the switch number of the member switch specified.

You can also use the "remote command" command.

```
remote command <switch no.> show qos-flow [ { <switch no.>/<nif no.>/<port no.> | interface vla
n <vlan id> } [ <qos flow list name> ] ]
remote command all show qos-flow [ interface vlan <vlan id> [ <qos flow list name> ] ]
```

Example

- The following figures show examples of displaying the QoS flow list information when bandwidth monitoring is not used.

Figure 30-1: 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 30-2: 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 30-3: Result of displaying the IPv6 QoS flow list information

```
> show qos-flow 1/0/11 telnet-qos
Date 20XX/07/14 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
>
```

- The following figures show examples of displaying the QoS flow list information when bandwidth monitoring is used.

Figure 30-4: Result of displaying the IPv4 QoS flow list information when minimum bandwidth monitoring is used

```
> show qos-flow 1/0/3 http-qos-min
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/3 in
IP qos-flow-list:http-qos-min
      remark "http access min-rate 256k"
      10 tcp(6) any any eq http(80) action cos 4 min-rate 256 min-rate-burst 256
penalty-discard-class 1
          matched packets(min-rate over) :     9826
          matched packets(min-rate under):  74699826
>
```

Figure 30-5: Result of displaying the IPv4 QoS flow list information when maximum bandwidth control is used

```
> show qos-flow 1/0/7 http-qos-max
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/7 in
IP qos-flow-list:http-qos-max
      remark "http access max-rate 256k"
      10 tcp(6) any any eq http(80) action cos 4 discard-class 2 max-rate 256 max-rate-burs
t 256 log trap
          matched packets(max-rate over) :     9826
          matched packets(max-rate under):  74699826
          rate-alarm
              state: exceed
              count:    0/    1
              total exceed-count/total conform-count:      154/     7295
>
```

Figure 30-6: Result of displaying the IPv4 QoS flow list information when minimum bandwidth monitoring and maximum bandwidth control are used

```
> show qos-flow 1/0/11 http-qos-rate
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/11 in
IP qos-flow-list:http-qos-rate
      remark "http access min-rate 64k and max-rate 256k"
      10 tcp(6) any any eq http(80) action cos 4 discard-class 2 max-rate 256 max-rate-burs
t 256 min-rate 64 min-rate-burst 64 penalty-discard-class 1 trap
          matched packets(max-rate over) :     9826
          matched packets(max-rate under):  74699826
          rate-alarm
              state: conform
```

```
                count:    0/    1
                total exceed-count/total conform-count:       154/     7295
    >
```

Display items

Table 30-1: 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 Vol. 1, 26. QoS".)	
Statistics	matched packets:\<packets>	Number of packets that meet the flow detection conditions in the QoS flow list
	matched packets(max-rate over):\<packets>	Number of packets that match the flow detection conditions but violate the maximum bandwidth control criteria of the QoS flow list.
	matched packets(max-rate under):\<packets>	Number of packets that match the flow detection conditions and conform to the maximum bandwidth control criteria of the QoS flow list.
	matched packets(min-rate over):\<packets>	Number of packets that match the flow detection conditions but violate the minimum bandwidth monitoring criteria of the QoS flow list.
	matched packets(min-rate under):\<packets>	Number of packets that match the flow detection condition and conform to the minimum bandwidth monitoring criteria of the QoS flow list.
Bandwidth status and monitoring status of bandwidth non-compliance notifications	rate-alarm	Information on bandwidth non-compliance notifications
	state:	Bandwidth status conform: Bandwidth compliance status exceed: Bandwidth non-compliance status
	count:	Monitoring status When state is conform (bandwidth compliance status): Bandwidth violation count/monitoring count When state is exceed (bandwidth non-compliance status): Bandwidth compliance count/monitoring count

Item	Displayed information	
	Detailed information	**Meaning**
Statistics on bandwidth non-compliance notifications	total exceed-count/total conform-count:	Total exceed-count/total conform-count In periodic monitoring of target QoS entries, how many times the number of bandwidth violation frames has increased compared with the previous monitoring (bandwidth violation count) and has not increased (bandwidth compliance count) are displayed regardless of the bandwidth status. The total values of the bandwidth violation count and bandwidth compliance count are summed up to get the total monitoring count.

Impact on communication

None

Response messages

Table 30-2: List of response messages for the show qos-flow command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. 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
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.
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.
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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. It also clears the bandwidth non-compliance notification statistics to zero.

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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch. You can also execute the command with the switch number of the member switch specified.

You can also use the "remote command" command.

```
remote command <switch no.> clear qos-flow [ { <switch no.>/<nif no.>/<port no.> | interface vl
an <vlan id> } [ <qos flow list name> ] ]
remote command all clear qos-flow [ interface vlan <vlan id> [ <qos flow list name> ] ]
```

Example

Figure 30-7: 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

Response messages

Table 30-3: List of response messages for the clear qos-flow command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. 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
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.
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.
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch. You can also execute the command with the switch number of the member switch specified.

You can also use the "remote command" command.

```
remote command { <switch no.> | all } show qos queueing
remote command <switch no.> show qos queueing <switch no.>/<nif no.>/<port no.>
```

Example

Figure 30-8: Result of displaying the information about all send queues

```
> show qos queueing
Date 20XX/01/01 12:00:00 UTC
Switch1 To-CPU (outbound)
 Max_Queue=8
  Queue  1: Qlen=     0, Limit_Qlen=   48, HOL1=           0
  Queue  2: Qlen=     0, Limit_Qlen=   48, HOL1=           0
  Queue  3: Qlen=     0, Limit_Qlen= 1024, HOL1=           0
  Queue  4: Qlen=     0, Limit_Qlen= 1024, HOL1=           0
  Queue  5: Qlen=     0, Limit_Qlen= 1024, HOL1=           0
  Queue  6: Qlen=     0, Limit_Qlen= 1024, HOL1=           0
  Queue  7: Qlen=     3, Limit_Qlen= 1024, HOL1=           0
  Queue  8: Qlen=     7, Limit_Qlen= 2048, HOL1=          25
 Tail_drop=         0
Switch1/NIF0/Port1 (outbound)
 Max_Queue=12, Rate_limit=64kbit/s, Burst_size=4kbyte, Qmode=pq/tail_drop
  Queue  1: Qlen=     0, Limit_Qlen= 2880, HOL1=           0
  Queue  2: Qlen=     0, Limit_Qlen= 2880, HOL1=           0
  Queue  3: Qlen=     0, Limit_Qlen= 2880, HOL1=           0
  Queue  4: Qlen=     0, Limit_Qlen= 2880, HOL1=           0
  Queue  5: Qlen=     0, Limit_Qlen= 2880, HOL1=           0
  Queue  6: Qlen=     0, Limit_Qlen= 2880, HOL1=           0
  Queue  7: Qlen=     0, Limit_Qlen= 2880, HOL1=           0
  Queue  8: Qlen=     0, Limit_Qlen= 2880, HOL1=           0
```

```
 Queue  9: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue 10: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue 11: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue 12: Qlen=      0, Limit_Qlen=  2880, HOL1=        655
 Tail_drop=          0
            .
            .
            .
Switch1/NIF0/Port52 (outbound)
 Max_Queue=12, Rate_limit=40Gbit/s, Burst_size=-, Qmode=pq/tail_drop
 Queue  1: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  2: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  3: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  4: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  5: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  6: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  7: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  8: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  9: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue 10: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue 11: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue 12: Qlen=      0, Limit_Qlen=  2880, HOL1=         54
 Tail_drop=          0
>
```

Figure 30-9: Result of displaying the information about all send queues (when the stack is enabled and stack ports are configured)

```
> show qos queueing
Switch 1 (Master)
-----------------
Date 20XX/01/01 12:00:00 UTC
Switch1 To-CPU (outbound)
 Max_Queue=11
 Queue  1: Qlen=      0, Limit_Qlen=    48, HOL1=          0
 Queue  2: Qlen=      0, Limit_Qlen=    48, HOL1=          0
 Queue  3: Qlen=      0, Limit_Qlen=  1024, HOL1=          0
 Queue  4: Qlen=      0, Limit_Qlen=  1024, HOL1=          0
 Queue  5: Qlen=      0, Limit_Qlen=  1024, HOL1=          0
 Queue  6: Qlen=      0, Limit_Qlen=  1024, HOL1=          0
 SQueue 1: Qlen=      0, Limit_Qlen=  1024, HOL1=          0
 SQueue 2: Qlen=      0, Limit_Qlen=  1024, HOL1=          0
 Queue  7: Qlen=      3, Limit_Qlen=  1024, HOL1=          0
 Queue  8: Qlen=      7, Limit_Qlen=  2048, HOL1=         25
 SQueue 3: Qlen=      0, Limit_Qlen=    64, HOL1=          0
 Tail_drop=          0
Switch1/NIF0/Port1 (outbound)
 Max_Queue=12, Rate_limit=64kbit/s, Burst_size=4kbyte, Qmode=pq/tail_drop
 Queue  1: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  2: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  3: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  4: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  5: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  6: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  7: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  8: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  9: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue 10: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue 11: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue 12: Qlen=      0, Limit_Qlen=  2880, HOL1=        655
 Tail_drop=          0
            .
            .
            .
Switch1/NIF0/Port49 (outbound)
 Max_Queue=14, Rate_limit=40Gbit/s, Burst_size=-, Qmode=pq/tail_drop
 Queue  1: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  2: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  3: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  4: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  5: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  6: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  7: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  8: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
 Queue  9: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
```

```
   Queue 10: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue 11: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue 12: Qlen=      0, Limit_Qlen=  2880, HOL1=         35
   SQueue 1: Qlen=      1, Limit_Qlen=   360, HOL1=          0
   SQueue 2: Qlen=      1, Limit_Qlen=   360, HOL1=          0
  Tail_drop=          0
               .
               .
               .
  Switch1/NIF0/Port52 (outbound)
   Max_Queue=12, Rate_limit=40Gbit/s, Burst_size=-, Qmode=pq/tail_drop
   Queue  1: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  2: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  3: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  4: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  5: Qlen=      0, Limit_Qlen=  2880, HOL1=      13870
   Queue  6: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  7: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  8: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  9: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue 10: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue 11: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue 12: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
  Tail_drop=       2561

  Switch 2 (Backup)
  -----------------
  Date 20XX/01/01 12:00:00 UTC
  Switch2 To-CPU (outbound)
   Max_Queue=11
   Queue  1: Qlen=      0, Limit_Qlen=    48, HOL1=          0
   Queue  2: Qlen=      0, Limit_Qlen=    48, HOL1=          0
   Queue  3: Qlen=      0, Limit_Qlen=  1024, HOL1=          0
   Queue  4: Qlen=      0, Limit_Qlen=  1024, HOL1=          0
   Queue  5: Qlen=      0, Limit_Qlen=  1024, HOL1=          0
   Queue  6: Qlen=      0, Limit_Qlen=  1024, HOL1=          0
   SQueue 1: Qlen=      0, Limit_Qlen=  1024, HOL1=          0
   SQueue 2: Qlen=      0, Limit_Qlen=  1024, HOL1=          0
   Queue  7: Qlen=      3, Limit_Qlen=  1024, HOL1=          0
   Queue  8: Qlen=      7, Limit_Qlen=  2048, HOL1=          0
   SQueue 3: Qlen=      0, Limit_Qlen=    64, HOL1=          0
  Tail_drop=          0
  Switch2/NIF0/Port1 (outbound)
   Max_Queue=12, Rate_limit=64kbit/s, Burst_size=4kbyte, Qmode=pq/tail_drop
   Queue  1: Qlen=      0, Limit_Qlen=  2880, HOL1=      53423
   Queue  2: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  3: Qlen=      0, Limit_Qlen=  2880, HOL1=       2347
   Queue  4: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  5: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  6: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  7: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  8: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  9: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue 10: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue 11: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue 12: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
  Tail_drop=       1532
               .
               .
               .
  Switch2/NIF0/Port49 (outbound)
   Max_Queue=14, Rate_limit=40Gbit/s, Burst_size=-, Qmode=pq/tail_drop
   Queue  1: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  2: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  3: Qlen=      0, Limit_Qlen=  2880, HOL1=         35
   Queue  4: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  5: Qlen=      0, Limit_Qlen=  2880, HOL1=      49873
   Queue  6: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  7: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  8: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue  9: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue 10: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue 11: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
   Queue 12: Qlen=      0, Limit_Qlen=  2880, HOL1=          0
```

```
   SQueue 1: Qlen=      1, Limit_Qlen=   360, HOL1=         0
   SQueue 2: Qlen=      1, Limit_Qlen=   360, HOL1=         0
 Tail_drop=          0
            .
            .
            .
Switch2/NIF0/Port52 (outbound)
 Max_Queue=12, Rate_limit=40Gbit/s, Burst_size=-, Qmode=pq/tail_drop
  Queue  1: Qlen=      0, Limit_Qlen=  2880, HOL1=         0
  Queue  2: Qlen=      0, Limit_Qlen=  2880, HOL1=         0
  Queue  3: Qlen=      0, Limit_Qlen=  2880, HOL1=         0
  Queue  4: Qlen=      0, Limit_Qlen=  2880, HOL1=         0
  Queue  5: Qlen=      0, Limit_Qlen=  2880, HOL1=         0
  Queue  6: Qlen=      0, Limit_Qlen=  2880, HOL1=         0
  Queue  7: Qlen=      0, Limit_Qlen=  2880, HOL1=         0
  Queue  8: Qlen=      0, Limit_Qlen=  2880, HOL1=         0
  Queue  9: Qlen=      0, Limit_Qlen=  2880, HOL1=         0
  Queue 10: Qlen=      0, Limit_Qlen=  2880, HOL1=         0
  Queue 11: Qlen=      0, Limit_Qlen=  2880, HOL1=         0
  Queue 12: Qlen=      0, Limit_Qlen=  2880, HOL1=        54
 Tail_drop=          0
>
```

Display items

Table 30-4: 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
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 Vol.1, traffic-shape rate".
	Qmode=<schedule name>/<drop name>	Scheduling (pq, 4pq+8rr, 4pq+8wfq, 4pq+8err, 4pq+8wrr)/ drop control mode(tail_drop) For details on scheduling, see "Configuration Command Reference Vol.1, qos-queue-list".

Item	Displayed information	
	Detailed information	**Meaning**
Queue information	Queue<queue no.>:	Send queue number[#1]
	SQueue<queue no.>:	System queue number[#2]
	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.)[#3, #4, #5] 2. There is no space in the packet buffer.[#6]
Port statistics	Tail_drop=<packets>	The number of packets discarded because the drop threshold for queuing priority 1 or 2 is exceeded[#3, #4]

#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

The system queue is used by the stack function for communication and exists only when the stack function is enabled. It is displayed in a send queue to the CPU and in a send queue on a stack port.

#3

Some control packets are handled with a queuing priority other than 3.

#4

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.

#5

The following figure shows an overview of processing that discards packets because the send queue is full.

Figure 30-10: Overview of processing that discards packets because the send queue is full
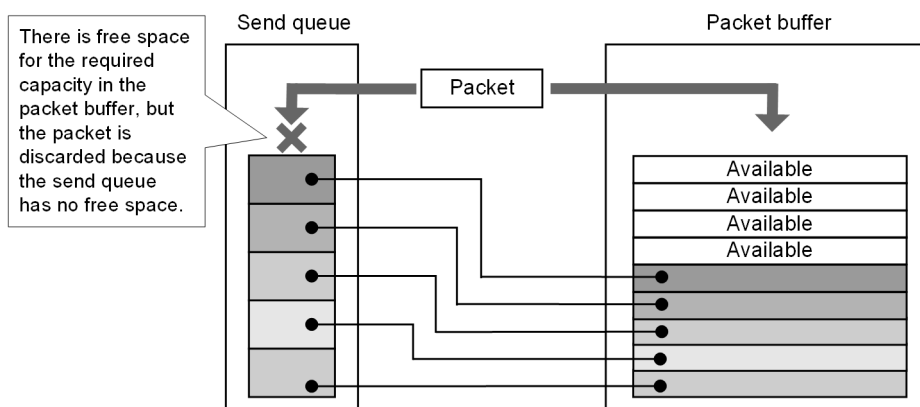
#6

The following figure shows an overview of processing that discards packets because the packet buffer is full.

Figure 30-11: Overview of processing that discards packets because the packet buffer is full
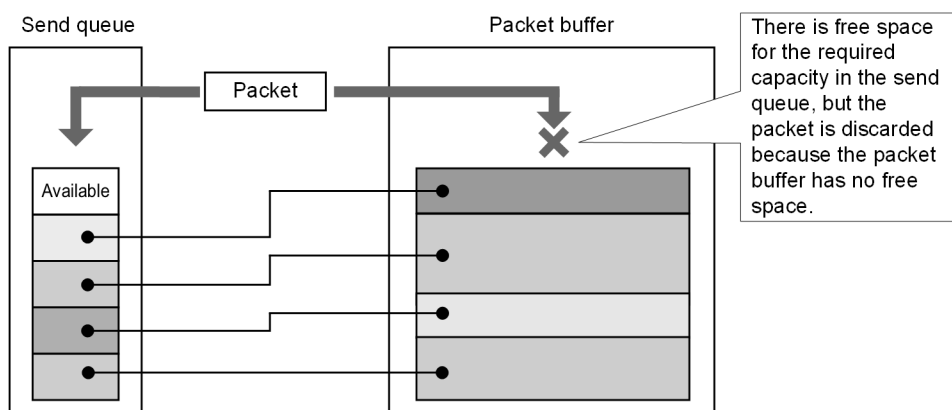
Impact on communication

None

Response messages

Table 30-5: List of response messages for the show qos queueing command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. 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
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch. You can also execute the command with the switch number of the member switch specified.

You can also use the "remote command" command.

```
remote command { <switch no.> | all } clear qos queueing
remote command <switch no.> clear qos queueing <switch no.>/<nif no.>/<port no.>
```

Example

Figure 30-12: 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

Response messages

Table 30-6: List of response messages for the clear qos queueing command

Message	Description
Can't execute for accounts mismatch.	This command cannot be executed because the account of the backup switch is different. Synchronize the account by using account operation commands (adduser, rmuser, password, and clear password).
Can't execute.	The command could not be executed. 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
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. In addition, the command might fail immediately after a member switch is added. In this case, re-execute the command. <switch no.>: Switch number
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

Notes

1. If this command is executed, the MIB information of the axsEtherTxQoS and axsToCpuQoS groups is also cleared to zero.

31 **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> | vlan {<
vlan id list> | dynamic} }]
```

Input mode

User mode and administrator mode

Parameters

{ port <port list> | channel-group-number <channel group list> | vlan {<vlan id list> | dynamic} }

> port <port list>
>
>> Displays statistics for port-based authentication for the physical ports specified in list format. 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>
>
>> Displays statistics for port-based authentication for the channel groups specified in list format. For details about how to specify <channel group list>, see "Specifiable values for parameters".
>
> vlan <vlan id list>
>
>> Displays statistics for VLAN-based authentication (static) of the specified VLANs 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.
>
> vlan dynamic
>
>> Displays statistics for VLAN-based authentication (dynamic).
>
> Behavior when this parameter is omitted:
>
>> Statistics for all the above types are displayed.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 31-1: Displaying the statistics for each port that uses IEEE 802.1X port-based authentication

```
> show dot1x statistics port 0/10
Date 20XX/01/23 12:32:00 UTC
[EAPOL frames]
Port  0/10 TxTotal   :        30 TxReq/Id  :        10 TxReq     :        10
           TxSuccess :        10 TxFailure :         0 TxNotify  :         0
           RxTotal   :        20 RxStart   :         0 RxLogoff  :         0
           RxResp/Id :        10 RxResp    :        10 RxNotify  :         0
           RxInvalid :         0 RxLenErr  :         0

[EAPoverRADIUS frames]
Port  0/10 TxTotal   :        10 TxNakResp :         0 TxNoNakRsp:        10
           RxTotal   :        30 RxAccAccpt:        10 RxAccRejct:        10
           RxAccChllg:        10 RxInvalid :         0
>
```

Figure 31-2: Displaying the statistics for each channel group that uses IEEE 802.1X port-based authentication

```
> show dot1x statistics channel-group-number 11
Date 20XX/01/23 12:32:00 UTC
[EAPOL frames]
ChGr  11   TxTotal  :         30 TxReq/Id :        10 TxReq    :        10
           TxSuccess :        10 TxFailure :         0 TxNotify  :         0
           RxTotal  :         20 RxStart   :         0 RxLogoff  :         0
           RxResp/Id :        10 RxResp    :        10 RxNotify  :         0
           RxInvalid :         0 RxLenErr  :         0

[EAPoverRADIUS frames]
ChGr  11   TxTotal  :         10 TxNakResp :         0 TxNoNakRsp:        10
           RxTotal  :         30 RxAccAccpt:        10 RxAccRejct:        10
           RxAccChllg:        10 RxInvalid :         0
>
```

Figure 31-3: Displaying the statistics for each VLAN that uses IEEE 802.1X VLAN-based authentication (static)

```
> show dot1x statistics vlan 20
Date 20XX/01/23 12:32:00 UTC
[EAPOL frames]
VLAN 20    TxTotal  :         30 TxReq/Id :        10 TxReq    :        10
           TxSuccess :        10 TxFailure :         0 TxNotify  :         0
           RxTotal  :         20 RxStart   :         0 RxLogoff  :         0
           RxResp/Id :        10 RxResp    :        10 RxNotify  :         0
           RxInvalid :         0 RxLenErr  :         0

[EAPoverRADIUS frames]
VLAN 20    TxTotal  :         10 TxNakResp :         0 TxNoNakRsp:        10
           RxTotal  :         30 RxAccAccpt:        10 RxAccRejct:        10
           RxAccChllg:        10 RxInvalid :         0
>
```

Figure 31-4: Displaying the statistics for IEEE 802.1X VLAN-based authentication (dynamic)

```
> show dot1x statistics vlan dynamic
Date 20XX/01/23 12:32:00 UTC
[EAPOL frames]
VLAN       TxTotal  :         30 TxReq/Id :        10 TxReq    :        10
(Dynamic)  TxSuccess :        10 TxFailure :         0 TxNotify  :         0
           RxTotal  :         20 RxStart   :         0 RxLogoff  :         0
           RxResp/Id :        10 RxResp    :        10 RxNotify  :         0
           RxInvalid :         0 RxLenErr  :         0

[EAPoverRADIUS frames]
VLAN       TxTotal  :         10 TxNakResp :         0 TxNoNakRsp:        10
(Dynamic)  RxTotal  :         30 RxAccAccpt:        10 RxAccRejct:        10
           RxAccChllg:        10 RxInvalid :         0
>
```

Figure 31-5: Displaying the statistics for all types of IEEE 802.1X authentication (port-based and VLAN-based authentication)

```
> show dot1x statistics
Date 20XX/01/23 12:32:00 UTC
[EAPOL frames]
Port  0/10 TxTotal  :         30 TxReq/Id :        10 TxReq    :        10
           TxSuccess :        10 TxFailure :         0 TxNotify  :         0
           RxTotal  :         20 RxStart   :         0 RxLogoff  :         0
           RxResp/Id :        10 RxResp    :        10 RxNotify  :         0
           RxInvalid :         0 RxLenErr  :         0
ChGr  11   TxTotal  :         30 TxReq/Id :        10 TxReq    :        10
           TxSuccess :        10 TxFailure :         0 TxNotify  :         0
           RxTotal  :         20 RxStart   :         0 RxLogoff  :         0
           RxResp/Id :        10 RxResp    :        10 RxNotify  :         0
           RxInvalid :         0 RxLenErr  :         0
VLAN 20    TxTotal  :         30 TxReq/Id :        10 TxReq    :        10
           TxSuccess :        10 TxFailure :         0 TxNotify  :         0
           RxTotal  :         20 RxStart   :         0 RxLogoff  :         0
           RxResp/Id :        10 RxResp    :        10 RxNotify  :         0
           RxInvalid :         0 RxLenErr  :         0
VLAN       TxTotal  :         30 TxReq/Id :        10 TxReq    :        10
(Dynamic)  TxSuccess :        10 TxFailure :         0 TxNotify  :         0
           RxTotal  :         20 RxStart   :         0 RxLogoff  :         0
           RxResp/Id :        10 RxResp    :        10 RxNotify  :         0
           RxInvalid :         0 RxLenErr  :         0
```

```
[EAPoverRADIUS frames]
Port  0/10 TxTotal   :        10 TxNakResp :         0 TxNoNakRsp:         10
           RxTotal   :        30 RxAccAccpt:        10 RxAccRejct:         10
           RxAccChllg:        10 RxInvalid :         0
ChGr  11   TxTotal   :        10 TxNakResp :         0 TxNoNakRsp:         10
           RxTotal   :        30 RxAccAccpt:        10 RxAccRejct:         10
           RxAccChllg:        10 RxInvalid :         0
VLAN 20    TxTotal   :        10 TxNakResp :         0 TxNoNakRsp:         10
           RxTotal   :        30 RxAccAccpt:        10 RxAccRejct:         10
           RxAccChllg:        10 RxInvalid :         0
VLAN       TxTotal   :        10 TxNakResp :         0 TxNoNakRsp:         10
(Dynamic)  RxTotal   :        30 RxAccAccpt:        10 RxAccRejct:         10
           RxAccChllg:        10 RxInvalid :         0
>
```

Display items

Table 31-1: Display items for the statistics concerning IEEE 802.1X authentication

Item	Meaning	Displayed detailed information
Port/ChGr/VLAN/VLAN(Dynamic)	Indicates the type of authentication. Port \<nif no.\>/\<port no.\>: Indicates a port for port-based authentication. ChGr \<channel group number\>: Indicates a channel group for port-based authentication. VLAN \<vlan id\>: Indicates a VLAN ID for VLAN-based authentication (static). VLAN(Dynamic): Indicates VLAN-based authentication (dynamic).	
[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)	

Item	Meaning	Displayed detailed information
[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	
RxInvalid	The number of invalid EAPoverRADIUS frames that have been received	

Impact on communication

None

Response messages

Table 31-2: List of response messages for the show dot1x statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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 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.
No operational VLAN(Dynamic).	VLAN-based authentication (dynamic) was not configured. Check the authentication mode set by the configuration.

Message	Description
No operational VLAN.	There are no available VLANs. 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.

Notes

None

show dot1x

Displays status information about IEEE 802.1X authentication.

Syntax

```
show dot1x [{ port <port list> | channel-group-number <channel group list> | vlan {<vlan id lis
t> | dynamic [<vlan id list>]} }] [detail]
```

Input mode

User mode and administrator mode

Parameters

{ port <port list> | channel-group-number <channel group list> | vlan {<vlan id list> | dynamic [<vlan id list>]} }

> port <port list>
>
>> Displays status information about port-based authentication for the physical ports specified in list format. 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>
>
>> Displays status information about port-based authentication for the channel groups specified in list format. For details about how to specify <channel group list>, see "Specifiable values for parameters".
>
> vlan <vlan id list>
>
>> Displays status information about VLAN-based authentication (static) for VLANs 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.
>
> vlan dynamic <vlan id list>
>
>> Displays status information about VLAN-based authentication (dynamic).
>>
>> 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.
>>
>> If <vlan id list> is omitted, status information about VLAN-based authentication (dynamic) for all VLANs is displayed.

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.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 31-6: Displaying the status information for the IEEE 802.1X device

```
> show dot1x
Date 20XX/01/23 12:32:00 UTC
System 802.1X : Enable
    AAA Authentication Dot1x   : Enable
        Authorization Network  : Enable
        Accounting Dot1x       : Enable


Port/ChGr/VLAN   AccessControl   PortControl      Status       Supplicants
Port  0/1        ---             Auto             Authorized   1
Port  0/10       Multiple-Auth   Auto             ---          1
ChGr  11         Multiple-Auth   Auto             ---          1
VLAN 20          Multiple-Auth   Auto             ---          1
VLAN(Dynamic)    Multiple-Auth   Auto             ---          1
>
```

Figure 31-7: Displaying the status information for each port that uses IEEE 802.1X port-based authentication (with no display option specified)

```
> show dot1x port 0/1
Date 20XX/01/23 12:32:00 UTC
Port  0/1
AccessControl  : ---                       PortControl   : Auto
Status         : Authorized                Last EAPOL    : 0012.e200.0021
Supplicants    : 1 / 1                     ReAuthMode    : Enable
TxTimer(s)     : ---   / 30                ReAuthTimer(s): 123   / 300
ReAuthSuccess  : 4                         ReAuthFail    : 0
KeepUnauth(s)  : ---   / 3600
>
```

Figure 31-8: Displaying the status information for each port that uses IEEE 802.1X port-based authentication (with the detail option specified)

```
> show dot1x port 0/1 detail
Date 20XX/01/23 17:57:03 UTC
Port  0/1
AccessControl  : ---                       PortControl   : Auto
Status         : Authorized                Last EAPOL    : 0012.e200.0021
Supplicants    : 1 / 1                     ReAuthMode    : Enable
TxTimer(s)     : ---   / 30                ReAuthTimer(s): 123   / 300
ReAuthSuccess  : 4                         ReAuthFail    : 0
KeepUnauth(s)  : ---   / 3600

  Supplicants MAC    Status       AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time
  0012.e200.0021     Authorized   Authenticated  Idle           0
                     177          20XX/01/23 17:55:00
>
```

Figure 31-9: Displaying the status information for each channel group that uses IEEE 802.1X port-based authentication (with no display option specified)

```
> show dot1x channel-group-number 11
Date 20XX/01/23 12:32:00 UTC
ChGr  11
AccessControl  : Multiple-Auth             PortControl   : Auto
Status         : ---                       Last EAPOL    : 0012.e200.0011
Supplicants    : 2 / 2 / 64                ReAuthMode    : Enable
TxTimer(s)     : 15    / 30                ReAuthTimer(s): 123   / 300
ReAuthSuccess  : 4                         ReAuthFail    : 0
SuppDetection  : Shortcut
>
```

Figure 31-10: Displaying the status information about each channel group for the IEEE 802.1X port-based authentication (with the detail option specified)

```
> show dot1x channel-group-number 11 detail
Date 20XX/01/23 17:57:03 UTC
ChGr  11
AccessControl  : Multiple-Auth             PortControl   : Auto
Status         : ---                       Last EAPOL    : 0012.e200.0011
Supplicants    : 2 / 2 / 64                ReAuthMode    : Enable
TxTimer(s)     : 15    / 30                ReAuthTimer(s): 123   / 300
ReAuthSuccess  : 4                         ReAuthFail    : 0
SuppDetection  : Shortcut

  Supplicants MAC    Status       AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time
  0012.e200.0011     Authorized   Authenticated  Idle           0
                     177          20XX/01/23 17:55:00
  0012.e200.0012     Authorized   Authenticated  Idle           0
```

```
                          5                 20XX/01/23 17:56:58
>
```

Figure 31-11: Displaying the status information about each VLAN for IEEE 802.1X VLAN-based
            authentication (static) (with no display option specified)

```
> show dot1x vlan 20
Date 20XX/10/17 12:32:00 UTC
VLAN  20
AccessControl  : Multiple-Auth          PortControl   : Auto
Status         : ---                     Last EAPOL    : 0012.e200.0003
Supplicants    : 2 / 2 / 256             ReAuthMode    : Enable
TxTimer(s)     : ---   / 30              ReAuthTimer(s): 123   / 300
ReAuthSuccess  : 4                       ReAuthFail    : 0
SuppDetection  : Disable
Port(s): 0/1-10, ChGr  1-5
Force-Authorized Port(s): 0/4,8-10, ChGr 1-5
>
```

Figure 31-12: Displaying the status information about each VLAN for IEEE 802.1X VLAN-based
            authentication (static) (with the detail option specified)

```
> show dot1x vlan 20 detail
Date 20XX/10/17 17:57:03 UTC
VLAN  20
AccessControl  : Multiple-Auth          PortControl   : Auto
Status         : ---                     Last EAPOL    : 0012.e200.0003
Supplicants    : 2 / 2 / 256             ReAuthMode    : Enable
TxTimer(s)     : ---   / 30              ReAuthTimer(s): 123   / 300
ReAuthSuccess  : 4                       ReAuthFail    : 0
SuppDetection  : Disable
Port(s): 0/1-10, ChGr  1-5
Force-Authorized Port(s): 0/4,8-10, ChGr 1-5

 Supplicants MAC     Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time
 [Port 0/1]
 0012.e200.0003      Authorized     Authenticated  Idle           0
                     177            20XX/10/17 17:55:00
 0012.e200.0004      Authorized     Authenticated  Idle           0
                     5              20XX/10/17 17:56:58
>
```

Figure 31-13: Displaying the status information about IEEE 802.1X VLAN-based authentication
            (dynamic) (with no display option specified)

```
> show dot1x vlan dynamic
Date 20XX/10/17 12:32:00 UTC
VLAN(Dynamic)
AccessControl  : Multiple-Auth          PortControl   : Auto
Status         : ---                     Last EAPOL    : 0012.e200.0005
Supplicants    : 2 / 2 / 256             ReAuthMode    : Enable
TxTimer(s)     : ---   / 30              ReAuthTimer(s): 123   / 300
ReAuthSuccess  : 4                       ReAuthFail    : 0
SuppDetection  : Disable
VLAN(s): 2-5

VLAN(Dynamic) Supplicants
VLAN 2    2         VLAN 3    0         VLAN 4    0         VLAN 5    0
>
```

Figure 31-14: Displaying the status information about IEEE 802.1X VLAN-based authentication
            (dynamic) (with the detail option specified)

```
> show dot1x vlan dynamic detail
Date 20XX/10/17 17:57:03 UTC
VLAN(Dynamic)
AccessControl  : Multiple-Auth          PortControl   : Auto
Status         : ---                     Last EAPOL    : 0012.e200.0005
Supplicants    : 2 / 2 / 256             ReAuthMode    : Enable
TxTimer(s)     : ---   / 30              ReAuthTimer(s): 123   / 300
ReAuthSuccess  : 4                       ReAuthFail    : 0
SuppDetection  : Disable
VLAN(s): 2-5

 Supplicants MAC     Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time
 [VLAN 2]            VLAN(Dynamic) Supplicants : 2
 0012.e200.0005      Authorized     Authenticated  Idle           0
                     177            20XX/10/17 17:55:00
```

```
0012.e200.0006      Authorized      Authenticated  Idle        0
                    5               20XX/10/17 17:56:58
>
```

Figure 31-15: Displaying the status information about each VLAN for IEEE 802.1X VLAN-based authentication (dynamic) (with no display option specified)

```
> show dot1x vlan dynamic 2
Date 20XX/10/17 12:32:00 UTC
VLAN(Dynamic)
AccessControl  : Multiple-Auth          PortControl  : Auto
Status         : ---                     Last EAPOL   : 0012.e200.0005
Supplicants    : 2 / 2 / 256             ReAuthMode   : Enable
TxTimer(s)     : ---   / 30              ReAuthTimer(s): 123   / 300
ReAuthSuccess  : 4                       ReAuthFail   : 0
SuppDetection  : Disable
VLAN(s): 2-5

VLAN(Dynamic) Supplicants
VLAN 2      2
>
```

Figure 31-16: Displaying the status information about each VLAN for IEEE 802.1X VLAN-based authentication (dynamic) (with the detail option specified)

```
> show dot1x vlan dynamic 2 detail
Date 20XX/10/17 17:57:03 UTC
VLAN(Dynamic)
AccessControl  : Multiple-Auth          PortControl  : Auto
Status         : ---                     Last EAPOL   : 0012.e200.0005
Supplicants    : 2 / 2 / 256             ReAuthMode   : Enable
TxTimer(s)     : ---   / 30              ReAuthTimer(s): 123   / 300
ReAuthSuccess  : 4                       ReAuthFail   : 0
SuppDetection  : Disable
VLAN(s): 2-5

 Supplicants MAC    Status        AuthState      BackEndState   ReAuthSuccess
                    SessionTime(s) Date/Time
 [VLAN 2]                         VLAN(Dynamic) Supplicants : 2
 0012.e200.0005     Authorized    Authenticated  Idle           0
                    177           20XX/10/17 17:55:00
 0012.e200.0006     Authorized    Authenticated  Idle           0
                    5             20XX/10/17 17:56:58
>
```

Figure 31-17: Displaying the status information for all types of IEEE 802.1X authentication

```
> show dot1x detail
Date 20XX/04/08 17:57:03 UTC
System 802.1X : Enable
   AAA Authentication Dot1x   : Enable
       Authorization Network  : Enable
       Accounting Dot1x       : Enable

Port  0/1
AccessControl  : ---                     PortControl  : Auto
Status         : Authorized              Last EAPOL   : 0012.e200.0021
Supplicants    : 1 / 1                   ReAuthMode   : Enable
TxTimer(s)     : ---   / 30              ReAuthTimer(s): 123   / 300
ReAuthSuccess  : 4                       ReAuthFail   : 0
KeepUnauth(s)  : ---   / 3600

 Supplicants MAC    Status        AuthState      BackEndState   ReAuthSuccess
                    SessionTime(s) Date/Time
 0012.e200.0021     Authorized    Authenticated  Idle           0
                    177           20XX/04/08 17:55:00

Port  0/20
AccessControl  : Multiple-Auth          PortControl  : Auto
Status         : ---                     Last EAPOL   : 0012.e200.0001
Supplicants    : 2 / 2 / 64              ReAuthMode   : Enable
TxTimer(s)     : 15    / 30              ReAuthTimer(s): 123   / 300
ReAuthSuccess  : 4                       ReAuthFail   : 0
SuppDetection  : Shortcut

 Supplicants MAC    Status        AuthState      BackEndState   ReAuthSuccess
                    SessionTime(s) Date/Time
 0012.e200.0001     Authorized    Authenticated  Idle           0
                    177           20XX/04/08 17:55:00
 0012.e200.0002     Authorized    Authenticated  Idle           0
```

```
                        5                 20XX/04/08 17:56:58

ChGr  11
AccessControl  : Multiple-Auth              PortControl   : Auto
Status         : ---                        Last EAPOL    : 0012.e200.0011
Supplicants    : 2 / 2 / 64                 ReAuthMode    : Enable
TxTimer(s)     : 15    / 30                 ReAuthTimer(s): 123   / 300
ReAuthSuccess  : 4                          ReAuthFail    : 0
SuppDetection  : Shortcut

 Supplicants MAC    Status        AuthState      BackEndState   ReAuthSuccess
                    SessionTime(s) Date/Time
 0012.e200.0011     Authorized    Authenticated  Idle           0
                    177           20XX/04/08 17:55:00
 0012.e200.0012     Authorized    Authenticated  Idle           0
                    5             20XX/04/08 17:56:58

VLAN  20
AccessControl  : Multiple-Auth              PortControl   : Auto
Status         : ---                        Last EAPOL    : 0012.e200.0003
Supplicants    : 2 / 2 / 256                ReAuthMode    : Enable
TxTimer(s)     : ---   / 30                 ReAuthTimer(s): 123   / 300
ReAuthSuccess  : 4                          ReAuthFail    : 0
SuppDetection  : Disable
Port(s): 0/1-15, ChGr 1-5
Force-Authorized Port(s): 0/4,8-15, ChGr 1-5

 Supplicants MAC    Status        AuthState      BackEndState   ReAuthSuccess
                    SessionTime(s) Date/Time
 [Port 0/1]
 0012.e200.0003     Authorized    Authenticated  Idle           0
                    177           20XX/04/08 17:55:00
*0012.e200.0004     Authorized    Authenticated  Idle           0
                    5             20XX/04/08 17:56:58

VLAN(Dynamic)
AccessControl  : Multiple-Auth              PortControl   : Auto
Status         : ---                        Last EAPOL    : 0012.e200.0005
Supplicants    : 2 / 2 / 256                ReAuthMode    : Enable
TxTimer(s)     : ---   / 30                 ReAuthTimer(s): 123   / 300
ReAuthSuccess  : 4                          ReAuthFail    : 0
SuppDetection  : Disable
VLAN(s): 2-5

 Supplicants MAC    Status        AuthState      BackEndState   ReAuthSuccess
                    SessionTime(s) Date/Time
 [VLAN 2]           VLAN(Dynamic) Supplicants : 2
 0012.e200.0005     Authorized    Authenticated  Idle           0
                    177           20XX/04/08 17:55:00
 0012.e200.0006     Authorized    Authenticated  Idle           0
                    5             20XX/04/08 17:56:58
>
```

Display items

Table 31-3: 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.)

Item		Meaning	Displayed detailed information
	Authorization Network	Displays whether VLAN allocation from RADIUS is enabled or disabled when VLAN-based authentication (dynamic) is used.	1. Enable (VLAN allocation from RADIUS is enabled.) 2. Disable (VLAN allocation from RADIUS is disabled.)
	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.)
Port/ChGr/VLAN/VLAN(Dynamic)		Indicates the type of authentication. Port <nif no.>/<port no.>: Indicates a port for port-based authentication. ChGr <channel group number>: Indicates a channel group for port-based authentication. VLAN <vlan id>: Indicates a VLAN ID for VLAN-based authentication (static). VLAN(Dynamic): Indicates VLAN-based authentication (dynamic).	
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
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>	

Item	Meaning	Displayed detailed information
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-based authentication: For port or a channel group to be authenticated VLAN-based authentication (static or dynamic): For VLAN 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
Port(s)	(For VLAN-based authentication (static) only) This item displays the list for ports belonging to the VLAN to be authenticated.	
Force-Authorized Port(s)	(For VLAN-based authentication (static) only) This item displays the list of ports excluded from authentication.	
VLAN(s)	(For VLAN-based authentication (dynamic) only) This item displays the list of VLANs to be authenticated.	
VLAN(Dynamic) Supplicants	(For VLAN-based authentication (dynamic) only) This item displays the number of supplicants already authenticated.	
Supplicant MAC	The supplicant's MAC address. Supplicants with an asterisk (*) on the left are being quarantined.	

Item	Meaning	Displayed detailed information
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.	
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

Response messages

Table 31-4: List of response messages for the show dot1x command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

Message	Description
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 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.
No operational VLAN(Dynamic).	VLAN-based authentication (dynamic) was not configured. Check the authentication mode set by the configuration.
No operational VLAN.	There are no available VLANs. 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.

Notes

Information about the supplicants for which VLAN dynamic assignment failed in VLAN-based authentication (dynamic) is not displayed. Execute the "show dot1x logging" and "show vlan mac-vlan" commands to make sure the information is not displayed.

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> | vlan {
<vlan id list> | dynamic} }]
```

Input mode

User mode and administrator mode

Parameters

{ port <port list> | channel-group-number <channel group list> | vlan {<vlan id list> | dynamic}

port <port list>

Clears statistics for port-based authentication of the specified physical port in list format. 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 statistics for port-based authentication of the specified channel group in list format. For details about how to specify <channel group list>, see "Specifiable values for parameters".

vlan <vlan id list>

Clears statistics for VLAN-based authentication (static) of the specified VLAN 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.

vlan dynamic

Clears statistics for VLAN-based authentication (dynamic) to zero.

Behavior when this parameter is omitted:

Statistics for all types of authentication are cleared to zero.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 31-18: Clearing the IEEE 802.1X authentication statistics to zero

```
> clear dot1x statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 31-5: List of response messages for the clear dot1x statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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 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.
No operational VLAN(Dynamic).	VLAN-based authentication (dynamic) was not configured. Check the authentication mode set by the configuration.
No operational VLAN.	There are no available VLANs. 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.

Notes

If this command is executed, the MIB information of the IEEE 802.1X MIB group is also cleared to zero.

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> | vlan {
<vlan id list> | dynamic [<vlan id list>]} | supplicant-mac <mac address> }] [-f]
```

Input mode

User mode and administrator mode

Parameters

{ port <port list> | channel-group-number <channel group list> | vlan {<vlan id list> | dynamic [<vlan id list>]} | supplicant-mac <mac address> }

> port <port list>
>
>> Initializes the authentication status for the ports specified in list format for port-based authentication. 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>
>
>> Initializes the authentication status for the channel groups specified in list format for port-based authentication. For details about how to specify <channel group list>, see "Specifiable values for parameters".
>
> vlan <vlan id list>
>
>> Initializes the authentication status of the VLANs specified in list format for VLAN-based authentication (static).
>>
>> 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.
>
> vlan dynamic <vlan id list>
>
>> Initializes the authentication status of the VLANs specified in list format for VLAN-based authentication (dynamic).
>>
>> 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.
>>
>> If <vlan id list> is omitted, the authentication status of all VLANs in VLAN-based authentication (dynamic) is initialized.
>
> 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.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 31-19: Initializing all the IEEE 802.1X authentication statuses 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 statuses on the relevant ports or VLANs are initialized, and communication is lost. To restore communication, re-authentication is necessary.

Response messages

Table 31-6: List of response messages for the clear dot1x auth-state command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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 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.
No operational VLAN(Dynamic).	VLAN-based authentication (dynamic) was not configured. Check the authentication mode set by the configuration.
No operational VLAN.	There are no available VLANs. 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.

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>, channel-group-number <channel group list>, vlan <vlan id list>, or vlan dynamic, EAP-Failure and EAP-Req/Id frames are multicasted once to the specified type of IEEE 802.1X authentication.

- If the parameter is vlan dynamic <vlan id list> and there is an authentication terminal, an EAP-Failure frame is unicasted once to the authentication terminal, and an EAP-Req/Id frame is multicasted once to the specified type of IEEE 802.1X authentication.

- If the parameter is supplicant-mac <mac address>, an EAP-Failure frame is unicasted 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> | vlan {<v
lan id list> | dynamic [<vlan id list>]} | supplicant-mac <mac address> }] [-f]
```

Input mode

User mode and administrator mode

Parameters

{ port <port list> | channel-group-number <channel group list> | vlan {<vlan id list> | dynamic [<vlan id list>]} | supplicant-mac <mac address> }

port <port list>

Initiates re-authentication for the ports specified in list format for port-based authentication. 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>

Initiates re-authentication for the channel groups specified in list format for port-based authentication. For details about how to specify <channel group list>, see "Specifiable values for parameters".

vlan <vlan id list>

Re-authenticates the authentication status of the VLANs specified in list format for VLAN-based authentication (static).

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.

vlan dynamic <vlan id list>

Re-authenticates the authentication status of the VLANs specified in list format for VLAN-based authentication (dynamic).

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.

If <vlan id list> is omitted, re-authentication for all VLANs for VLAN-based authentication (dynamic) is initiated.

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.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 31-20: Re-authenticating all the IEEE 802.1X-authenticated ports and VLANs 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.

Response messages

Table 31-7: List of response messages for the reauthenticate dot1x command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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 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.
No operational VLAN(Dynamic).	VLAN-based authentication (dynamic) was not configured. Check the authentication mode set by the configuration.
No operational VLAN.	There are no available VLANs. 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.

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.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 31-21: Restarting the IEEE 802.1X program

```
> restart dot1x
802.1X restart OK?  (y/n) : y
>
```

Figure 31-22: Restarting the IEEE 802.1X program (when the –f parameter is 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.

Response messages

Table 31-8: List of response messages for the restart dot1x command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Dot1x doesn't seem to be running.	The IEEE 802.1X setting has not been enabled. Check 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.

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

Operation when a stack configuration is used

This command is not supported.

Example

Figure 31-23: Taking an online dump of the IEEE 802.1X program

```
> dump protocols dot1x
>
```

Display items

None

Impact on communication

None

Response messages

Table 31-9: List of response messages for the dump protocols dot1x command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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 setting has not been enabled. Check the configuration.

Message	Description
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.

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.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 31-24: Displaying IEEE 802.1X action log messages

```
> show dot1x logging
Date 20XX/01/23 13:32:00 UTC
No=1:Jan 23 13:31:43:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=0/1 VLAN=10 Login succeeded. ; New S
upplicant Auth Success.
 No=16:Jan 23 13:16:55:NORMAL:LOGOUT: MAC=0012.e200.0001 PORT=0/1 VLAN=10 Force Logout. ; Port
link down.
 No=2:Jan 23 13:16:10:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=0/1 VLAN=10 Login succeeded. ; Supp
licant Re-Auth Success.
 No=1:Jan 23 13:15:10:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=0/1 VLAN=10 Login succeeded. ; New
Supplicant Auth Success.
 No=30:Jan 23 13:10:34:NOTICE:LOGIN: MAC=0012.e200.0001 PORT=0/1 VLAN=10 Login failed. ; RADIUS
 authentication failed.
```

Display items

The following table shows the items displayed when an IEEE 802.1X action log message is displayed.

Table 31-10: Items displayed for IEEE 802.1X action log messages

Item	Meaning	Displayed detailed information
Level	Levels of action log messages	Severity of a log message
<log>	Action log message	Contents of a registered action log message

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 31-13: 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 31-11: Log ID and type of action log messages"

- Log type: "Table 31-11: Log ID and type of action log messages"

- Additional information: "Table 31-12: Additional information"

- List of messages: "Table 31-13: List of action log messages"

Table 31-11: 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 a communication failure.
ERROR	SYSTEM	Indicates a failure while IEEE 802.1X program is running.

Table 31-12: 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 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 31-13: List of action log messages

No.	Log ID	Log type	Message text	Meaning and action	Added info
1	NOR-MAL	LOGIN	Login succeeded. ; New Supplicant Auth Success.	[Meaning] A new supplicant was authenticated successfully. [Action] None	MAC address Port number or channel group number VLAN ID
2	NOR-MAL	LOGIN	Login succeeded. ; Supplicant Re-Auth Success.	[Meaning] A supplicant was re-authenticated successfully. [Action] None	MAC address Port number or channel group number VLAN ID
3	NOR-MAL	LOGIN	Login succeeded. ; Limited by ACL.	[Meaning] 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	NOR-MAL	LO-GOUT	Logout succeeded.	[Meaning] 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	NOR-MAL	LO-GOUT	Force logout. ; "clear dot1x auth-state" command succeeded.	[Meaning] Authentication has been canceled by a command. [Action] None	MAC address Port number or channel group number VLAN ID
12	NOR-MAL	LO-GOUT	Force logout. ; The supplicant was cleared, because it was registered to MAC VLAN with the configuration.	[Meaning] An attempt to authenticate the relevant suppliant was canceled because the MAC address was configured for the MAC VLAN. [Action] None	MAC address Port number or channel group number VLAN ID
13	NOR-MAL	LO-GOUT	Force logout. ; The supplicant was cleared, because it was registered to mac-address-table with the configuration.	[Meaning] 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	NOR-MAL	LO-GOUT	Force logout. ; The status of port was changed to Unauthorized, because another supplicant was detection in single mode.	[Meaning] The authentication status has been changed to Unauthorized because multiple supplicants were detected on a single mode port.	MAC address Port number or channel group number VLAN ID

No.	Log ID	Log type	Message text	Meaning and action	Added info
				[Action] None	
15	NOR-MAL	LO-GOUT	Force logout. ; Dot1x configuration deleted.	[Meaning] 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
16	NOR-MAL	LO-GOUT	Force logout. ; Port link down.	[Meaning] 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	NOR-MAL	LO-GOUT	Force logout. ; VLAN status down.	[Meaning] Authentication has been canceled because the VLAN has gone down or the VLAN was deleted from the configuration of the port. [Action] None	MAC address Port number or channel group number VLAN ID
18	NOR-MAL	LO-GOUT	Force logout. ; Re-Auth failed.	[Meaning] Re-authentication processing failed. [Action] None	MAC address Port number or channel group number VLAN ID
19	NOR-MAL	LO-GOUT	Force logout. ; Could not be registered to hardware.	[Meaning] 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
30	NOTICE	LOGIN	Login failed. ; RADIUS authentication failed.	[Meaning] 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

No.	Log ID	Log type	Message text	Meaning and action	Added info
31	NOTICE	LOGIN	Login failed. ; RADIUS authentication failed. (Re-Auth)	[Meaning] 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
32	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: "aaa authorization network default" is not configured.)	[Meaning] VLAN dynamic assignment failed because the "aaa authorization network default" configuration command was not configured. [Action] Set the "aaa authorization network default" configuration command.	MAC address Port number or channel group number
33	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: No Tunnel-Type Attribute.)	[Meaning] VLAN dynamic assignment 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).)	[Meaning] VLAN dynamic assignment 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
35	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: No Tunnel-Medium-Type Attribute.)	[Meaning] VLAN dynamic assignment 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).)	[Meaning] VLAN dynamic assignment 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

No.	Log ID	Log type	Message text	Meaning and action	Added info
37	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: No Tunnel-Private-Group-ID Attribute.)	[Meaning] VLAN dynamic assignment 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.)	[Meaning] VLAN dynamic assignment 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.)	[Meaning] VLAN dynamic assignment 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
40	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The Port doesn't belong to VLAN.)	[Meaning] VLAN dynamic assignment failed because the authentication port did not belong to the VLAN ID. [Action] Make sure the VLAN ID set for the Tunnel-Private-Group-ID attribute in the Accept packet to be sent by the RADIUS server is included in the VLAN IDs set for the authentication port by the "switchport mac" configuration command with the vlan parameter specified.	MAC address Port number or channel group number VLAN ID
41	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The VLAN ID is not set to radius-vlan.)	[Meaning] VLAN dynamic assignment failed because the VLAN ID was not subject to VLAN-based authentication (dynamic). [Action]	MAC address Port number or channel group number VLAN ID

No.	Log ID	Log type	Message text	Meaning and action	Added info
				Make sure the VLAN ID set for the Tunnel-Private-Group-ID attribute in the Accept packet to be sent by the RADIUS server is included in the VLAN IDs set by the "dot1x vlan dynamic radius-vlan" configuration command.	
42	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The VLAN status is disabled.)	[Meaning] VLAN dynamic assignment failed because the VLAN is disabled for VLAN-based authentication (dynamic). [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.	[Meaning] 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.	[Meaning] 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)	[Meaning] 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	Meaning and action	Added info
46	NOTICE	LOGIN	Login failed. ; Failed to authenticate the supplicant because it could not be registered to MAC VLAN.(code=x)	[Meaning] 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.	[Meaning] 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.)	[Meaning] 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.	[Meaning] 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.	[Meaning] An invalid EAP over RADIUS frame has been received. [Action] Check whether there is any problem with the following:	—

No.	Log ID	Log type	Message text	Meaning and action	Added info
				• The contents of packets sent by the RADIUS server • Transmission line quality	
82	WARN-ING	SYS-TEM	Failed to connect to RA-DIUS server.	[Meaning] 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 ad-dress
83	WARN-ING	SYS-TEM	Failed to connect to RA-DIUS server.	[Meaning] 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 ad-dress
84	WARN-ING	SYS-TEM	Failed to connect to Ac-counting server.	[Meaning] An attempt to connect to the ac-counting server failed. [Action] Check the following: • Communication between the Switch and the accounting server is available. • The accounting server function is enabled.	Server IP ad-dress
85	WARN-ING	SYS-TEM	Failed to connect to Ac-counting server.	[Meaning] An attempt to connect to the ac-counting server failed. [Action] Check the following: • Communication between the Switch and the accounting server is available. • The accounting server function is enabled.	Server IPv6 ad-dress
86	WARN-ING	SYS-TEM	Failed in the name reso-lution with the DNS server.	[Meaning] Name resolution by the DNS server failed. [Action] Change the server set by the "ra-dius-server host" configuration command to IPv4 or IPv6 ad-dress.	Server name

No.	Log ID	Log type	Message text	Meaning and action	Added info
90	ERROR	SYS-TEM	Failed to open socket.	[Meaning] 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

Response messages

Table 31-14: List of response messages for the show dot1x logging command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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 setting has not been enabled. Check 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.

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

Operation when a stack configuration is used

This command is not supported.

Example

Figure 31-25: Clearing IEEE 802.1X action log messages

```
> clear dot1x logging
>
```

Display items

None

Impact on communication

None

Response messages

Table 31-15: List of response messages for the clear dot1x logging command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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 setting has not been enabled. Check 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.

Notes

None

32 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 a name with 1 to 16 characters.

<password>

Specify a password.

Only alphanumeric characters can be used, and the characters are case sensitive. Specify a name with 1 to 16 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 or legacy 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.

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 32-1: List of response messages for the set web-authentication user command

Message	Description
Already user '<user name>' exists.	The specified user has already been registered.
Can't execute.	The command could not be executed. Re-execute the command.
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.
The number of users exceeds 300.	The number of users to be registered exceeds 300.
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

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 a name with 1 to 16 characters.

<old password>

> Specify the password before the change.
> Only alphanumeric characters can be used, and the characters are case sensitive. Specify a name with 1 to 16 characters.

<new password>

> Specify the password after the change.
> Only alphanumeric characters can be used, and the characters are case sensitive. Specify a name with 1 to 16 characters.

Operation when a stack configuration is used

This command is not supported.

Example

To change the password for user "USER01":

```
# set web-authentication passwd USER01 user0101 user1111
```

Display items

None

Impact on communication

None

Response messages

Table 32-2: List of response messages for the set web-authentication passwd command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
The old-password is different.	The old password for the specified user is incorrect.
Unknown user '<user name>'.	The specified user has not been registered.
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

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 a name with 1 to 16 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.

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 32-3: List of response messages for the set web-authentication vlan command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

Message	Description
Unknown user '<user name>'.	The specified user has not been registered.
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

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 a name with 1 to 16 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.

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 32-4: List of response messages for the remove web-authentication user command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
Unknown user '<user name>'.	The specified user has not been registered.
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

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.

Operation when a stack configuration is used

This command is not supported.

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
  username          VLAN
  0123456789012345     3
  USER01            4094
  ```

- 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
  username          VLAN
  0123456789012345     4
  USER02            4094
  USER03               2
  ```

Display items

Table 32-5: 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
username	User name	A registered user name
VLAN	VLAN	The VLAN set for the registered user

Impact on communication

None

Response messages

Table 32-6: List of response messages for the show web-authentication user command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

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

Operation when a stack configuration is used

This command is not supported.

Example

The following commands show examples of displaying authenticated users:

- When the authentication mode is legacy mode:
  ```
  # show web-authentication login
  Date 20XX/10/15 10:52:49 UTC
  Total user counts:2
  Username
  VLAN    MAC address      Login time             Limit time
  0123456789012345678901234567890 1
     3    0012.e2e3.9166   20XX/11/15 09:58:04 UTC  00:10:20
  USER01
  4094    0012.e268.7527   20XX/11/15 10:10:23 UTC  00:20:35
  ```

- When the authentication mode is dynamic VLAN mode:
  ```
  # show web-authentication login
  Date 20XX/10/15 10:52:49 UTC
  Total user counts:2
  F Username
    VLAN    MAC address      Login time             Limit time
  * 0123456789012345678901234567890 1
       3    0012.e2e3.9166   20XX/10/15 09:58:04 UTC  00:10:20
  * USER01
    4094    0012.e268.7527   20XX/10/15 10:10:23 UTC  00:20:35
  ```

- When the authentication mode is fixed VLAN mode:
  ```
  # show web-authentication login
  Date 20XX/10/15 10:52:49 UTC
  Total user counts:2
  F Username
    VLAN    MAC address      Port  IP address
    Login time             Limit time
  * 0123456789012345678901234567890 1
       3    0012.e2e3.9166   0/5   192.168.0.1
    20XX/10/15 09:58:04 UTC  00:10:20
  * USER01
    4094    0012.e268.7527   0/6   192.168.1.10
    20XX/10/15 10:10:23 UTC  00:20:35
  ```

Display items

Table 32-7: Items displayed for authenticated users

Item	Meaning	Displayed detailed information
Total user counts	Total number of users	The number of the authenticated, currently logged-in users
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
MAC address	MAC address	The MAC addresses of the authenticated, currently logged-in users
Port	Port number	The port numbers of the physical ports accommodating the authenticated, currently logged-in users (displayed for fixed VLAN mode)
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

Response messages

Table 32-8: List of response messages for the show web-authentication login command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

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.

Operation when a stack configuration is used

This command is not supported.

Example

- When the parameter is omitted:
  ```
  # show web-authentication logging
  Date 20XX/11/15 10:52:49 UTC
   No=1:Nov 15 00:09:50:NORMAL:LOGIN:MAC=0012.e200.0001 USER=testdata1 Login succeeded.
   No=2:Nov 15 00:10:10:NORMAL:LOGOUT: MAC=0012.e200.0001 USER=testdata1 Logout succeeded.
   No=90:Nov 15 00:09:55:NORMAL:SYSTEM: connection failed ; L2MacManager.
  ```

- When "user" is specified for the parameter:
  ```
  # show web-authentication logging user
  Date 20XX/11/15 11:13:15 UTC
   No=1:Nov 15 00:09:50:NORMAL:LOGIN: MAC=0012.e200.0001 USER=testdata1 Login succeeded.
   No=2:Nov 15 00:10:10:NORMAL:LOGOUT: MAC=0012.e200.0001 USER=testdata1 Logout succeeded.
  ```

Display items

Table 32-9: Display items of Web authentication action log messages

Item	Meaning	Displayed detailed information
Level	Levels of action log messages	Severity of a log message
<log>	Action log message	Contents of a registered action log message

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 32-12: 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 32-10: Log ID and type of action log messages"
- Log type: "Table 32-10: Log ID and type of action log messages"
- Additional information: "Table 32-11: Additional information"
- List of messages: "Table 32-12: List of action log messages"

Table 32-10: 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.
ERROR	SYSTEM	Indicates a communication failure or a failure while the Web authentication program is running.

Table 32-11: 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	Indicates the port number.

Table 32-12: List of action log messages

No.	Log ID	Log type	Message text	Meaning and action	Added info
1	NOR-MAL	LOGIN	Login succeeded.	[Meaning] The client was successfully authenticated. [Action] None	MAC address User name IP address[1] VLAN ID[1] Port number[1]

No.	Log ID	Log type	Message text	Meaning and action	Added info
2	NOR-MAL	LO-GOUT	Logout succeeded.	[Meaning] The client successfully canceled authentication. [Action] None	MAC address User name IP address[#1] VLAN ID[#1] Port number[#1]
3	NOR-MAL	LOGIN	Login update succeeded.	[Meaning] The user's login time was successfully updated. [Action] None	MAC address User name IP address[#1] VLAN ID[#1] Port number[#1]
4	NOR-MAL	LO-GOUT	Force logout ; clear web-authentication command succeeded.	[Meaning] Authentication has been canceled by a command. [Action] None	MAC address User name IP address[#1] VLAN ID[#1] Port number[#1]
5	NOR-MAL	LO-GOUT	Force logout ; Connection time was beyond a limit.	[Meaning] Authentication was canceled because the maximum connection time was exceeded. [Action] None	MAC address User name IP address[#1] VLAN ID[#1] Port number[#1]
6	NOR-MAL	LO-GOUT	Force logout ; mac-address-table aging.	[Meaning] 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[#1] VLAN ID[#1] Port number[#1]
7	NOR-MAL	LO-GOUT	Force logout ; VLAN deleted.	[Meaning] Authentication was canceled because a VLAN for Web authentication was deleted. 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 configuration for the VLAN settings.	MAC address User name VLAN ID

No.	Log ID	Log type	Message text	Meaning and action	Added info
8	NOR-MAL	LO-GOUT	Force logout ; Authentic method changed (RADIUS <-> Local).	[Meaning] Authentication was canceled because the authentication method was switched between the RADIUS authentication and local authentication. [Action] None	MAC address User name IP address[#1] VLAN ID Port number[#1]
10	NOTICE	LOGIN	Login failed ; User name not found to web authentication DB.	[Meaning] 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.	User name
11	NOTICE	LOGIN	Login failed ; Password not found to web authentication DB. [Password=[password]]	[Meaning] 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
12	NOTICE	LOGIN	Login failed ; ARP resolution.	[Meaning] Authentication failed because ARP resolution of the client PC's IP address failed. [Action] Log in again.	User name IP address
13	NOTICE	LO-GOUT	Logout failed ; ARP resolution.	[Meaning] Authentication could not be canceled because ARP resolution of the client PC's IP address failed. [Action] Log out again.	User name[#1] IP address
14	NOTICE	LOGIN	Login failed ; Double login.	[Meaning] 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.	MAC address User name

No.	Log ID	Log type	Message text	Meaning and action	Added info
				• 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.	
15	NOTICE	LOGIN	Login failed ; Number of login was beyond limit.	[Meaning] 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.	[Meaning] Authentication cannot be performed because the MAC address could not be registered due to hardware specifications. [Action] Log in from another PC.	MAC address User name
17	NOTICE	LOGIN	Login failed ; VLAN not specified.	[Meaning] 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.	[Meaning] Authentication could not be performed because registration of the MAC address failed. [Action] Log in again.	MAC address User name

No.	Log ID	Log type	Message text	Meaning and action	Added info
19	NOTICE	LO-GOUT	Logout failed ; MAC address could not delete.	[Meaning] Authentication could not be performed because deletion of the MAC address failed. [Action] Log out again.	MAC address[#2] User name[#1, #2] VLAN ID[#1, #2] Port number[#1, #2]
20	NOTICE	LOGIN	Login failed ; RADIUS authentication failed.	[Meaning] Authentication could not be performed because RADIUS authentication failed. [Action] Use the correct user ID to log in.	MAC address User name IP address[#1] VLAN ID[#1] Port number[#1]
21	NOTICE	LOGIN	Login failed ; Failed to connection to RADIUS server.	[Meaning] 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[#1] VLAN ID[#1] Port number[#1]
22	NOTICE	LOGIN	Login failed ; Connection failed L2MacManager.	[Meaning] Authentication failed because an attempt to communicate with the VLAN program failed. [Action] Log in again. If this message appears frequently, execute the "restart vlan" command with the mac-manager parameter specified.	MAC address User name
23	NOTICE	LOGIN	Login failed ; L2MacManager failed.	[Meaning] Authentication failed because a notification from the VLAN program was received indicating that authentication could not performed. [Action] Log in again. If this message appears frequently, execute the "restart vlan" command with the mac-manager parameter specified.	MAC address User name

No.	Log ID	Log type	Message text	Meaning and action	Added info
24	NOTICE	LO-GOUT	Logout failed ; L2MacManager failed.	[Meaning] Canceling authentication failed because a notification from the VLAN program indicating that authentication cancellation could not be performed was received. The cause is either of the following: • IEEE 802.1X authentication was performed on the same PC after Web authentication. • After Web authentication, the same MAC address as that of the authenticated terminal is registered by using the "mac-address" configuration command. [Action] Analyze the cause and log in again.	MAC address
25	NOTICE	LOGIN	Login failed ; Double login. (L2MacManager)	[Meaning] Authentication failed because a notification from the VLAN 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 MAC address for the terminal to be authenticated had already been registered by the "mac-address" configuration command. [Action] Use another terminal to log in.	MAC address User name VLAN ID
26	NOR-MAL	LO-GOUT	Force logout ; VLAN deleted.	[Meaning] When the mode is in legacy mode, authentication of the user logged in to a VLAN was canceled because the VLAN set for the interface was deleted. [Action] Configure the VLAN (MAC VLAN) again.	[Legacy mode] MAC address User name VLAN ID

No.	Log ID	Log type	Message text	Meaning and action	Added info
				[Meaning] 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.	[Fixed VLAN mode or Dynamic VLAN mode] MAC address User name IP address VLAN ID Port number
27	NOTICE	LOGIN	Login failed ; VLAN not specified.	[Meaning] In legacy mode, authentication cannot be performed because the authentication request was sent from a VLAN that was not set for the interface. [Action] Correctly configure the VLAN again.	MAC address User name VLAN ID
28	NOR-MAL	LO-GOUT	Force logout ; Polling time out.	[Meaning] Authentication was canceled because disconnection of an authenticated terminal was detected. [Action] None	MAC address User name IP address VLAN ID Port number
29	NOR-MAL	LO-GOUT	Force logout ; Client moved.	[Meaning] 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
31	NOR-MAL	LO-GOUT	Force logout ; Port not specified.	[Meaning] 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
32	NOTICE	LOGIN	Login update failed.	[Meaning] 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	Meaning and action	Added info
33	NOR-MAL	LO-GOUT	Force logout ; Port link down.	[Meaning] 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
34	NOTICE	LOGIN	Login failed ; Port not specified.	[Meaning] 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
39	NOTICE	LOGIN	Login failed ; VLAN not specified.	[Meaning] 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
40	NOR-MAL	LO-GOUT	Force logout ; Ping packet accepted.	[Meaning] Authentication of the user was canceled because a logout ping was received. [Action] None	MAC address User name IP address VLAN ID Port number
41	NOR-MAL	LO-GOUT	Force logout ; Other authentication program.	[Meaning] 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
48	NOR-MAL	LO-GOUT	Force logout ; Program stopped.	[Meaning] Authentication of all users was canceled because the Web authentication program has stopped.	MAC address User name IP address VLAN ID Port number

No.	Log ID	Log type	Message text	Meaning and action	Added info
				[Action] If you still want to authenticate users through Web authentication, set the configuration.	
49	NOR-MAL	LO-GOUT	Force logout ; Authentic mode had changed (dynamic vlan -> static vlan).	[Meaning] Authentication of all users was canceled because the authentication method was switched from the legacy mode or dynamic VLAN mode to the fixed VLAN mode. [Action] None	MAC address User name IP address[#1] VLAN ID Port number[#1]
50	NOR-MAL	LO-GOUT	Force logout ; Authentic mode had changed (static vlan -> dynamic vlan).	[Meaning] Authentication of all users was canceled because the authentication method was switched from the fixed VLAN mode to the legacy mode or dynamic VLAN mode. [Action] None	MAC address User name IP address VLAN ID Port number
51	NOTICE	LOGIN	Login failed ; IP address is not right.	[Meaning] In fixed VLAN mode or dynamic VLAN mode, login operation was performed by using an IP address other than Web authentication IP address. [Action] Log in by using the Web authentication IP address.	User name IP address
52	NOR-MAL	LO-GOUT	Force logout ; Authentic mode had changed (Legacy -> dynamic vlan).	[Meaning] All authentications were canceled because the authentication method was changed from the legacy mode to the dynamic VLAN mode. [Action] None	MAC address User name VLAN ID
53	NOR-MAL	LO-GOUT	Force logout ; Authentic mode had changed (dynamic vlan -> Legacy).	[Meaning] All authentications were canceled because the authentication method was changed from the dynamic VLAN mode to the legacy mode. [Action] None	MAC address User name IP address VLAN ID Port number

No.	Log ID	Log type	Message text	Meaning and action	Added info
54	NOR-MAL	LOGIN	Force login succeed-ed.	[Meaning] Forced authentication succeeded. [Action] None	MAC address User name IP address VLAN ID Port number
55	NOR-MAL	LOGIN	Force login update succeeded.	[Meaning] Updating of the user's login time by forced authentication was success-ful. [Action] None	MAC address User name IP address VLAN ID Port number
56	NOTICE	LOGIN	Login failed ; Number of login was beyond limit of port.	[Meaning] 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
57	NOR-MAL	LO-GOUT	Force logout ; Num-ber of login was be-yond limit of port.	[Meaning] Authentication was canceled be-cause the number of ports after mov-ing terminals exceeded the maximum allowable number. [Action] Reduce the number of terminals to be authenticated.	MAC address User name IP address VLAN ID Port number
82	NOR-MAL	SYSTEM	Accepted clear auth-state command.	[Meaning] A request issued by the "clear web-authentication auth-state" command to cancel authentication was re-ceived. [Action] None	―
83	NOR-MAL	SYSTEM	Accepted clear statis-tics command.	[Meaning] A request issued by the "clear web-authentication statistics" command to clear statistics was received. [Action] None	―

No.	Log ID	Log type	Message text	Meaning and action	Added info
84	NOR-MAL	SYSTEM	Accepted commit command.	[Meaning] A commit notification issued by the "commit web-authentication" command for the internal DB was received. [Action] None	—
85	NOR-MAL	SYSTEM	Accepted dump command.	[Meaning] A dump output request issued by the "dump protocols web-authentication" command was received. [Action] None	—
86	NOR-MAL	LO-GOUT	Force logout ; MAC address not found L2MacManager.	[Meaning] A MAC address is available for Web authentication, but it is not available for the VLAN program. Therefore, an attempt was made to register a MAC address in the VLAN program, but it failed and authentication is canceled. [Action] Log in again.	MAC address User name
87	NOR-MAL	SYSTEM	MAC address existed in the L2MacManager.	[Meaning] A MAC address, which is available for the VLAN 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
88	ERROR	SYSTEM	WAD could not initialize.[error code]	[Meaning] 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

No.	Log ID	Log type	Message text	Meaning and action	Added info
89	ERROR	SYSTEM	Connection failed ; Operation command. error=[error-code]	[Meaning] 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.	[Meaning] An attempt to communicate with the VLAN program was made, but failed. [Action] If this message appears frequently, execute the "restart vlan" command with the mac-manager parameter specified.	—
92	ERROR	SYSTEM	Disconnection failed ; L2MacManager.	[Meaning] Communication with the VLAN program was interrupted. [Action] If this message appears frequently, execute the "restart vlan" command with the mac-manager parameter specified.	—
96	ERROR	SYSTEM	Program failed ; Log-in information could not delete.	[Meaning] An attempt to delete the login information failed. [Action] If this message appears frequently, use the "restart web-authentication" command to restart the Web authentication program.	—
97	ERROR	SYSTEM	Connection failed ; Driver. [error code]	[Meaning] Connection with the driver 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

No.	Log ID	Log type	Message text	Meaning and action	Added info
98	NOTICE	LO-GOUT	Logout failed ; User is not authenticating.	[Meaning] 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.	[Meaning] 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	NOR-MAL	SYSTEM	Accepted clear logging command.	[Meaning] A request to delete the action log by the "clear web-authentication logging" command was received. [Action] None	—
103	NOR-MAL	SYSTEM	Synchronized ; Wad -> L2MacManager.	[Meaning] 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.	MAC address User name
104	NOR-MAL	LO-GOUT	Force logout ; L2MacManager synchronize.	[Meaning] The authentication status was cleared 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.	MAC address User name

No.	Log ID	Log type	Message text	Meaning and action	Added info
105	NOTICE	LOGIN	Login failed ; VLAN suspended.	[Meaning] An authentication error occurred because the VLAN used by the login user to be switched after authentication was in disable state. [Action] Enable the post-authentication VLAN, and then log in again.	MAC address User name VLAN ID
106	NOR-MAL	LO-GOUT	Force logout ; VLAN suspended.	[Meaning] Authentication was canceled because the status of the VLAN for the login user changed to disable. [Action] Enable the post-authentication VLAN, and then log in again.	MAC address User name IP address[#1] VLAN ID Port number[#1]
110	NOR-MAL	SYSTEM	Accepted clear dead-interval-timer command.	[Meaning] A request issued by the "clear web-authentication dead-interval-timer" command for recovering the dead interval function was received. [Action] None	—
255	ERROR	SYSTEM	The other error. [error-code]	[Meaning] 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 Web authentication.	Error code

Legend: — Not applicable

#1: Displayed when the mode is in fixed VLAN mode or dynamic VLAN mode.

#2: 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

Response messages

Table 32-13: List of response messages for the show web-authentication logging command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

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

Operation when a stack configuration is used

This command is not supported.

Example

- When the authentication mode is in legacy mode and the authentication method is local authentication with no registered VLANs:
```
# show web-authentication
Date 20XX/10/15 10:52:49 UTC
web-authentication Information:
   Authentic-mode   : Legacy
   Authentic-method : Local         Accounting-state : disable
         Max-timer : 60                   Max-user  : 256
        VLAN Count : 0                   Auto-logout : enable
   Syslog-send       : enable
   Jump-URL          : http://www.example.com/
   Web-port          : http  : 80          https : 443
```

- When the authentication mode is in legacy mode and the authentication method is local authentication with registered VLANs:
```
# show web-authentication
Date 20XX/10/15 10:52:49 UTC
web-authentication Information:
   Authentic-mode   : Legacy
   Authentic-method : Local         Accounting-state : disable
         Max-timer : 60                   Max-user  : 256
        VLAN Count : 16                  Auto-logout : disable
   Syslog-send       : enable
   Jump-URL          : http://www.example.com/
   Web-port          : http  : 80          https : 443

VLAN Information:
          VLAN ID :    5,10,15,20,25,30,35,40,1000-1007
```

- When the authentication mode is in fixed VLAN mode and the authentication method is RADIUS authentication with registered VLANs:
```
# show web-authentication
Date 20XX/10/15 10:52:49 UTC
web-authentication Information:
   Authentic-mode   : Static-VLAN
   Authentic-method : RADIUS        Accounting-state : disable
   Dead-interval    : 10
         Max-timer : 60                   Max-user  : 256
        VLAN Count : -                   Auto-logout : -
   Syslog-send       : enable
```

```
Alive-detection  : enable
          timer : 60     interval-timer : 3     count : 3
URL-redirect     : enable    Protocol : http
Jump-URL         : http://www.example.com/
Web-IP-address   : 192.168.1.1
FQDN             : aaa.example.com
Web-port         : http : 80, 8080      https : 443, 8443
ARP-relay Port   : 0/1-2
Force-Authorized : disable
Auth-max-user    : 1024

      Port         :   0/1
      VLAN ID      :   5,10,15
      Access-list-No:  100
      Max-user     :   64

      Port         :   0/2
      VLAN ID      :   15-16
      Access-list-No:  100
      Max-user     :   64
```

- When the authentication mode is in dynamic VLAN mode and the authentication method is local authentication:

```
# show web-authentication
Date 20XX/10/15 10:52:49 UTC
web-authentication Information:
  Authentic-mode   : Dynamic-VLAN
  Authentic-method : Local          Accounting-state : disable
  Dead-interval    : 10
      Max-timer : 60                 Max-user  : 256
      VLAN Count : -                 Auto-logout : disable
  Syslog-send      : enable
  URL-redirect     : enable    Protocol : http
  Jump-URL         : http://www.example.com/
  Web-IP-address   : 192.168.1.1
  FQDN             : aaa.example.com
  Web-port         : http : 80, 8080      https : 443, 8443
  ARP-relay Port   : 0/10,12
  Force-Authorized : enable
  Auth-max-user    : 1024

      Port         :   0/10
      VLAN ID      :   1000,1500
      Native VLAN  :   10
      Forceauth VLAN:  1000
      Access-list-No:  100
      Max-user     :   64

      Port         :   0/12
      VLAN ID      :   1000,1500
      Native VLAN  :   10
      Forceauth VLAN:  -
      Access-list-No:  100
      Max-user     :   64
```

- When the authentication mode is in dynamic VLAN mode and the authentication method is RADIUS authentication:

```
# show web-authentication
Date 20XX/10/15 10:52:49 UTC
web-authentication Information:
  Authentic-mode   : Dynamic-VLAN
  Authentic-method : RADIUS         Accounting-state : enable
  Dead-interval    : 10
      Max-timer : 60                 Max-user  : 256
      VLAN Count : -                 Auto-logout : disable
  Syslog-send      : enable
  URL-redirect     : enable    Protocol : http
  Jump-URL         : http://www.example.com/
  Web-IP-address   : 192.168.1.1
```

```
FQDN            : aaa.example.com
Web-port        : http : 80, 8080      https : 443, 8443
ARP-relay Port  : 0/10,12
Force-Authorized : enable
Auth-max-user   : 1024

    Port        :    0/10
    VLAN ID     :    1000,1500
    Native VLAN :    10
    Forceauth VLAN:  1000
    Access-list-No:  100
    Max-user    :    256

    Port        :    0/12
    VLAN ID     :    1000,1500
    Native VLAN :    10
    Forceauth VLAN:  -
    Access-list-No:  100
    Max-user    :    256
```

Display items

Table 32-14: Items displayed for the Web authentication configuration

Item	Meaning	Displayed detailed information
Authentic-mode	Authentication mode	Authentication mode for the Web authentication function Legacy: Indicates the legacy mode. Dynamic-VLAN: Indicates the dynamic VLAN mode Static-VLAN: Indicates the fixed VLAN mode
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
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	The total number of VLANs registered in legacy mode for Web authentication. Note that "-" is displayed in mode other than legacy mode.
Auto-logout	Whether forced logout by MAC address aging is available	Whether forced logout by MAC address aging in legacy mode and 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.

Item	Meaning	Displayed detailed information
Syslog-send	The usage state of the syslog server output function	The usage state of the function that outputs the Web authentication action log to the syslog server. enable: Used disable: Not used
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
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
ARP-relay port	ARP relay	The port number of the port that is used as a relay port if arp-relay is specified "-" 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
VLAN Information	VLAN information	Detailed information about a VLAN registered in Web authentication

Item	Meaning	Displayed detailed information
Port	Port information	The port number of the port embedded in a VLAN
VLAN ID	VLAN information	VLAN ID registered in Web authentication
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.
Access-list No.	Access lists	Access list number or 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

Response messages

Table 32-15: List of response messages for the show web-authentication command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

Notes

None

show web-authentication statistics

Shows statistics for Web authentication.

Syntax

```
show web-authentication statistics
```

Input mode

Administrator mode

Parameters

None

Operation when a stack configuration is used

This command is not supported.

Example

- Below is an example of executing the command when the authentication mode is in fixed mode or dynamic VLAN mode, 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/10/15 11:10:49 UTC
web-authentication Information:
  Authentication Request Total :        100
  Authentication Current Count :         10
  Authentication Error Total   :         30
  Force Authorized Count       :         10
Port Information:
  Port     User-count
   0/10       5/ 256
   0/12       5/1024
```

- When the authentication mode is in fixed VLAN mode or dynamic VLAN mode, and the authentication method is RADIUS authentication:
```
# show web-authentication statistics
Date 20XX/10/15 11:10:49 UTC
web-authentication Information:
  Authentication Request Total :        100
  Authentication Current Count :         10
  Authentication Error Total   :         30
  Force Authorized Count       :         10
RADIUS web-authentication Information:
[RADIUS frames]
        TxTotal    :        10  TxAccReq :        10  TxError   :         0
        RxTotal    :        30  RxAccAccpt:       10  RxAccRejct:        10
                                RxAccChllg:       10  RxInvalid :         0
Account web-authentication Information:
[Account frames]
        TxTotal    :        10  TxAccReq :        10  TxError   :         0
        RxTotal    :        20  RxAccResp :       10  RxInvalid :         0
Port Information:
  Port     User-count
   0/10       5/ 256
   0/12       5/1024
```

- When the authentication mode is in legacy mode and the authentication method is local authentication:
```
# show web-authentication statistics
```

```
Date 20XX/10/12 11:10:49 UTC
web-authentication Information:
  Authentication Request Total :          100
  Authentication Current Count :           10
  Authentication Error Total   :           30
```

- When the authentication mode is the legacy mode and the authentication method is RADIUS authentication:

```
# show web-authentication statistics
Date 20XX/10/12 11:10:49 UTC
web-authentication Information:
  Authentication Request Total :          100
  Authentication Current Count :           10
  Authentication Error Total   :           30
RADIUS web-authentication Information:
[RADIUS frames]
        TxTotal  :        10  TxAccReq :        10  TxError  :         0
        RxTotal  :        30  RxAccAccpt:       10  RxAccRejct:       10
                             RxAccChllg:       10  RxInvalid :        0
Account web-authentication Information:
[Account frames]
        TxTotal  :        10  TxAccReq :        10  TxError  :         0
        RxTotal  :        20  RxAccResp :       10  RxInvalid :        0
```

Display items

Table 32-16: 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 Note that this item is not displayed in legacy mode.
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

Item	Meaning
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 Note that this item is not displayed in legacy mode.
Port	Port 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

Response messages

Table 32-17: List of response messages for the show web-authentication statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

Notes

None

clear web-authentication logging

Clears log information for Web authentication.

Syntax

```
clear web-authentication logging
```

Input mode

Administrator mode

Parameters

None

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 32-18: List of response messages for the clear web-authentication logging command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

Notes

None

clear web-authentication statistics

Clears Web authentication statistics.

Syntax

```
clear web-authentication statistics
```

Input mode

Administrator mode

Parameters

None

Operation when a stack configuration is used

This command is not supported.

Example

The following command shows an example of clearing the Web authentication statistics:

```
# clear web-authentication statistics
```

Display items

None

Impact on communication

None

Response messages

Table 32-19: List of response messages for the clear web-authentication statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

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.

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 32-20: List of response messages for the commit web-authentication command

Message	Description
Can not commit.	An attempt to update the authentication information failed. Execute the "restart web-authentication" command to update the authentication information again.
Can't execute.	The command could not be executed. Re-execute the command.
Command information was damaged.	Information was discarded because the execution information is corrupted.

Message	Description
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.
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.
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

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.

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 32-21: List of response messages for the store web-authentication command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

Message	Description
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

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 in the flash memory.

The following shows an example of executing the "show flash" command:

```
> show flash
Date 20XX/04/01 19:46:29 JST
Flash :
        user area   config area    dump area    area total
   used  37,063kB         65kB         16kB      37,144kB
   free    616kB        7,199kB      8,152kB     15,967kB
   total 37,679kB       7,265kB      8,168kB     53,112kB
```

Note: The underlined part (the value for free indicating the free capacity of the user area) must be at least 20 KB.

If the free capacity in flash memory is insufficient, use the "rm" command to delete unnecessary files before creating the backup files.

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.

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 32-22: List of response messages for the load web-authentication command

Message	Description
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 execute.	The command could not be executed. Re-execute the command.
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.
File format error.	Registration is not possible because the file is not a backup file.
Load operation failed.	Restoration from the backup file failed.
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.
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

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 a user name with 1 to 16 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 ('), semi-colon (;), dollar sign ($), grave accent mark (`), backslash (\), sharp sign (#) at the beginning, and per-cent 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.

Operation when a stack configuration is used

This command is not supported.

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.

Response messages

Table 32-23: List of response messages for the clear web-authentication auth-state command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
The specified user is not login user.	The specified user is not a logged-in user.
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

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> [-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:

- Store the above in a directory other than /config/wa/htdocs.
- 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"

   Reply-Message page: "loginProcess.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.

-f

Replaces pages, messages, and icons without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Operation when a stack configuration is used

This command is not supported.

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  1263 Dec  6 09:59 loginProcess.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

# set web-authentication html-files k-html
Would you wish to install new html-files ? (y/n):y
executing…
Install complete.
```

Display items

None

Impact on communication

None

Response messages

Table 32-24: List of response messages for the set web-authentication html-files command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Can't put a sub directory in the directory.	The specified directory contains a subdirectory.
Can't specify "/config/wa/htdocs" in this command.	The "/config/wa/htdocs" directory cannot be specified.
Directory size over.	The capacity of the specified directory exceeds the limit (1024 KB).
Install operation failed.	An attempt to register the 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.
Too many files.	The number of files exceeds the limit of 100.

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 or legacy mode, if you associate the loginOK.html file with another file, the login success page might not be displayed correctly.

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 [-f]
```

Input mode

Administrator mode

Parameters

-f

Deletes the pages, messages, and icons without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Operation when a stack configuration is used

This command is not supported.

Example

The following command shows an example of deleting the registered html file:

```
# clear web-authentication html-files
Would you wish to clear registered html-files and initialize? (y/n):y
Clear complete.
```

Display items

None

Impact on communication

None

Response messages

Table 32-25: List of response messages for the clear web-authentication html-files command

Message	Description
Can't clear because it is default now.	The file could not be deleted because it had default status.
Can't execute.	The command could not be executed. Re-execute the command.
Clear operation failed.	An attempt to delete the file failed.

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.

Operation when a stack configuration is used

This command is not supported.

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:
```
# show web-authentication html-files
Date 20XX/04/15 10:07:04 UTC
TOTAL SIZE      :      62777
--------------------------------------------------
                    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
```
- 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      :      62777
---------------------------------------------------
                         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
```

Display items

None

Impact on communication

None

Response messages

Table 32-26: List of response messages for the show web-authentication html-files command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

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

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 32-27: List of response messages for the clear web-authentication dead-interval-timer command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

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

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 32-28: List of response messages for the set web-authentication ssl-crt command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Install operation failed.	A registration attempt failed.

Message	Description
No such file.	The specified file does not exist.

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

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 32-29: List of response messages for the clear web-authentication ssl-crt command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Clear operation failed.	A deletion attempt failed.

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

Operation when a stack configuration is used

This command is not supported.

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 32-30: 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

743

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

Response messages

Table 32-31: List of response messages for the show web-authentication ssl-crt command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

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 the Web authentication core file and the Web server core file at restart.
>
> 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.

Operation when a stack configuration is used

This command is not supported.

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).

Response messages

Table 32-32: List of response messages for the restart web-authentication command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
WA is not configured.	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.

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

Web server core file: httpd.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

Operation when a stack configuration is used

This command is not supported.

Example

The following command shows an example of collecting Web authentication dump information:

```
> dump protocols web-authentication
```

Display items

None

Impact on communication

None

Response messages

Table 32-33: List of response messages for the dump protocols web-authentication command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
WA is not configured.	The Web authentication function is not enabled. Check the configuration.

747

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.

33 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

Operation when a stack configuration is used

This command is not supported.

Example

The following command shows an example of displaying authenticated MAC addresses:

```
# show mac-authentication login
Date 20XX/10/15 10:52:49 UTC
Total client counts:2
F MAC address     Port   VLAN   Login time                 Limit time   Mode
* 0012.e200.0001  0/1    3      20XX/10/15 09:58:04 UTC    00:10:20     Static
* 0012.e200.0002  0/10   4094   20XX/10/15 10:10:23 UTC    00:20:35     Dynamic
```

Display items

The following table describes the items displayed for authenticated MAC addresses.

Table 33-1: 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	The port numbers of physical ports accommodating the authenticated, currently logged-in terminals
VLAN	VLAN	The VLANs set for the authenticated, currently logged-in terminals. The VLANs that were switched after authentication in dynamic VLAN mode.
Login time	Login date and time	The login times of the authenticated, currently logged-in terminals

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

Impact on communication

None

Response messages

Table 33-2: List of response messages for the show mac-authentication login command

Message	Description
Can't execute.	The command could not be executed.
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.
Mac-authentication is not configured.	The MAC-based authentication function is not configured. Check the configuration.

Notes

None

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.

Operation when a stack configuration is used

This command is not supported.

Example

The following examples show action log messages displayed for MAC-based authentication.

- When the parameter is omitted:

```
# show mac-authentication logging
Date 20XX/12/01 10:52:49 UTC
 No=1:Dec  1 10:09:50:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=0/1 VLAN=3 Login succeeded.
 No=2:Dec  1 10:10:10:NORMAL:LOGOUT: MAC=0012.e212.0001 PORT=0/1 VLAN=3 Logout succeeded.
 No=3:Dec  1 10:10:55:NORMAL:SYSTEM: accepted clear auth-state command.
```

- When "client" is specified for the parameter:

```
# show mac-authentication logging client
Date 20XX/12/01 11:13:15 UTC
 No=1:Dec  1 10:09:50:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=0/1 VLAN=3 Login succeeded.
 No=2:Dec  1 10:10:10:NORMAL:LOGOUT: MAC=0012.e212.0001 PORT=0/1 VLAN=3 Logout succeeded.
```

Display items

The following table describes the items displayed for MAC-based authentication action log messages.

Table 33-3: Items displayed for MAC-based authentication action log messages

Item	Meaning	Displayed detailed information
Level	Levels of action log messages	Severity of a log message
<log>	Action log message	Contents of a registered action log message

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 33-6: 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 33-4: Log ID and type of action log messages"
- Log type: "Table 33-4: Log ID and type of action log messages"
- Additional information: "Table 33-5: Additional information"
- List of messages: "Table 33-6: List of action log messages"

Table 33-4: 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.
ERROR	SYSTEM	Indicates a communication failure or a failure while the MAC-based authentication program is running.

Table 33-5: 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	Indicates the port number.

Table 33-6: List of action log messages

No.	Log ID	Log type	Message text	Meaning and action	Added info
1	NOR-MAL	LOGIN	Login succeeded.	[Meaning] The terminal was successfully authenticated. [Action] None	MAC address VLAN ID Port number

No.	Log ID	Log type	Message text	Meaning and action	Added info
2	NOR-MAL	LO-GOUT	Force logout ; Port link down.	[Meaning] 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
3	NOR-MAL	LO-GOUT	Force logout ; Authentic method changed (RADIUS <-> Local).	[Meaning] Authentication was canceled because of a switch between the RADIUS authentication and local authentication methods. [Action] None	MAC address VLAN ID Port number
4	NOR-MAL	LO-GOUT	Force logout ; Clear mac-authentication command succeeded.	[Meaning] Authentication was canceled by an operation command. [Action] None	MAC address VLAN ID Port number
5	NOR-MAL	LO-GOUT	Force logout ; Connection time was beyond a limit.	[Meaning] 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
6	NOTICE	LOGIN	Login failed ; Port link down.	[Meaning] 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
7	NOTICE	LOGIN	Login failed ; Port not specified.	[Meaning] 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

No.	Log ID	Log type	Message text	Meaning and action	Added info
8	NOTICE	LOGIN	Login failed ; VLAN not specified.	[Meaning] 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
9	NOR-MAL	LO-GOUT	Force logout ; Program stopped.	[Meaning] 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
10	NOR-MAL	LO-GOUT	Force logout ; Other authentication program.	[Meaning] 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
11	NOR-MAL	LO-GOUT	Force logout ; VLAN deleted.	[Meaning] 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
12	NOR-MAL	LO-GOUT	Force logout ; Client moved.	[Meaning] 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

No.	Log ID	Log type	Message text	Meaning and action	Added info
13	NOTICE	LOGIN	Login failed ; Double login. (L2MacManager)	[Meaning] The VLAN 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
14	NOTICE	LOGIN	Login failed ; Double login.	[Meaning] 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
15	NOTICE	LOGIN	Login failed ; Number of login was beyond limit.	[Meaning] 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.	[Meaning] 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

No.	Log ID	Log type	Message text	Meaning and action	Added info
18	NOTICE	LOGIN	Login failed ; MAC address could not register. [error-code]	[Meaning] 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	LO-GOUT	Logout failed ; MAC address could not delete. [error-code]	[Meaning] An attempt to delete a MAC address failed. [Action] Attempt authentication cancellation again.	MAC address[1] VLAN ID[1] Port number[1] error code
20	NOTICE	LOGIN	Login failed ; RADIUS authentication failed.	[Meaning] 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
21	NOTICE	LOGIN	Login failed ; Failed to connection to RADIUS server.	[Meaning] 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
22	NOTICE	LOGIN	Login failed ; Connection failed L2MacManager.	[Meaning] Authentication failed because an attempt to communicate with the VLAN program failed. [Action] Attempt authentication again. If this message appears frequently, execute the "restart vlan" command with the mac-manager parameter specified.	MAC address
28	NOR-MAL	LO-GOUT	Force logout ; Port not specified.	[Meaning] Authentication was canceled because the setting was deleted from the port. [Action] Check the configuration.	MAC address VLAN ID Port number

No.	Log ID	Log type	Message text	Meaning and action	Added info
29	NOTICE	LOGIN	Login failed ; Port number failed.	[Meaning] Authentication is impossible because port number acquisition failed. [Action] Attempt authentication again.	MAC address Port number
30	NOR-MAL	LO-GOUT	Force logout ; mac-address-table aging.	[Meaning] 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
31	NOR-MAL	LO-GOUT	Force logout ; Authentic mode had changed (dynamic vlan -> static vlan).	[Meaning] 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
32	NOR-MAL	LO-GOUT	Force logout ; Authentic mode had changed (static vlan -> dynamic vlan).	[Meaning] 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
33	NOR-MAL	LOGIN	Force login succeeded.	[Meaning] Forced authentication for the terminal was successful. [Action] None	MAC address VLAN ID Port number
34	NOR-MAL	LOGIN	Un-authorized Port Accepted.	[Meaning] Communication with an authentication exemption terminal was detected. [Action] None	MAC address VLAN ID Port number
35	NOR-MAL	LO-GOUT	Force logout ; Interface mode had changed.	[Meaning] 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

No.	Log ID	Log type	Message text	Meaning and action	Added info
36	NOTICE	LOGIN	Login failed ; Number of login was beyond limit of port.	[Meaning] 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
37	NOR-MAL	LO-GOUT	Force logout ; Number of login was beyond limit of port.	[Meaning] 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
82	NOR-MAL	SYSTEM	Accepted clear auth-state command.	[Meaning] A notification issued by the "clear mac-authentication auth-state" command for forced logout was received. [Action] None	—
83	NOR-MAL	SYSTEM	Accepted clear statistics command.	[Meaning] A request issued by the "clear mac-authentication statistics" command for deleting statistics was received. [Action] None	—
84	NOR-MAL	SYSTEM	Accepted commit command.	[Meaning] A notification issued by the "commit mac-authentication" command for re-configuring the authentication information was received. [Action] None	—
85	NOR-MAL	SYSTEM	Accepted dump command.	[Meaning] A dump output request issued by the "dump protocols mac-authentication" command was received. [Action] None	—

No.	Log ID	Log type	Message text	Meaning and action	Added info
86	NOR-MAL	LO-GOUT	Force logout ; MAC address not found L2MacManager.	[Meaning] An attempt to register a MAC address in the VLAN program was made because the MAC address exists on MAC-based authentication but not in the VLAN program. However, authentication was canceled because the registration attempt failed. [Action] Attempt authentication again.	MAC address VLAN ID Port number
88	ERROR	SYSTEM	Macauthd could not initialize.[error-code]	[Meaning] 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]	[Meaning] 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.	[Meaning] An attempt to communicate with the VLAN program was made, but failed. [Action] If this message appears frequently, execute the "restart vlan" command with the mac-manager parameter specified.	—
92	ERROR	SYSTEM	Disconnection failed ; L2MacManager.	[Meaning] Communication with the VLAN program was interrupted. [Action] If this message appears frequently, execute the "restart vlan" command with the mac-manager parameter specified.	—
93	ERROR	SYSTEM	Program failed ; Configuration command. [error-code]	[Meaning] An attempt to read the configuration failed.	Error code

No.	Log ID	Log type	Message text	Meaning and action	Added info
				[Action] Use the "restart mac-authentication" command to restart the MAC-based authentication program.	
94	ERROR	SYSTEM	Program failed ; Internal data update. [error-code]	[Meaning] 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]	[Meaning] 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.	[Meaning] 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.	[Meaning] 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	NOR-MAL	SYSTEM	Accepted clear logging command.	[Meaning] A request to delete the action log by the "clear mac-authentication logging" command was received. [Action] None	—

No.	Log ID	Log type	Message text	Meaning and action	Added info
103	NOR-MAL	SYSTEM	Synchronized ; Mac-authd -> L2Mac-Manager.	[Meaning] 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.	[Meaning] An authentication error occurred because the VLAN was in disable state. [Action] Enable the VLAN, and then attempt authentication again.	MAC address VLAN ID Port number
106	NOR-MAL	LO-GOUT	Force logout ; VLAN suspended.	[Meaning] 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
107	NOTICE	LOGIN	Login failed ; MAC address not found to MAC authentication DB.	[Meaning] 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.	[Meaning] 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	NOR-MAL	SYSTEM	Accepted clear dead-interval-timer command.	[Meaning] A request issued by the "clear mac-authentication dead-interval-timer" command for recovering the dead interval function was received. [Action] None	—

No.	Log ID	Log type	Message text	Meaning and action	Added info
255	ERROR	SYSTEM	The other error. [error-code]	[Meaning] An internal MAC-based authentication error occurred. Communication failed with an internal function indicated by the error code in [] after The other error. [Action] 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

Response messages

Table 33-7: List of response messages for the show mac-authentication logging command

Message	Description
Can't execute.	The command could not be executed.
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.
Mac-authentication is not configured.	The MAC-based authentication function is not configured. Check the configuration.

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

Operation when a stack configuration is used

This command is not supported.

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/10/15 10:52:49 UTC
mac-authentication Information:
    Authentic-method : RADIUS        Accounting-state  : disable
    Dead-interval    : 10
    Syslog-send      : enable
    Force-Authorized : disable
    Auth-max-user    : 1024

    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/10/15 10:52:49 UTC
mac-authentication Information:
    Authentic-method : RADIUS        Accounting-state  : disable
    Dead-interval    : 10
    Syslog-send      : enable
    Force-Authorized : enable
    Auth-max-user    : 1024

    Authentic-mode   : Static-VLAN
        Max-timer  : 60                 Max-terminal : 256
        Port Count : 2                  Auto-logout : enable
    VLAN-check       : enable
        Vid-key    : %VLAN

    Authentic-mode   : Dynamic-VLAN
        Max-timer  : 60                 Max-terminal : 256
        Port Count : 2                  Auto-logout : enable

    Port Information:
        Port              :    0/1
            Static-VLAN    :
```

```
        VLAN ID       :   5,10,15
        Auth type     :   force-authorized
     Dynamic-VLAN     :
        VLAN ID       :   1200,1500
        Native VLAN   :   10
        Forceauth VLAN:   1500
     Access-list-No   :   100
     Max-user         :   64

   Port               :   0/2
     Dynamic-VLAN     :
        VLAN ID       :   1300-1310
        Native VLAN   :   20
        Forceauth VLAN:   1300
     Access-list-No   :   100
     Max-user         :   64

   Port               :   0/10
     Static-VLAN      :
        VLAN ID       :   300,305
     Access-list-No   :   100
     Max-user         :   64
```

Display items

Table 33-8: 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 re-try interval	The interval time (in minutes) at which a RADIUS connection attempt is retried if a RADIUS connection fails
Syslog-send	The usage state of the sys-log server output function	The usage of the function for outputting the MAC-based au-thentication action log to the syslog server. enable: Used disable: Not used
Force-Authorized	Status of forced authenti-cation	Status of forced authentication. enable: Forced authentication is enabled. disable: Forced authentication is disabled.
Auth-max-user	Maximum number of au-thenticated users allowed on the device	Maximum number of authenticated users allowed on the de-vice
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 au-thenticated terminals	Maximum number of authentication terminals that can simul-taneously login to the MAC-based authentication function.
Port Count	Total number of ports	Total number of ports registered for MAC-based authentication

Item	Meaning	Displayed detailed information
Auto-logout	Auto-logout setting for when no accesses detected status continues	The status of the auto-logout function when continuing no-access status is detected for the relevant MAC address. enable: The auto-logout function when the no access state is detected is enabled. disable: The auto-logout function when the no access state is detected is disabled.
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	The number of the port registered for MAC-based authentication
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.
Access-list No.	Access lists	Access list number or 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

Response messages

Table 33-9: List of response messages for the show mac-authentication command

Message	Description
Can't execute.	The command could not be executed.

Message	Description
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.
Mac-authentication is not configured.	The MAC-based authentication function is not configured. Check the configuration.

Notes

None

show mac-authentication statistics

Displays MAC-based authentication statistics.

Syntax

```
show mac-authentication statistics
```

Input mode

Administrator mode

Parameters

None

Operation when a stack configuration is used

This command is not supported.

Example

The following command shows an example of displaying the MAC-based authentication statistics:

```
# show mac-authentication statistics
Date 20XX/10/15 11:10:49 UTC
mac-authentication Information:
  Authentication Request Total :        100
  Authentication Current Count :         10
  Authentication Error Total   :         30
  Force Authorized Count       :         10
Unauthorized Information:
  Unauthorized Client Count    :          5
RADIUS mac-authentication Information:
[RADIUS frames]
        TxTotal   :        10  TxAccReq  :        10  TxError   :         0
        RxTotal   :        30  RxAccAccpt:        10  RxAccRejct:        10
                                RxAccChllg:        10  RxInvalid :         0
Account mac-authentication Information:
[Account frames]
        TxTotal   :        10  TxAccReq  :        10  TxError   :         0
        RxTotal   :        20  RxAccResp :        10  RxInvalid :         0
Port Information:
  Port    User-count
  0/10       5/ 256
  0/12       5/1024
```

Display items

Table 33-10: 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

Item	Meaning
Unauthorized Client Count	Number of current authentication exemption terminals
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	Port 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

Response messages

Table 33-11: List of response messages for the show mac-authentication statistics command

Message	Description
Can't execute.	The command could not be executed.

Message	Description
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.
Mac-authentication is not configured.	The MAC-based authentication function is not configured. Check the configuration.

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.

Operation when a stack configuration is used

This command is not supported.

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.

Response messages

Table 33-12: List of response messages for the clear mac-authentication auth-state command

Message	Description
Can't execute.	The command could not be executed.
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.
Mac-authentication is not configured.	The MAC-based authentication function is not configured. Check the configuration.

Notes

None

clear mac-authentication logging

Clears log information for MAC-based authentication.

Syntax

```
clear mac-authentication logging
```

Input mode

Administrator mode

Parameters

None

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 33-13: List of response messages for the clear mac-authentication logging command

Message	Description
Can't execute.	The command could not be executed.
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.
Mac-authentication is not configured.	The MAC-based authentication function is not configured. Check the configuration.

Notes

None

clear mac-authentication statistics

Clears MAC-based authentication statistics.

Syntax

```
clear mac-authentication statistics
```

Input mode

Administrator mode

Parameters

None

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 33-14: List of response messages for the clear mac-authentication statistics command

Message	Description
Can't execute.	The command could not be executed.
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.
Mac-authentication is not configured.	The MAC-based authentication function is not configured. Check the configuration.

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.

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 33-15: List of response messages for the set mac-authentication mac-address command

Message	Description
Already mac address "<mac>","<vlan id>" exists.	The specified MAC address has already been registered.
Can't execute.	The command could not be executed. Re-execute the command.
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.
The number of client exceeds 1024.	The number of registered MAC addresses exceeds the capacity limit.

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.

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 33-16: List of response messages for the remove mac-authentication mac-address command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
Unknown mac-address '<mac>'.	The specified MAC address has not been registered.

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.

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 33-17: List of response messages for the commit mac-authentication command

Message	Description
Can not commit.	An attempt to update the authentication information failed. Execute the "restart mac-authentication" command to update the authentication information again.
Can't execute.	The command could not be executed. Re-execute the command.
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.
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.

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.

Operation when a stack configuration is used

This command is not supported.

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 33-18: 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

Item	Meaning	Displayed detailed information
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

Response messages

Table 33-19: List of response messages for the show mac-authentication mac-address command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

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.

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 33-20: List of response messages for the store mac-authentication command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Mac-authentication command is not configured.	The MAC-based authentication function is not configured. Check the configuration.

Message	Description
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.

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 in the flash memory.

The following shows an example of executing the "show flash" command:

```
> show flash
Date 20XX/12/01 19:46:29 JST
Flash :
        user area    config area     dump area     area total
   used  37,063kB          65kB          16kB       37,144kB
   free     616kB        7,199kB        8,152kB     15,967kB
   total  37,679kB        7,265kB        8,168kB     53,112kB
```

Note: The underlined part (the value for free indicating the free capacity of the user area) must be at least 100 KB.

If the free capacity in flash memory is insufficient, use the "rm" command to delete unnecessary files before creating the backup files.

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.

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 33-21: List of response messages for the load mac-authentication command

Message	Description
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.
Can't execute.	The command could not be executed. Re-execute the command.
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.
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 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.

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 restarted.

Behavior when this parameter is omitted:

A core file is not output.

Operation when a stack configuration is used

This command is not supported.

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.

Response messages

Table 33-22: List of response messages for the restart mac-authentication command

Message	Description
Can't execute.	The command could not be executed.
Mac-authentication is not configured.	The MAC-based authentication function is not configured. Check the configuration.

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

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 33-23: List of response messages for the dump protocols mac-authentication command

Message	Description
Can't execute.	The command could not be executed.
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.
Mac-authentication is not configured.	The MAC-based authentication function is not configured. Check the configuration.

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

Operation when a stack configuration is used

This command is not supported.

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

Response messages

Table 33-24: List of response messages for the clear mac-authentication dead-interval-timer command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
Mac-authentication is not configured.	The MAC-based authentication function is not configured. Check the configuration.

Notes

None

34 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". Note that you specify <interface number> without <switch no.>.

- 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.

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of displaying all DHCP snooping entries.

Figure 34-1: 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:      2/   3070

Bindings: 5
MAC Address     IP Address      Expire(min)  Type     VLAN  Port
0012.e287.0001  192.168.0.201   -            static*  1     0/1
0012.e287.0002  192.168.0.204   1439         dynamic  2     0/4
0012.e287.0003  192.168.0.203   -            static   3     0/3
0012.e287.0004  192.168.0.202   3666         dynamic  4     ChGr:2
0012.e2be.b0fb  192.168.100.11  59           dynamic* 12    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:      2/   3070

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 34-1: 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	—

Item	Meaning	Displayed detailed information
MAC Address	Terminal MAC address.	—
IP Address	Terminal IP address.	—
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 to which a terminal is connected	Displays the NIF number and port number if the applicable interface is an Ethernet interface. One of the following values are displayed for a port channel interface: ChGr:1 to ChGr:48

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

Response messages

Table 34-2: List of response messages for the show ip dhcp snooping binding command

Message	Description
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not running.
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Indicates the port number.
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: Location of the error

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". Note that you specify <interface number> without <switch no.>.

> - 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.

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of clearing all the dynamically registered entries.

Figure 34-2: 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.

Response messages

Table 34-3: List of response messages for the clear ip dhcp snooping binding command

Message	Description
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not running.
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Indicates the port number.
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: Location of the error

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

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of displaying statistics for DHCP snooping.

Figure 34-3: 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
0/1              170           170
0/3             1789            10
        :
0/25               0             0
ChGr:1          3646          2457
>
```

Display items

Table 34-4: 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 NIF number and port number if the applicable interface is an Ethernet interface. One of the following values are displayed for a port channel interface: ChGr:1 to ChGr:48
Recv	Number of DHCP packets received on untrusted ports for DHCP snooping	The number of packets discarded by Filter is included.

Item	Meaning	Displayed detailed information
Filter	Of the DHCP packets received (Recv) on the un-trusted port for DHCP snooping, the number of DHCP packets discarded as invalid packets	—

Legend: —: Not applicable

Impact on communication

None

Response messages

Table 34-5: List of response messages for the show ip dhcp snooping statistics command

Message	Description
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not run-ning.
Program error occurred: <error message>	A program error occurred. Re-execute the command. ered. <error message>: Location of the error

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

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of clearing the DHCP snooping statistics.

Figure 34-4: Result of executing the command to clear the DHCP snooping statistics

```
> clear ip dhcp snooping statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 34-6: List of response messages for the clear ip dhcp snooping statistics command

Message	Description
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not running.
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: Location of the error

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

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of displaying the statistics for dynamic ARP inspection.

Figure 34-5: 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 )
0/1                 0          15  (         15           0 )
0/2               584         883  (        883           0 )
0/3                 0           0  (          0           0 )
                                :
ChGr:2            170          53  (         53           0 )
>
```

Display items

Table 34-7: Items displayed for the dynamic ARP inspection statistics

Item	Meaning	Displayed detailed information
Port	Port number	Displays the NIF number and port number if the applicable interface is an Ethernet interface. One of the following values are displayed for a port channel interface: ChGr:1 to ChGr:48
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	—

Item	Meaning	Displayed detailed information
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

Response messages

Table 34-8: List of response messages for the show ip arp inspection statistics command

Message	Description
ARP Inspection doesn't seem to be running.	The command could not be executed because dynamic ARP inspection is not running.
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: Location of the error

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

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of clearing the statistics for dynamic ARP inspection.

Figure 34-6: 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

Response messages

Table 34-9: List of response messages for the clear ip arp inspection statistics command

Message	Description
ARP Inspection doesn't seem to be running.	The command could not be executed because dynamic ARP inspection is not running.
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: Location of the error

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.

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of displaying an action log message for DHCP snooping.

Figure 34-7: 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(0/2/1/0012.e2ff.fe01/192.168.100.254).
>
```

Display items

The following shows the display format of a message:

```
Apr 20 11:00:00 ID=2201 NOTICE DHCP server packets were received at an untrust
 (1)     (2)     (3)    (4)                     (5)
port(0/2/1/0012.e2ff.fe01/192.168.100.254).
```

(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 34-10: Levels and their description

Level	Type	Description
ERROR	Problem	Interruption of communication is detected or configurations of events were inconsistent.

Level	Type	Description
WARN	Warning	Malicious packets were detected or events that occurred when configurations were inconsistent.
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 shows the contents of action log messages.

Table 34-11: List of action log messages

Message ID	Level	Message text	Description
1109	INFO	The binding entry was deleted all.	[Meaning] All binding database entries were deleted. [Explanation of message variables] None. [Action] None
1110	INFO	The source guard entry was deleted all.	[Meaning] All terminal filter entries were deleted. [Explanation of message variables] None. [Action] None
1201	INFO	The binding entry was created(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	[Meaning] An entry was added to the binding database. [Explanation of message variables] <nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] None
1202	INFO	The binding entry timed out(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	[Meaning] An entry was deleted from the binding database because an aging time expired. [Explanation of message variables] <nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information.

Mes-sage ID	Level	Message text	Description
			\<nif no.>: Indicates the NIF number. \<port no.>: Indicates the port number. \<vlan id>: Indicates the VLAN ID. \<mac address>: Indicates the MAC address. \<ip address>: Indicates the IP address. [Action] None
1203	INFO	The binding entry was deleted by received DHCPRELEASE(\<nif no.>/\<port no.>/\<vlan id>/\<mac address>/\<ip address>).	[Meaning] An entry was deleted from the binding database because DHCPRELEASE was received. [Explanation of message variables] \<nif no.>/\<port no.>/\<vlan id>/\<mac address>/\<ip address>: Indicates DHCP client terminal information. 　\<nif no.>: Indicates the NIF number. 　\<port no.>: Indicates the port number. 　\<vlan id>: Indicates the VLAN ID. 　\<mac address>: Indicates the MAC address. 　\<ip address>: Indicates the IP address. [Action] None
1204	INFO	The binding entry was deleted by received DHCPDECLINE(\<nif no.>/\<port no.>/\<vlan id>/\<mac address>/\<ip address>).	[Meaning] An entry was deleted from the binding database because DHCPDECLINE was received. [Explanation of message variables] \<nif no.>/\<port no.>/\<vlan id>/\<mac address>/\<ip address>: Indicates DHCP client terminal information. 　\<nif no.>: Indicates the NIF number. 　\<port no.>: Indicates the port number. 　\<vlan id>: Indicates the VLAN ID. 　\<mac address>: Indicates the MAC address. 　\<ip address>: Indicates the IP address. [Action] None
1205	INFO	The binding entry was re-newed(\<nif no.>/\<port no.>/\<vlan id>/\<mac address>/\<ip address>).	[Meaning] A binding database entry was updated because lease renewal was detected. [Explanation of message variables] \<nif no.>/\<port no.>/\<vlan id>/\<mac address>/\<ip address>: Indicates DHCP client terminal information. 　\<nif no.>: Indicates the NIF number. 　\<port no.>: Indicates the port number. 　\<vlan id>: Indicates the VLAN ID. 　\<mac address>: Indicates the MAC address.

Mes-sage ID	Level	Message text	Description
			<ip address>: Indicates the IP address. [Action] None
1206	INFO	The binding entry was delet-ed(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip ad-dress>).	[Meaning] An entry was deleted from the binding database. [Explanation of message variables] <nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] None
1207	INFO	The source guard entry was add-ed(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip ad-dress>).	[Meaning] A terminal filter entry was added. [Explanation of message variables] <nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>: Indicates a DHCP client terminal filter setting. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] None
1208	INFO	The source guard entry was de-leted(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip ad-dress>).	[Meaning] A terminal filter entry was deleted. [Explanation of message variables] <nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>: Indicates a DHCP client terminal filter setting. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] None

Mes-sage ID	Level	Message text	Description
1301	INFO	The binding entry was created(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).	[Meaning] An entry was added to the binding database. [Explanation of message variables] ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] None
1302	INFO	The binding entry timed out(Ch-Gr:<channel group number>/<vlan id>/<mac address>/<ip address>).	[Meaning] An entry was deleted from the binding database because an aging time expired. [Explanation of message variables] ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] None
1303	INFO	The binding entry was deleted by received DHCPRELEASE(Ch-Gr:<channel group number>/<vlan id>/<mac address>/<ip address>).	[Meaning] An entry was deleted from the binding database because DHCPRELEASE was received. [Explanation of message variables] ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] None
1304	INFO	The binding entry was deleted by received DHCPDECLINE(Ch-Gr:<channel group number>/<vlan id>/<mac address>/<ip address>).	[Meaning] An entry was deleted from the binding database because DHCPDECLINE was received.

Mes-sage ID	Level	Message text	Description
			[Explanation of message variables] ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] None
1305	INFO	The binding entry was re-newed(ChGr:<channel group number>/<vlan id>/<mac ad-dress>/<ip address>).	[Meaning] A binding database entry was updated because lease renewal was detected. [Explanation of message variables] ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] None
1306	INFO	The binding entry was delet-ed(ChGr:<channel group num-ber>/<vlan id>/<mac address>/<ip address>).	[Meaning] An entry was deleted from the binding database. [Explanation of message variables] ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] None
2105	NOTICE	Discard of packets occurred by a reception rate limit of DHCP packets and ARP packets.	[Meaning] Packets were discarded due to the reception rate limit for DHCP packets and ARP packets. [Explanation of message variables] None. [Action] Revise the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.

Mes-sage ID	Level	Message text	Description
2201	NOTICE	DHCP server packets were received at an untrust port(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	[Meaning] An invalid DHCP server was detected. This message is output once every five minutes on a port-by-port basis. [Explanation of message variables] <nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>: Indicates DHCP server information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] Check the connected device.
2202	NOTICE	Lease release was received from the client who isn't in binding(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	[Meaning] Invalid lease release was detected. This message is output once every five minutes on a port-by-port basis. [Explanation of message variables] <nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] If this occurs frequently, it might have been caused by an attack. Check the connected devices.
2203	NOTICE	DHCP direct request was received from the client who isn't in binding(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	[Meaning] An invalid DHCP request was detected. This message is output once every five minutes on a port-by-port basis. [Explanation of message variables] <nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] If this occurs frequently, it might have been caused by an attack. Check the connected devices.

Mes-sage ID	Level	Message text	Description
2204	NOTICE	ARP packet was received from the client who isn't in bind-ing(<nif no.>/<port no.>/<vlan id>/<mac address>).	[Meaning] 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. [Explanation of message variables] <nif no.>/<port no.>/<vlan id>/<mac address>: Indicates ARP terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. [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 re-ceived at an untrust port(Ch-Gr:<channel group number>/<vlan id>/<mac address>/<ip address>).	[Meaning] An invalid DHCP server was detected. This message is output once every five minutes on a port-by-port basis. [Explanation of message variables] ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>: Indicates DHCP server information. <channel group number>: Indicates the chan-nel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] Check the connected device.
2302	NOTICE	Lease release was received from the client who isn't in bind-ing(ChGr:<channel group num-ber>/<vlan id>/<mac address>/<ip address>).	[Meaning] Invalid lease release was detected. This message is output once every five minutes on a port-by-port basis. [Explanation of message variables] ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the chan-nel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] If this occurs frequently, it might have been caused by an attack. Check the connected devic-es.

Mes-sage ID	Level	Message text	Description
2303	NOTICE	DHCP direct request was received from the client who isn't in binding (ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).	[Meaning] An invalid DHCP request was detected. This message is output once every five minutes on a port-by-port basis. [Explanation of message variables] ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [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>).	[Meaning] 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. [Explanation of message variables] ChGr:<channel group number>/<vlan id>/<mac address>: Indicates ARP terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. [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(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	[Meaning] An Option 82 packet was discarded. This message is output once every five minutes on a port-by-port basis. [Explanation of message variables] <nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.

Mes-sage ID	Level	Message text	Description
			[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(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	[Meaning] 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. [Explanation of message variables] <nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. 　<nif no.>: Indicates the NIF number. 　<port no.>: Indicates the port number. 　<vlan id>: Indicates the VLAN ID. 　<mac address>: Indicates the MAC address. 　<ip address>: Indicates the IP address. [Action] Revise the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.
3203	WARN	ARP packet was discarded for src-mac inspection(<nif no.>/<port no.>/<vlan id>/<mac address>).	[Meaning] 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. [Explanation of message variables] <nif no.>/<port no.>/<vlan id>/<mac address>: Indicates ARP terminal information. 　<nif no.>: Indicates the NIF number. 　<port no.>: Indicates the port number. 　<vlan id>: Indicates the VLAN ID. 　<mac address>: Indicates the MAC address. [Action] Check the connected devices because this might be caused by an attack.
3204	WARN	ARP packet was discarded for dst-mac inspection(<nif no.>/<port no.>/<vlan id>/<mac address>).	[Meaning] 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.

Mes-sage ID	Level	Message text	Description

			[Explanation of message variables]
			<nif no.>/<port no.>/<vlan id>/<mac address>: Indicates ARP terminal information.
			  <nif no.>: Indicates the NIF number.
			  <port no.>: Indicates the port number.
			  <vlan id>: Indicates the VLAN ID.
			  <mac address>: Indicates the MAC address.
			[Action]
			Check the connected devices because this might be caused by an attack.

3205	WARN	ARP packet was discarded for ip inspection(<nif no.>/<port no.>/<vlan id>/<mac address>).	[Meaning]
			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.
			[Explanation of message variables]
			<nif no.>/<port no.>/<vlan id>/<mac address>: Indicates ARP terminal information.
			  <nif no.>: Indicates the NIF number.
			  <port no.>: Indicates the port number.
			  <vlan id>: Indicates the VLAN ID.
			  <mac address>: Indicates the MAC address.
			[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>).	[Meaning]
			An Option 82 packet was discarded.
			This message is output once every five minutes on a port-by-port basis.
			[Explanation of message variables]
			ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information.
			  <channel group number>: Indicates the channel group number.
			  <vlan id>: Indicates the VLAN ID.
			  <mac address>: Indicates the MAC address.
			  <ip address>: Indicates the IP address.
			[Action]
			Revise the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.

3302	WARN	Discard of the DHCP packet which SMAC and chaddr isn't identica(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).	[Meaning] A DHCP packet whose source MAC address and client hardware address do not match was discarded.

Mes-sage ID	Level	Message text	Description
			This message is output once every five minutes on a port-by-port basis. [Explanation of message variables] ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [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>).	[Meaning] 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. [Explanation of message variables] ChGr:<channel group number>/<vlan id>/<mac address>: Indicates ARP terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. [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>).	[Meaning] 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. [Explanation of message variables] ChGr:<channel group number>/<vlan id>/<mac address>: Indicates ARP terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. [Action] Check the connected devices because this might be caused by an attack.

Mes- sage ID	Level	Message text	Description
3305	WARN	ARP packet was discarded for ip inspection(ChGr:<channel group number>/<vlan id>/<mac ad-dress>).	[Meaning] 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. [Explanation of message variables] ChGr:<channel group number>/<vlan id>/<mac address>: Indicates ARP terminal information. <channel group number>: Indicates the chan-nel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. [Action] Check the connected devices because this might be caused by an attack.
4201	ERROR	The number of the binding entry exceeded the capacity of this sys-tem(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip ad-dress>).	[Meaning] The number of entries in the binding database exceeds the capacity limit of the device. [Explanation of message variables] <nif no.>/<port no.>/<vlan id>/<mac address>/ <ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] Review the system configuration. If this mes-sage 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>).	[Meaning] The number of entries for the terminal filter ex-ceeds the capacity limit of the device. [Explanation of message variables] <nif no.>/<port no.>/<vlan id>/<mac address>/ <ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] Review the system configuration. If this mes-sage is displayed because a static entry or a channel group has been added, delete the rele-vant static entry or channel group, and then re-view the system configuration.

Mes-sage ID	Level	Message text	Description
4204	ERROR	The number of the source guard entry exceeded the capacity of this port(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	[Meaning] The number of entries for the terminal filter exceeds the capacity limit of a port. [Explanation of message variables] <nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. 　<nif no.>: Indicates the NIF number. 　<port no.>: Indicates the port number. 　<vlan id>: Indicates the VLAN ID. 　<mac address>: Indicates the MAC address. 　<ip address>: Indicates the IP address. [Action] Review the system configuration. If this message is displayed because a static entry or a channel group has been added, delete the relevant static entry or channel group, and then review the system configuration.
4301	ERROR	The number of the binding entry exceeded the capacity of this system(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).	[Meaning] The number of entries in the binding database exceeds the capacity limit of the device. [Explanation of message variables] ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>: Indicates DHCP client terminal information. 　<channel group number>: Indicates the channel group number. 　<vlan id>: Indicates the VLAN ID. 　<mac address>: Indicates the MAC address. 　<ip address>: Indicates the IP address. [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

Response messages

Table 34-12: List of response messages for the show ip dhcp snooping logging command

Message	Description
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not running.
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: Location of the error

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

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of clearing log messages for DHCP snooping.

Figure 34-8: 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

Response messages

Table 34-13: List of response messages for the clear ip dhcp snooping logging command

Message	Description
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not running.
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: Location of the error

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.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 34-9: 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

None

Response messages

Table 34-14: List of response messages for the restart dhcp snooping command

Message	Description
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.
Restarting dhcp_snoopingd, wait awhile.	The DHCP snooping program is being restarted. Wait a while.

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. In addition, do not use the "copy" command to copy the configuration. 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

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of outputting logs or internal information for DHCP snooping to a file.

Figure 34-10: Result of executing the DHCP snooping dump command

```
> dump protocols dhcp snooping
>
```

Display items

None

Impact on communication

None

Response messages

Table 34-15: List of response messages for the dump protocols dhcp snooping command

Message	Description
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not running.
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: Location of the error

Notes

Output file: /usr/var/dhsn/dhcp_snoopingd.dmp

35 **GSRP**

show gsrp

Shows GSRP information.

Syntax

```
show gsrp [<gsrp group id> { vlan-group <vlan group id list> | [port <port list>] [channel-grou
p-number <channel group list>] } ] [detail]
```

Input mode

User mode and administrator mode

Parameters

<gsrp group id> { vlan-group <vlan group id list> | [port <port list>] [channel-group-number <channel group list>] }

    <gsrp group id>

        Displays GSRP information for the specified GSRP group ID.

        The specifiable values are from 1 to 65535.

    vlan-group <vlan group id list>

        Displays GSRP information for the specified VLAN group ID.

        The specifiable values are from 1 to 64.

    [port <port list>] [channel-group-number <channel group list>]

        Displays GSRP information about the specified port or the specified channel group. The port and the channel group can be specified at the same time. In that case, GSRP information for the specified port and the specified channel group is displayed.

    port <port list>

        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.>. Ports configured as direct link ports, and ports belonging to VLANs that are part of VLAN groups can be specified.

    channel-group-number <channel group list>

        For details about how to specify <channel group list>, see "Specifiable values for parameters". IDs for channel groups configured as direct links and for channel groups belonging to VLANs that are part of VLAN groups can be specified.

    Behavior when this parameter is omitted:

        All GSRP information is displayed.

detail

    Displays detailed information about GSRP.

    The display contents are the same when a VLAN group is specified.

    Behavior when this parameter is omitted:

        Summary information about GSRP is displayed.

Behavior when all parameters are omitted:

    All GSRP summary information is displayed.

Operation when a stack configuration is used

This command is not supported.

Example 1

Figure 35-1: Example of displaying the GSRP summary information

```
> show gsrp
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 3
 Local MAC Address      : 0012.e2a8.2527
 Neighbor MAC Address   : 0012.e2a8.2505
 Total VLAN Group Counts : 3
 Layer 3 Redundancy     : On
 Virtual MAC Learning   : Interval 120  (Output Rate 30pps)
 VLAN Port Counts       : Configuration   15,  Capacity 3600

 VLAN Group ID     Local State       Neighbor State
 1                 Backup            Master
 2                 (disable)         -
 8                 Master            -

>
```

Display items in Example 1

Table 35-1: Items displayed for the GSRP summary information

Item	Meaning	Displayed detailed information
GSRP ID	GSRP group ID	1 to 65535
Local MAC Address	MAC address of this device	—
Neighbor MAC Address	MAC address of the partner device	"-" is displayed if the partner device is unknown.
Total VLAN Group Counts	Total number of VLAN groups in this device	0 to 64
Layer 3 Redundancy	Layer 3 redundancy switching	Off: Not set. On: Layer 3 redundancy switching is enabled.
Virtual MAC Learning	Number of frames for virtual MAC address learning	—
Interval	Sending interval	4 to 120 (seconds)
(Output Rate)	Sending rate (packet/s)	Displays the current sending rate for frames for virtual MAC address learning. This item is not displayed when Layer 3 redundancy switching is not used in the configuration.
VLAN Port Counts	Number of sending ports for frames for virtual MAC address learning	This item is not displayed when Layer 3 redundancy switching is not used in the configuration.

Item	Meaning	Displayed detailed information
Configuration	Number of target ports where frames for virtual MAC address learning are sent to	Displays the number of VLAN ports# where the frames for virtual MAC address learning are sent to. If this value is greater than the number of ports enabled for sending frames for virtual MAC address learning, it means that the differentials of frames for virtual MAC address learning were not sent.
Capacity	Number of ports enabled for sending frames for virtual MAC address learning	Displays the number of VLAN ports where frames can be sent at the sending rate for frames for virtual MAC address learning.
VLAN Group ID	VLAN group ID	1 to 64

Local State	Status of VLAN groups on this device	Master:
		  Indicates that the VLAN group is the master group.
		Backup:
		  Indicates that the VLAN group is the backup group.
		Backup(Lock):
		  Indicates that the VLAN group is the backup (fixed) group.
		Backup(Waiting):
		  Indicates that the VLAN group is the backup (master wait) group.
		Backup(No Neighbor):
		  Indicates that the VLAN group is the backup (neighbor unknown) group.
		(disable)
		  Indicates that the VLAN group is disabled.

Neighbor State	Status of VLAN groups on the partner device	Master:
		  Indicates that the VLAN group is the master group.
		Backup:
		  Indicates that the VLAN group is the backup group.
		Backup(Lock):
		  Indicates that the VLAN group is the backup (fixed) group.
		Backup(Waiting):
		  Indicates that the VLAN group is the backup (master wait) group.
		Backup(No Neighbor):
		  Indicates that the VLAN group is the backup (neighbor unknown) group.
		("-" is displayed if the partner device is unknown.)

Total number of member ports among VLAN ports that belong to the master VLAN group. Each channel group is counted as one port.

Example 2

Figure 35-2: Example of displaying the GSRP information when a VLAN group ID is specified

```
> show gsrp 3 vlan-group 1,2,8
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 3
```

```
Local MAC Address      : 0012.e2a8.2527
Neighbor MAC Address   : 0012.e2a8.2505
Total VLAN Group Counts : 3
Layer 3 Redundancy     : On
Virtual MAC Learning   : Interval 120  (Output Rate 30pps)
VLAN Port Counts       : Configuration   15,  Capacity 3600

VLAN Group ID : 1
 VLAN ID               : 110,200-2169
 Member Port           : 0/6-8
 Active Port           : 0/6-8
 Last Transition       : 20XX/07/14 10:00:00  (Master to Backup)
 Transition by reason  : Priority was lower than neighbor's
 Master to Backup Counts : 4
 Backup to Master Counts : 4
 Virtual MAC Address   : 0000.8758.1387

                          Local             Neighbor
 State                 : Backup            Master
 Acknowledged State    : Backup            -
 Advertise Hold Timer  : 3                 -
 Priority              : 100               101
 Active Ports          : 3                 3
 Up Ports              : 3                 -

VLAN Group ID : 2
 VLAN ID               : 120
 Member Port           : -
 Active Port           : -
 Last Transition       : -          ( - )
 Transition by reason  : -
 Master to Backup Counts : -
 Backup to Master Counts : -
 Virtual MAC Address   : 0000.8758.138f

                          Local             Neighbor
 State                 : (disable)         -
 Acknowledged State    : -                 -
 Advertise Hold Timer  : -                 -
 Priority              : 100               -
 Active Ports          : -                 -
 Up Ports              : -                 -

VLAN Group ID : 8
 VLAN ID               : 180
 Member Port           : 0/6-8
 Active Port           : 0/6-8
 Last Transition       : 20XX/07/14 11:00:00  (Backup to Master)
 Transition by reason  : "set gsrp master"command was executed
 Master to Backup Counts : 0
 Backup to Master Counts : 1
 Virtual MAC Address   : 0000.8758.13bf

                          Local             Neighbor
 State                 : Master            -
 Acknowledged State    : -                 -
 Advertise Hold Timer  : 0                 -
 Priority              : 100               -
 Active Ports          : 3                 -
 Up Ports              : 3                 -

 >
```

Display items in Example 2

Table 35-2: Items displayed for the GSRP information when a VLAN group ID is specified

Item	Meaning	Displayed detailed information
GSRP ID	GSRP group ID	1 to 65535
Local MAC Address	MAC address of this device	—
Neighbor MAC Address	MAC address of the partner device	"-" is displayed if the partner device is unknown.
Total VLAN Group Counts	Total number of VLAN groups in this device	0 to 64
Layer 3 Redundancy	Layer 3 redundancy switching	Off: Not set. On: Layer 3 redundancy switching is enabled.
Virtual MAC Learning	Number of frames for virtual MAC address learning	—
Interval	Sending interval	4 to 120 (seconds)
(Output Rate)	Sending rate (packet/s)	Displays the current sending rate for frames for virtual MAC address learning. This item is not displayed when Layer 3 redundancy switching is not used in the configuration.
VLAN Port Counts	Number of sending ports for frames for virtual MAC address learning	This item is not displayed when Layer 3 redundancy switching is not used in the configuration.
Configuration	Number of target ports where frames for virtual MAC address learning are sent to	Displays the number of VLAN ports[#] where the frames for virtual MAC address learning are sent to. If this value is greater than the number of ports enabled for sending frames for virtual MAC address learning, it means that the differentials of frames for virtual MAC address learning were not sent.
Capacity	Number of ports enabled for sending frames for virtual MAC address learning	Displays the number of VLAN ports where frames can be sent at the sending rate for frames for virtual MAC address learning.
VLAN Group ID	VLAN group ID	1 to 64
VLAN ID	VLAN ID	1 to 4094 When used in combination with Ring Protocol, VLANs that do not belong to the VLAN group are not included.
Member Port	Ports belonging to a VLAN which is configured for a VLAN group	"-" is displayed if no active ports belong to a VLAN group, or if the VLAN group is in disable state. A channel group is expanded to a list of aggregated ports and then displayed.
Active Port	Active port	"-" is displayed if no active ports belong to a VLAN group, or if the VLAN group is in disable state. A channel group is expanded to a list of aggregated ports and then displayed. Note, however, that a ring port is not counted as an active port.

Item	Meaning	Displayed detailed information
Last Transition	Last status transition time	yyyy/mm/dd hh:mm:ss, meaning year/month/day hour:minute:second. The status transition is shown within parentheses. "-" is displayed if no status transitions have been performed, or if the VLAN group is in disable state.
Transition by reason	Reason for the status transition	Active ports were more than neighbor's: 　The number of active ports on this device is greater than the number of active ports on the partner device. Priority was higher than neighbor's.: 　The priority of this device is higher than that of the partner device. MAC address was larger than neighbor's: 　The MAC address of this device is greater than that of the partner device. "set gsrp master" command was executed: 　The "set gsrp master" command was executed. Direct link failure was detected: 　A direct link failure was detected. Forced shift time was expired: 　The automatic master transition wait time elapsed. Active ports was less than neighbor's: 　The number of active ports in this device is smaller than the number of active ports in the partner device. Priority was lower than neighbor's: 　The priority of this device is lower than that of the partner device. MAC address was smaller than neighbor's: 　The MAC address of this device is smaller than that of the partner device. BackupLock was enabled: 　backup-lock was set. Double Master was detected: 　It was detected that the device and the partner device were in master status. "-" is displayed if no status transitions have been performed, or the port is disabled. Also, when the GSRP device does not recognize the partner device in master status, if the "restart vlan" command is executed, "-" is displayed.
Master to Backup Counts	Number of transitions from the master status to the backup status (statistics)	0 to 4294967295 "-" is displayed if the VLAN group is disabled.
Backup to Master Counts	Number of transitions from the backup status to the master status (statistics)	0 to 4294967295 "-" is displayed if the VLAN group is disabled.
Virtual MAC Address	Virtual MAC address	"-" is displayed when Layer 3 redundancy switching is not set.
Local	Information about this device	—
Neighbor	Information about the partner device	"-" is displayed if the partner device is unknown.

Item	Meaning	Displayed detailed information
State	VLAN group status	Master: 　Indicates that the VLAN group is the master group. Backup: 　Indicates that the VLAN group is the backup group. Backup(Lock): 　Indicates that the VLAN group is the backup (fixed) group. Backup(Waiting): 　Indicates that the VLAN group is the backup (master wait) group. Backup(No Neighbor): 　Indicates that the VLAN group is the backup (neighbor unknown) group. (disable): 　Indicates that the VLAN group is disabled.
Acknowledged State	Status of a VLAN group on this device which is recognized by the partner device	Master: 　Indicates that the VLAN group is the master group. Backup: 　Indicates that the VLAN group is the backup group. Backup(Lock): 　Indicates that the VLAN group is the backup (fixed) group. Backup(Waiting): 　Indicates that the VLAN group is the backup (master wait) group. Backup(No Neighbor): 　Indicates that the VLAN group is the backup (neighbor unknown) group. "-" is displayed if the partner device is unknown or disabled. ("-" is displayed for information about the partner device.)
Advertise Hold Timer	Length of time that an Advertise frame continues to be active	0 to 120 (seconds) "-" is displayed if the VLAN group is disabled. ("-" is displayed for information about the partner device.)
Priority	Priority information	0 to 255 (The greater the value, the higher the priority.)
Active Ports	Number of active ports	0 to the maximum number of ports per device. Each channel group is counted as one port. "-" is displayed if the VLAN group is disabled. Note, however, that a ring port is not counted as an active port.
Up Ports	Number of enabled ports belonging to a VLAN that is configured to be in a VLAN group	0 to the maximum number of ports per device. Each channel group is counted as one port. "-" is displayed if the VLAN group is disabled. ("-" is displayed for information about the partner device.)

\# Total number of member ports among VLAN ports that belong to the master VLAN group. Each channel group is counted as one port.

Example 3

Figure 35-3: Example of displaying the detailed GSRP information

```
> show gsrp detail
Date 20XX/11/07 12:00:00 UTC

GSRP ID: 3
 Local MAC Address      : 0012.e2a8.2527
 Neighbor MAC Address   : 0012.e2a8.2505
 Total VLAN Group Counts : 3
 GSRP VLAN ID           : 105
 Direct Port            : 0/10-11
 Limit Control          : Off
 GSRP Exception Port    : 0/1-5
 No Neighbor To Master  : manual
 Backup Lock            : disable
 Port Up Delay          : 0
 Last Flush Receive Time : -
 Forced Shift Time      : -
 Layer 3 Redundancy     : On
 Virtual MAC Learning   : Interval 120  (Output Rate 30pps)
 VLAN Port Counts       : Configuration   15,  Capacity 3600
 Virtual Link ID        : 100(VLAN ID : 20)

                          Local             Neighbor
 Advertise Hold Time    : 5                 5
 Advertise Hold Timer   : 4                 -
 Advertise Interval     : 1                 1
 Selection Pattern      : ports-priority-mac  ports-priority-mac

 VLAN Group ID    Local State       Neighbor State
 1                Backup            Master
 2                (disable)         -
 8                Master            -
>
```

Display items in Example 3

Table 35-3: Items displayed for the detailed GSRP information

Item	Meaning	Displayed detailed information
GSRP ID	GSRP group ID	1 to 65535
Local MAC Address	MAC address of this device	—
Neighbor MAC Address	MAC address of the partner device	"-" is displayed if the partner device is unknown.
Total VLAN Group Counts	Total number of VLAN groups in this device	0 to 64
GSRP VLAN ID	VLAN ID used for transmitting Advertise frames	1 to 4094
Direct Port	Port used for transmitting Advertise frames	"-" is displayed if the port is not configured.
Limit Control	GSRP VLAN group-only control	Off: Not set. On: The function restricting GSRP control to VLANs that are in VLAN groups is being applied.

Item	Meaning	Displayed detailed information
GSRP Exception Port	Port which is not subject to GSRP control	"-" is displayed if the port is not configured. When used with Ring Protocol, if a ring port is configured, it is displayed as Exception Port.

No Neighbor To Master	Operation setting in backup (neighbor unknown) status	manual:
		  Until a GSRP Advertise frame is received or a master transition command is executed, the backup (neighbor unknown) status continues.
		direct-down:
		  If a direct link goes down, it automatically transitions to master status.

Backup Lock	backup-lock configuration setting	enable:
		  backup-lock configuration is set.
		disable:
		  backup-lock configuration is not set.

Port Up Delay	Delay time until an active port becomes subject to be counted when the line is enabled	0 to 43200 (seconds) or infinity (infinity means unlimited.)
Last Flush Receive Time	Time when the last GSRP Flush request frame was received	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second "-" is displayed if no GSRP Flush request frames were received.
Forced Shift Time	Automatic master transition wait time delay	-: Not set. 0 to 3600 (seconds) During the transition wait time, the time until the transition will occur is displayed in the following form: Now Waiting, 20Sec, left
Layer 3 Redundancy	Layer 3 redundancy switching	Off: Not set. On: Layer 3 redundancy switching is enabled.
Virtual MAC Learning	Number of frames for virtual MAC address learning	—
Interval	Sending interval	4 to 120 (seconds)
(Output Rate)	Sending rate (packet/s)	Displays the current sending rate for frames for virtual MAC address learning. This item is not displayed when Layer 3 redundancy switching is not used in the configuration.
VLAN Port Counts	Number of sending ports for frames for virtual MAC address learning	This item is not displayed when Layer 3 redundancy switching is not used in the configuration.
Configuration	Number of target ports where frames for virtual MAC address learning are sent to	Displays the number of VLAN ports[#] where the frames for virtual MAC address learning are sent to. If this value is greater than the number of ports enabled for sending frames for virtual MAC address learning, it means that the differentials of frames for virtual MAC address learning were not sent.
Capacity	Number of ports enabled for sending frames for virtual MAC address learning	Displays the number of VLAN ports where frames can be sent at the sending rate for frames for virtual MAC address learning.

Item	Meaning	Displayed detailed information
Virtual Link ID	Virtual link ID	1 to 250 "-" is displayed if no virtual link IDs are set. Information enclosed in parentheses indicates the virtual link VLAN ID.
Local	Information about this device	—
Neighbor	Information about the partner device	"-" is displayed if the partner device is unknown.
Advertise Hold Time	Retention time of an Advertise frame	1 to 120 (seconds) (The value set by using the "advertise-holdtime" configuration command is displayed.)
Advertise Hold Timer	Length of time that an Advertise frame continues to be active	0 to 120 (seconds) ("-" is displayed for information about the partner device.)
Advertise Interval	Sending interval between Advertise frames	0.5 to 60 (seconds)
Selection Pattern	Method for selecting the master or backup status	ports-priority-mac: 　The master is selected and determined in the order of the number of active ports, the priority, and the device MAC address. priority-ports-mac: 　The master is selected and determined in the order of the priority, the number of active ports, and the device MAC address.
VLAN Group ID	VLAN group ID	1 to 64
Local State	Status of VLAN groups on this device	Master: 　Indicates that the VLAN group is the master group. Backup: 　Indicates that the VLAN group is the backup group. Backup(Lock): 　Indicates that the VLAN group is the backup (fixed) group. Backup(Waiting): 　Indicates that the VLAN group is the backup (master wait) group. Backup(No Neighbor): 　Indicates that the VLAN group is the backup (neighbor unknown) group. (disable): 　Indicates that the VLAN group is disabled.

Item	Meaning	Displayed detailed information
Neighbor State	Status of VLAN groups on the partner device	Master: Indicates that the VLAN group is the master group. Backup: Indicates that the VLAN group is the backup group. Backup(Lock): Indicates that the VLAN group is the backup (fixed) group. Backup(Waiting): Indicates that the VLAN group is the backup (master wait) group. Backup(No Neighbor): Indicates that the VLAN group is the backup (neighbor unknown) group. ("-" is displayed if the partner device is unknown.)

\# Total number of member ports among VLAN ports that belong to the master VLAN group. Each channel group is counted as one port.

Example 4

Figure 35-4: Example of displaying the GSRP information when a port is specified

```
> show gsrp 10 port 0/6-11
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
 Port Information
 0/6    GSRP    : Active    Port   : Up
        Type    : Member    Flush  : Reset    Delay         : 0
        TxFrame : 0         RxFrame : 0       Discard Frame : 0
 0/7    GSRP    : Active    Port   : Up
        Type    : Member    Flush  : Reset    Delay         : 0
        TxFrame : 0         RxFrame : 0       Discard Frame : 0
 0/8    GSRP    : Active    Port   : Up
        Type    : Member    Flush  : GSRP     Delay         : 0
        TxFrame : 0         RxFrame : 0       Discard Frame : 0
 0/10   GSRP    : Not Active Port  : Up
(CH:  1) Type   : Direct    Flush  : No       Delay         : 0
        TxFrame : 960       RxFrame : 954     Discard Frame : 0
 0/11   GSRP    : Not Active Port  : Up
(CH:  1) Type   : Direct    Flush  : No       Delay         : 0
        TxFrame : 960       RxFrame : 954     Discard Frame : 0


>
```

Display items in Example 4

Table 35-4: Items displayed for the GSRP information when a port is specified

Item	Meaning	Displayed detailed information
GSRP ID	GSRP group ID	1 to 65535
Port Information	Port information	—
\<nif no.>/\<port no.>	Port number	—
CH	Channel group number	—

Item	Meaning	Displayed detailed information
GSRP	Status of a port belonging to a VLAN configured for a VLAN group, or of a port belonging to a GSRP-managed VLAN	Active: Indicates that the port status is active Not Active: Indicates that the port status is not active.
Port	Port status	Up: Indicates that the port is up. Down: Indicates that the port is down.
Type	Port type	Direct: Indicates that the port is a direct link port. Member: Indicates that the port belongs to a VLAN configured for a VLAN group.
Flush	Method of clearing mac_address_table for adjacent switches	GSRP: The GSRP Flush request frame is sent. Reset: Port resetting is used. No: The GSRP Flush request frame is not sent.
Delay	Delay time until an active port becomes subject to be counted when the line is enabled	Indicates the remaining time until a port belonging to a VLAN set for a VLAN group becomes an active port. 0 to 43200 (seconds) or infinity
TxFrame	Number of sent GSRP Advertise frames (statistics)	0 to 4294967295 The same value is displayed for all ports in the same channel group.
RxFrame	Number of received GSRP Advertise frames (statistics)	0 to 4294967295 The same value is displayed for all ports in the same channel group.
Discard Frame	Number of GSRP Advertise frames discarded when they are received (statistics)	0 to 262140 (The maximum value is 65535, the maximum number by reason why the frame is discarded, times 4, the number of components.) The same value is displayed for all ports in the same channel group.

Example 5

Figure 35-5: Displaying the detailed GSRP information when a port is specified

```
> show gsrp 10 port 0/6 detail
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
 Port Information
 0/6    GSRP   : Active     Port   : Up
        Type   : Member     Flush  : Reset      Delay        : 0
        TxFrame : 0         RxFrame : 0         Discard Frame : 0
        Discard Frame by reason
           mismatch GSRP VLAN ID    : 0
           mismatch GSRP ID         : 0
           loopback GSRP frame      : 0
           illegal GSRP frame       : 0

>
```

Display items in Example 5

Table 35-5: Items displayed for the detailed GSRP information when a port is specified

Item	Meaning	Displayed detailed information
GSRP ID	GSRP group ID	1 to 65535
Port Information	Port information	—
<nif no.>/<port no.>	Port number	—
CH	Channel group number	—
GSRP	Status of a port belonging to a VLAN which is configured for a VLAN group	Active: Indicates that the port status is active Not Active: Indicates that the port status is not active.
Port	Port status	Up: Indicates that the port is up. Down: Indicates that the port is down.
Type	Port type	Direct: Indicates that the port is a direct link port. Member: Indicates that the port belongs to a VLAN configured for a VLAN group.
Flush	Method of clearing mac_address_table for adjacent switches	GSRP: The GSRP Flush request frame is sent. Reset: Port resetting is used. No: The GSRP Flush request frame is not sent.
Delay	Delay time until an active port becomes subject to be counted when the line is enabled	Indicates the remaining time until a port belonging to a VLAN set for a VLAN group becomes an active port. 0 to 43200 (seconds) or infinity
TxFrame	Number of sent GSRP Advertise frames (statistics)	0 to 4294967295 The same value is displayed for all ports in the same channel group.
RxFrame	Number of received GSRP Advertise frames (statistics)	0 to 4294967295 The same value is displayed for all ports in the same channel group.
Discard Frame	Number of GSRP Advertise frames discarded when they are received (statistics)	0 to 262140 (The maximum value is 65535, the maximum number by reason why the frame is discarded, times 4, the number of components.) The same value is displayed for all ports in the same channel group.
Discard Frame by reason	Detailed statistics for discarded frames by reason	—

Item	Meaning	Displayed detailed information
mismatch GSRP VLAN ID	Number of GSRP Advertise frames discarded due to GSRP-managed VLAN ID mismatch (statistics)	0 to 65535
mismatch GSRP ID	Number of GSRP Advertise frames discarded due to GSRP ID mismatch (statistics)	0 to 65535 Note: Counted only if frames are transmitted via a direct link.
loopback GSRP frame	Number of GSRP Advertise frames discarded because a GSRP Advertise frame sent from this device was received (statistics)	0 to 65535
illegal GSRP frame	Number of GSRP Advertise frames discarded because an invalid GSRP Advertise frame was received. (statistics)	0 to 65535

Impact on communication

None

Response messages

Table 35-6: List of response messages for the show gsrp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
GSRP is not configured.	GSRP has not been configured. Check the configuration.
Specified GSRP ID is not configured:<gsrp group id>.	The specified GSRP group ID has not been configured. <gsrp group id>: Indicates the GSRP group ID.
Specified port is not operational.	The specified port and channel group are not active.
Specified VLAN group ID is not configured:<vlan group id>.	The specified VLAN group ID has not been configured. <vlan group id>: Indicates the VLAN group ID.

Notes

The counter will no longer be updated when statistics reach the maximum value.

show gsrp aware

Shows GSRP aware information.

Syntax

```
show gsrp aware
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

The command can display information only for the master switch.

Example

Figure 35-6: 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 35-7: Items displayed for the GSRP aware information

Item	Meaning	Displayed detailed information
Last mac_ad-dress_table Flush Time	Time mac_address_table Flush was last performed	yyyy/mm/dd hh:mm:ss year/month/day hour:min-ute:second
GSRP Flush Re-quest Parameters	Information about the GSRP Flush re-quest frame when 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 Ad-dress	MAC address from which the received GSRP Flush request frame was sent	—

Impact on communication

None

Response messages

Table 35-8: List of response messages for the show gsrp aware command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
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.
No received flush request frame.	No GSRP Flush request frames were received.

Notes

Receiving a GSRP Flush request frame clears all mac_address_table for every VLAN group ID.

clear gsrp

Clears the GSRP statistics.

Syntax

```
clear gsrp [<gsrp group id> { vlan-group <vlan group id list> | [port <port list>] [channel-gro
up-number <channel group list>] } ]
```

Input mode

User mode and administrator mode

Parameters

<gsrp group id> { vlan-group <vlan group id list> | [port <port list>] [channel-group-number <channel group list>] }

> <gsrp group id>
>
>> Clears all statistics for GSRP relating to the specified GSRP group ID.
>>
>> Specifiable values for GSRP group IDs are from 1 to 65535.
>
> vlan-group <vlan group id list>
>
>> Clears statistics for GSRP relating to the specified VLAN group ID.
>>
>> The specifiable values are from 1 to 64.
>>
>> The items to be cleared are Master to Backup Counts and Backup to Master Counts.
>
> [port <port list>] [channel-group-number <channel group list>]
>
>> Clears statistics for GSRP relating to the specified port or channel group. Both port and channel groups can be specified at the same time. In this case, GSRP statistics for the specified port and statistics for the specified channel group are cleared.
>>
>> Behavior when this parameter is omitted:
>>
>>> Statistics for GSRP relating to all ports and channel groups are cleared.
>
> port <port list>
>
>> Clears statistics for GSRP relating to the specified port.
>>
>> The items to be cleared are TxFrame, RxFrame, Discard Frame, mismatch GSRP VLAN ID, mismatch GSRP ID, loopback GSRP frame, and illegal GSRP frame.
>>
>> 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 statistics for GSRP relating to the specified channel group.
>>
>> The items to be cleared are TxFrame, RxFrame, Discard Frame, mismatch GSRP VLAN ID, mismatch GSRP ID, loopback GSRP frame, and illegal GSRP frame.
>>
>> For details about how to specify <channel group list>, see "Specifiable values for parameters".
>
> Behavior when this parameter is omitted:
>
>> All GSRP statistics are cleared.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 35-7: Example of clearing all the GSRP statistics

```
> clear gsrp
>
```

Figure 35-8: Example of clearing the GSRP statistics when a VLAN group ID is specified

```
> show gsrp 10 vlan-group 1
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
 Local MAC Address      : 0012.e2a8.2527
 Neighbor MAC Address   : 0012.e2a8.2505
 Total VLAN Group Counts : 1

 VLAN Group ID : 1
  VLAN ID              : 110,200-2169
  Member Port          : 0/6-8
  Active Port          : 0/6-8
  Last Transition      : 20XX/07/14 10:00:00  (Master to Backup)
  Transition by reason : Priority was lower than neighbor's
  Master to Backup Counts : 4
  Backup to Master Counts : 4

                         Local              Neighbor
  State                : Backup             Master
  Acknowledged State   : Backup             -
  Advertise Hold Timer : 3                  -
  Priority             : 100                101
  Active Ports         : 3                  3
  Up Ports             : 3                  -

> clear gsrp 10 vlan-group 1

> show gsrp 10 vlan-group 1
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
 Local MAC Address      : 0012.e2a8.2527
 Neighbor MAC Address   : 0012.e2a8.2505
 Total VLAN Group Counts : 1

 VLAN Group ID : 1
  VLAN ID              : 110,200-2169
  Member Port          : 0/6-8
  Active Port          : 0/6-8
  Last Transition      : 20XX/07/14 10:00:00  (Master to Backup)
  Transition by reason : Priority was lower than neighbor's
  Master to Backup Counts : 0
  Backup to Master Counts : 0

                         Local              Neighbor
  State                : Backup             Master
  Acknowledged State   : Backup             -
  Advertise Hold Timer : 3                  -
  Priority             : 100                101
  Active Ports         : 3                  3
  Up Ports             : 3                  -
```

Figure 35-9: Example of clearing the GSRP statistics when a port is specified

```
> show gsrp 10 port 0/10 detail
Date 20XX/07/14 12:00:00 UTC
```

```
GSRP ID: 10
 Port Information
 0/10    GSRP   : Not Active Port   : Up
(CH:  1) Type   : Direct     Flush  : No        Delay       : 0
         TxFrame : 1027       RxFrame : 1020      Discard Frame : 2
         Discard Frame by reason
            mismatch GSRP VLAN ID    : 1
            mismatch GSRP ID         : 1
            loopback GSRP frame      : 0
            illegal GSRP frame       : 0

> clear gsrp 10 port 0/10

> show gsrp 10 port 0/10 detail
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
 Port Information
 0/10    GSRP   : Not Active Port   : Up
(CH:  1) Type   : Direct     Flush  : No        Delay       : 0
         TxFrame : 0          RxFrame : 0         Discard Frame : 0
         Discard Frame by reason
            mismatch GSRP VLAN ID    : 0
            mismatch GSRP ID         : 0
            loopback GSRP frame      : 0
            illegal GSRP frame       : 0
```

Display items

None

Impact on communication

None

Response messages

Table 35-9: List of response messages for the clear gsrp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
GSRP is not configured.	GSRP has not been configured. Check the configuration.
Specified GSRP ID is not configured:<gsrp group id>.	The specified GSRP group ID has not been configured. <gsrp group id>: Indicates the GSRP group ID.
Specified port is not operational.	The specified port and channel group are not active.
Specified VLAN group ID is not configured:<vlan group id>.	The specified VLAN group ID has not been configured. <vlan group id>: Indicates the VLAN group ID.

Notes

- Even if statistics are cleared, the value for the MIB information obtained by using SNMP is not cleared.

- If the configuration is deleted or added, the target statistics are cleared to zero.

set gsrp master

Changes backup (neighbor unknown) status to master status.

This command is effective only for the backup (neighbor unknown) status.

Syntax

```
set gsrp master <gsrp group id> vlan-group <vlan group id> [-f]
```

Input mode

User mode and administrator mode

Parameters

<gsrp group id>

Specify a GSRP group ID.

Specifiable values for GSRP group IDs are from 1 to 65535.

<vlan group id>

After a confirmation message is output, the status of the specified VLAN group ID is changed to the master status.

Specifiable values for a VLAN group ID are from 1 to 64.

-f

Switches the status to the master status without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 35-10: Example of executing the master transition command

```
> set gsrp master 10 vlan-group 8

Transit to Master. Are you sure? (y/n):y

> set gsrp master 10 vlan-group 8 -f

>
```

Display items

None

Impact on communication

The status is switched from communication disabled to communication enabled.

Response messages

Table 35-10: List of response messages for the set gsrp master command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
GSRP is not configured.	GSRP has not been configured. Check the configuration.
Specified GSRP ID is not configured:<gsrp group id>	The specified GSRP group ID has not been configured. <gsrp group id>: Indicates the GSRP group ID.
Specified VLAN group ID is not configured:<vlan group id>.	The specified VLAN group ID has not been configured. <vlan group id>: Indicates the VLAN group ID.
Specified VLAN group is not no neighbor state.	The specified VLAN group is not in backup (neighbor unknown) status. Use the "show gsrp" command to make sure the specified VLAN group is in backup (neighbor unknown) status before re-executing the "set gsrp master" command.

Notes

Execute this command after making sure the applicable VLAN group of the partner device is in backup status.

clear gsrp port-up-delay

Immediately puts the specified port, which is active and belongs to a VLAN that is configured to be a member of a VLAN group, in active port state without waiting for the delay time that was specified using the "port-up-delay" configuration command.

Syntax

```
clear gsrp port-up-delay [port <port list>] [channel-group-number <channel group list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

> Immediately puts a specified port, which is active and belongs to a VLAN that is configured to be a member of a VLAN group, in active state. 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>

> Immediately puts a specified channel group, which is active and belongs to a VLAN that is configured to be a member of a VLAN group, in active state. For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when all parameters are omitted:

> All ports, which are active and belong to a VLAN that is configured to be a member of a VLAN group, are immediately put in active state.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 35-11: Example of executing the clear gsrp port-up-delay command

```
> show gsrp 10 port 0/6-10
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
 Port Information
 0/6    GSRP   : Not Active Port   : Up
        Type   : Member    Flush  : Reset      Delay        : 43172
        TxFrame : 0         RxFrame : 0         Discard Frame : 0
 0/7    GSRP   : Not Active Port   : Up
        Type   : Member    Flush  : Reset      Delay        : 43174
        TxFrame : 0         RxFrame : 0         Discard Frame : 0
 0/8    GSRP   : Active    Port    : Up
        Type   : Member    Flush  : GSRP       Delay        : 0
        TxFrame : 0         RxFrame : 0         Discard Frame : 0
 0/10   GSRP   : Not Active Port   : Up
(CH:  1) Type  : Direct    Flush  : No         Delay        : 0
        TxFrame : 1993      RxFrame : 1987      Discard Frame : 0

> clear gsrp port-up-delay

> show gsrp 10 port 0/6-10
Date 20XX/07/14 12:00:00 UTC
```

```
GSRP ID: 10
 Port Information
 0/6     GSRP   : Active     Port   : Up
         Type   : Member     Flush  : Reset      Delay       : 0
         TxFrame : 0         RxFrame : 0         Discard Frame : 0
 0/7     GSRP   : Active     Port   : Up
         Type   : Member     Flush  : Reset      Delay       : 0
         TxFrame : 0         RxFrame : 0         Discard Frame : 0
 0/8     GSRP   : Active     Port   : Up
         Type   : Member     Flush  : GSRP       Delay       : 0
         TxFrame : 0         RxFrame : 0         Discard Frame : 0
 0/10    GSRP   : Not Active Port   : Up
(CH:  1) Type   : Direct     Flush  : No         Delay       : 0
         TxFrame : 2073      RxFrame : 2068       Discard Frame : 0

>
```

Figure 35-12: Example of executing the port-up-delay command when a port is specified

```
> show gsrp 10 port 0/6
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
 Port Information
 0/6     GSRP   : Not Active Port   : Up
         Type   : Member     Flush  : Reset      Delay        : 43180
         TxFrame : 0         RxFrame : 0         Discard Frame : 0

> clear gsrp port-up-delay port 0/6

> show gsrp 10 port 0/6
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
 Port Information
 0/6     GSRP   : Active     Port   : Up
         Type   : Member     Flush  : Reset      Delay       : 0
         TxFrame : 0         RxFrame : 0         Discard Frame : 0

>
```

Display items

None

Impact on communication

None

Response messages

Table 35-11: List of response messages for the clear gsrp port-up-delay command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
GSRP is not configured.	GSRP has not been configured. Check the configuration.
Specified port is not operational.	The specified port and channel group are not active.

Notes

None

clear gsrp forced-shift

Cancels the wait period for automatically switching to the master status when the function for switchover to the master status by an independently started GSRP switch is enabled. The current status of the VLAN group remains unchanged, and the GSRP switch is not automatically changed to the master status next time it is started.

This command is valid until the status is changed to the master status automatically by the master transition function the GSRP switch is independently started.

Syntax

```
clear gsrp forced-shift [<gsrp group id>]
```

Input mode

User mode and administrator mode

Parameters

<gsrp group id>

Cancels the automatic-transition-to-master and associated wait (delay) for the designated GSRP group ID. Even if the waiting state is canceled, the current status of the VLAN group remains unchanged, and the GSRP switch is not automatically changed to the master status.

Specifiable values for GSRP group IDs are from 1 to 65535.

Behavior when this parameter is omitted:

For all GSRP groups, the automatic-transition-to-master and associated wait (delay) is canceled. Even if the waiting state is canceled, the current status of the VLAN group remains unchanged, and the GSRP switch is not automatically changed to the master status.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 35-13: Example of canceling the GSRP automatic-transition-to-master wait time

```
> clear gsrp forced-shift 1

>
```

Display items

None

Impact on communication

None

Response messages

Table 35-12: List of response messages for the clear gsrp forced-shift command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
GSRP is not configured.	GSRP has not been configured. Check the configuration.
Specified GSRP ID is not configured:<gsrp group id>	The specified GSRP group ID has not been configured. <gsrp group id>: Indicates the GSRP group ID.

Notes

None

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} restart gsrp [-f] [core-file]
```

Example

Figure 35-14: 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.

Response messages

Table 35-13: List of response messages for the restart gsrp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
GSRP program failed to be restarted.	An attempt to restart the GSRP program by using this command failed. Re-execute the command.

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

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} dump protocols gsrp
```

Example

Figure 35-15: Example of taking a GSRP dump

```
> dump protocols gsrp

>
```

Display items

None

Impact on communication

None

Response messages

Table 35-14: List of response messages for the dump protocols gsrp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

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.

36 VRRP

show vrrpstatus(IPv4)

Displays the status of VRRP virtual routers.

Syntax

```
show vrrpstatus [detail][statistics][group][protocol ip][{ name <virtual router name> | interfa
ce vlan <vlan id> [vrid <vrid>]}]
```

Input mode

User mode and administrator mode

Parameters

detail

Displays detailed information about the virtual router status.

Behavior when this parameter is omitted:

An overview of virtual routers is displayed.

statistics

Display statistics for virtual routers.

Behavior when this parameter is omitted:

Information about the virtual router status is displayed.

group

Displays group information.

Behavior when this parameter is omitted:

Information about the virtual router status is displayed.

protocol ip

Displays information about an IPv4 protocol virtual router.

Behavior when this parameter is omitted:

Displays information about both IPv4 and IPv6-protocol virtual routers.

{ name <virtual router name> | interface vlan <vlan id> [vrid <vrid>]}

name <virtual router name>

Specifies the name of a virtual router.

interface vlan <vlan id> [vrid <vrid>]

Specifies the interface that is used to configure the virtual router.

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

For vrid <vrid>, specify a virtual router ID. If it is omitted, information about all virtual routers for the specified interface is displayed.

Behavior when this parameter is omitted:

Information about virtual routers for all interfaces is displayed.

Behavior when all parameters are omitted:

A list of virtual routers, and information about their statuses are displayed.

Operation when a stack configuration is used

This command is not supported.

Example 1

Figure 36-1: Example of displaying the summary information about IPv4 protocol virtual routers

```
> show vrrpstatus protocol ip
Date 20XX/12/10 12:00:00 UTC
VLAN0010 VRID 1 VRF 2 MASTER virtual-ip 170.10.10.2 priority 150/150
VLAN0030 VRID 2 BACKUP virtual-ip 170.10.10.3 priority 100/100
>
```

Display items in Example 1

Table 36-1: Items displayed for the summary information about IPv4 protocol virtual routers

Item		Meaning	Displayed detailed information
<interface name> VRID <vrid> [VRF <vrf id>] <state> virtual-ip <virtual ip address> priority <priority>/<original priority>			
Summary information	<interface name>	Name of the interface where a virtual router is running	—
	VRID <vrid>	Virtual router ID	—
	VRF <vrf id> [SL-L3A]	VRF ID	This is not displayed if the virtual router is running in a global network.
	<state>	Current status of a virtual router	MASTER: Indicates that the virtual router is working as the master. BACKUP: Indicates that the virtual router is working as the backup. INITIAL: Indicates that the virtual router is in initial status.
	virtual-ip <virtual ip address>	Virtual IP address	—
	priority <priority>/ <original priority>	Virtual router priority	<priority>: Indicates the current priority of the virtual router. <original priority>: Indicates the priority set in the configuration. If the configuration setting is omitted, the initial value, 100, is displayed.
	primary <virtual router name>	Virtual router name	This item is not displayed if the virtual router name is not set or if the virtual router is a follower virtual router.
	follow <primary virtual router name>	Name of the primary virtual router that follows actions	This item is displayed if the virtual router is a follower virtual router.

Example 2

Figure 36-2: Displaying the detailed virtual router status (for a primary virtual router)

```
> show vrrpstatus detail interface vlan 10 vrid 1
Date 20XX/12/10 12:00:00 UTC
VLAN0010: VRID 1 VRF 2
   Virtual Router IP Address : 170.10.10.2
   Virtual MAC Address : 0000.5e00.0101
```

```
          Virtual Router Name : VRRPNAME1 (primary)
          Virtual Router Follow :-
          Number of Follow virtual routers : 4
          Current State : MASTER
          Admin State : enable
          Priority : 80 /100
          IP Address Count : 1
          Master Router's IP Address : 170.10.10.2
          Primary IP Address : 170.10.10.1
          Authentication Type : SIMPLE TEXT PASSWORD
          Authentication Key : ABCDEFG
          Advertisement Interval : 1 sec
          Preempt Mode : ON
          Preempt Delay : 60
          Non Preempt swap timer :30
          Accept Mode : ON
          Virtual Router Up Time : Mon Dec  6 16:55:00 20XX
          track 10 VLAN0022 VRF 3 Status : (IF UP) Down Priority : 50
            Target Address : 192.168.0.20
            Vrrp Polling Status : reachable
          track 20 VLAN0023  Status : (IF UP) Down Priority : 40
          track 30 gigabitethernet 0/10 Status : (IF DOWN) Down Priority : 20
          track 40 port-channel 2 Status : (IF UP) Down Priority : 20
>
```

Figure 36-3: Displaying the detailed virtual router status (for a follower virtual router)

```
> show vrrpstatus detail interface vlan 10 vrid 2
Date 20XX/12/10 12:00:00 UTC
VLAN0010: VRID 2 VRF 2
   Virtual Router IP Address : 170.10.10.2
   Virtual MAC Address : 0000.5e00.0101
   Virtual Router Name :VRRPNAME2 (follow)
   Virtual Router Follow : VRRPNAME1
   Number of Follow virtual routers : 0
   Current State : MASTER
   Admin State : enable
   Priority : - /100 (Disable)
   IP Address Count : 1
   Master Router's IP Address : - (Disable)
   Primary IP Address : 170.10.10.1
   Authentication Type : SIMPLE TEXT PASSWORD(Disable)
   Authentication Key : ABCDEFG (Disable)
   Advertisement Interval : 20 sec (Disable)
   Preempt Mode : ON (Disable)
   Preempt Delay : 60 (Disable)
   Non Preempt swap timer :30 (Disable)
   Accept Mode : ON
   Virtual Router Up Time : Mon Dec  6 16:55:00 20XX
   track 10 VLAN0022 VRF 3 Status : (Disable) Down Priority : 50
     Target Address : 192.168.0.20
     Vrrp Polling Status : (Disable)
   track 20 VLAN0023  Status : (Disable) Down Priority : 40
   track 30 gigabitethernet 0/10 Status : (Disable) Down Priority : 20
   track 40 port-channel 2 Status : (Disable) Down Priority : 20
>
```

Display items in Example 2

Table 36-2: Items displayed for the virtual router status

Item	Meaning	Displayed detailed information
<interface name>: VRID <vrid> [VRF <vrf id>]	Name of the interface where a virtual router is running, and its VRID information	<interface name>: Indicates the name of the interface where the virtual router is running. <vrid>: Indicates the virtual router ID. VRF <vrf id>: Indicates the VRF ID. This is not displayed if the virtual router is running in a global network. [SL-L3A]

Item	Meaning	Displayed detailed information
Virtual Router IP Address : <ip address>[(ADDRESS OWNER)]	IP address of the virtual router	(ADDRESS OWNER): Displayed if the user is the owner of the address.
Virtual MAC Address : <mac address>	MAC address of the virtual router	—
Virtual Router Name : <virtual router name>({primary | follow })	Virtual router name	{primary	follow}: Type of virtual router
Virtual Router Follow : <virtual router name> ({ <interface name>: VRID <vrid> [VRF <vrf id>] | not running })	Name of the primary virtual router that follows actions	<virtual router name>: "-" is displayed for the primary virtual router. For a follower virtual router, the item displays the name of the primary virtual router that follows actions. < interface name>: Indicates the name of the interface where the primary virtual router is running. <vrid>: Indicates the virtual router ID of the primary virtual router. VRF <vrf id>: Indicates the VRF ID of the primary virtual router. This is not displayed if the primary virtual router is running in a global network. [SL-L3A] not running: The primary virtual router with the specified name does not exist.
Number of Follow virtual routers : <N>	The number of follower virtual routers that follow actions	N: Indicates a value from 0 to 4094.
Current State : <status>	Current status of a virtual router	MASTER: Indicates that the virtual router is working as the master. BACKUP: Indicates that the virtual router is working as the backup. INITIAL: Indicates that the virtual router is in initial status.
Admin State : [enable	disable<flag>]	Current behavior status of a virtual router	enable: Indicates that the virtual router is running. disable: Indicates that the virtual router is not running. <flag>: Indicates the reason why the virtual router is not running. (IF DOWN): Indicates that the status of the applicable interface is DOWN. (TRACK DOWN): The priority was set to 0 by the tracking function. (NOIP): The IP address of the applicable interface was not set. (NOJOIN): An attempt to join a multicast group failed. (S/W FAIL): An attempt to register a virtual MAC address in the hardware failed.

Item	Meaning	Displayed detailed information
Priority : <priority> /<original priority> [(Disable)]	Virtual router priority	<priority>: Indicates the current priority of the virtual router. <original priority>: Indicates the priority set in the configuration. If the configuration setting is omitted, the initial value, 100, is displayed. (Disable): Indicates that the virtual router is disabled. This function is disabled for follower virtual routers. A hyphen (-) is displayed for <priority>. This item is displayed for primary virtual routers.
IP Address Count : <N>	Number of virtual router IP addresses	—
Master Router's IP Address : <ip address> [(Disable)]	IP address of the router currently working as the master	<ip address>: IP address of the router currently working as the master A hyphen (-) is displayed for follower virtual routers. (Disable): Indicates that the virtual router is disabled. This function is disabled for follower virtual routers. This item is displayed for primary virtual routers.
Primary IP Address : <ip address>	IP address of an interface for which VRRP is configured	—
Authentication Type : <type> [(Disable)]	Packet authentication type	NONE: No packet authentication is performed. SIMPLE TEXT PASSWORD: Indicates a text password. (Disable): Indicates that the virtual router is disabled. This function is disabled for follower virtual routers. This function is disabled if the router is not supported in VRRP running mode.
Authentication Key : <text> [(Disable)]	Text password	(Disable): Indicates that the virtual router is disabled. This function is disabled for follower virtual routers. It is also is disabled if the router is not supported in VRRP running mode.
Advertisement Interval : <second> sec [(Disable)]	Sending interval for ADVERTISEMENT packets (in seconds)	1 to 255 (Disable): Indicates that the virtual router is disabled. This function is disabled for follower virtual routers. This item is displayed for primary virtual routers.
Preempt Mode : {ON	OFF} [(Disable)]	Automatic preemption setting	ON: Indicates that the automatic switchback function is enabled. OFF: Indicates that the automatic switchback function is suppressed. (Disable): Indicates that the virtual router is disabled. This function is disabled for follower virtual routers. This item is displayed for primary virtual routers.
Preempt Delay : <second> [(Now Waiting, <N> sec left)] [(Disable)]	Suppression timer setting period (in seconds)	(Now Waiting, <N>sec left): Displays the remaining time until the state is changed to master while switching to the master status is suppressed by this setting. N: Indicates a value from 1 to 65535. (Disable): Indicates that the virtual router is disabled. This function is disabled for follower virtual routers. This item is displayed for primary virtual routers.

Item	Meaning	Displayed detailed information
Non Preempt swap timer : <second> [(Now Waiting, <N> sec left)] [(Disable)]	Preemption suppression time (in seconds) while automatic preemption is suppressed	(Now Waiting, <N>sec left): Displays the remaining time until the state is changed to master while switching to the master status is suppressed by this setting. N: Indicates a value from 1 to 65535. (Disable): Indicates that the virtual router is disabled. This function is disabled for follower virtual routers. This item is displayed for primary virtual routers.
Accept Mode : {ON | OFF}	Accept mode	ON: Indicates the accept mode. OFF: Indicates that accept mode is turned off. For an address owner, "-" is displayed regardless of the address mode setting.
Virtual Router Up Time : <time string>	Time when a virtual router is changed from the INITIAL state	This item is not displayed if the virtual router is in INITIAL state.

track <track-number> {<interface name> [VRF <vrf id>]|<interface type> <interface number>} Status : <status> {Down Priority|Critical Priority} : <priority>	Information about a track assigned to a virtual router	<track-number>: Indicates the track number of the track assigned to a virtual router.
		<interface name>: Indicates the interface name of the VLAN interface that monitors for failures.
		VRF <vrf id>: Indicates the VRF ID.
		When the destination for VRRP polling is a global network, this item is not displayed. [SL-L3A]
		<interface type> <interface number>: Indicates an interface that monitors for failures. Note that <interface number> is displayed without <switch no.>.
		• Ethernet interface
		• Port channel interface
		<status>: Indicates the current status of an interface that monitors failures.
		  (IF UP): Indicates that the interface is in UP status.
		  (IF DOWN): Indicates that the interface is in DOWN status.
		  (Disable): Indicates that the track assigned to a virtual router is invalid.
		Method for changing priority
		Down Priority : <priority>: Indicates the priority is decreased if an interface that monitors failures is in DOWN status.
		Critical Priority : <priority>: Indicates the priority to be replaced when the interface that monitors failures is in DOWN status.

Target Address : <target-address> [(check reply interface)]	Destination address for VRRP polling	<target-address>: Indicates the target address for VRRP polling. This item is not displayed if the IP address for VRRP polling has not been specified, or for a fault monitoring interface. (check reply interface): This information is displayed if the "track check-reply-interface" configuration command has been used to configure this.

Item	Meaning	Displayed detailed information

Vrrp Polling Status : <status>[<reason>] [(Disable)]	VRRP polling information	This item is not displayed if the IP address for VRRP polling has not been specified, or for a fault monitoring interface.
		<status>: Indicates connectivity detected through VRRP polling.
		  reachable: Indicates that communication is possible.
		  (Disable): Indicates that the virtual router is disabled.
		  unreachable: Indicates that communication is impossible.
		<reason>: Provides a detailed reason why communication is impossible.
		This information is displayed if <status> is unreachable.
		  (interface down): Indicates that the source interface for polling is in DOWN status.
		  (no response): Indicates that there were no responses from the polling destination.
		  (no route): Indicates that there are no routes to the polling destination.
		  (invalid response): When the "track check-reply-interface" configuration command is set, responses from the interface that sent the polling request and also from another interface were received.

Example 3

Figure 36-4: Displaying the virtual router statistics

```
> show vrrpstatus statistics interface vlan 10 vrid 1
Date 20XX/12/10 12:00:00 UTC
VLAN0010: VRID 1 VRF 2
   5 times transitions to master
   1500 advertisement received
            0 with bad advertisement interval
            0 with authentication failed
            0 with bad ip ttl
            3 with priority zero
            0 with invalid type
            0 with bad ip address list
            0 with bad authentication type
            0 with authentication type mismatch
            0 with packet length error
            0 with different VRRP version
            0 with low priority
   1300 advertisement sent
            0 with priority zero
   1 virtual MAC learning frame sent
   0 change by command
   0 change by interface down
   0 change by receiving advertisement with high priority
   0 change by Master_Down_Timer timeout
   0 master transition delay count
   track 10  VLAN0022 VRF 3 Target-Address : 192.168.0.20
     VRRP Polling round-trip min/avg/max = 0.266/0.274/0.286 ms
     1 priority down by detected
   track 20  VLAN0023  line-protocol
     0 priority down by detected
   track 30 gigabitethernet 0/10 line-protocol
     0 priority down by detected
   track 40 port-channel 2 line-protocol
     0 priority down by detected
>
```

Display items in Example 3

Table 36-3: Items displayed for the virtual router statistics

Item	Meaning	Displayed detailed information
<interface name> : VRID <vrid> [VRF <vrf id>]	Name of the interface where a virtual router is running, and its VRID information	<interface name>: Indicates the name of the interface where the virtual router is running. <vrid>: Indicates the virtual router ID. VRF <vrf id>: Indicates the VRF ID. This is not displayed if the virtual router is running in a global network. [SL-L3A]
<number of packets> times transitions to master	Number of transitions to the master status	—
<number of packets> advertisement received	Number of received ADVERTISEMENT packets	—
<number of packets> with bad advertisement interval	Number of received ADVERTISEMENT packets that have invalid packet-sending intervals	—
<number of packets> with authentication failed	Number of received ADVERTISEMENT packets of which authentication failed	—
<number of packets> with bad ip ttl	Number of received ADVERTISEMENT packets whose TTL for the IP header is not 255	—
<number of packets> with priority zero	Number of received ADVERTISEMENT packets whose priority is 0	—
<number of frame> virtual MAC learning frame sent	Number of frames sent for MAC address learning	—
<number of packets> with invalid type	Number of received ADVERTISEMENT packets that had an invalid value in the type field	—
<number of packets> with bad ip address list	Number of received ADVERTISEMENT packets that have invalid virtual router IPv4 addresses	—

Item	Meaning	Displayed detailed information
\<number of packets\> with bad authentication type	Number of received ADVERTISE-MENT packets with invalid packet authentication types	—
\<number of packets\> with authentication type mismatch	Number of received ADVERTISE-MENT packets whose packet authentication type did not match the local setting.	—
\<number of packets\> with packet length error	Number of received ADVERTISE-MENT packets whose packet length was invalid	—
\<number of packets\> with different VRRP version	Number of received packets whose version of ADVERTISEMENT packets and that of VRRP running mode do not match	—
\<number of packets\> with low priority	Number of received ADVERTISE-MENT packets with lower priority	—
\<number of packets\> advertisement sent	Number of sent ADVERTISE-MENT packets	—
\<number of packets\> with priority zero	Number of sent ADVERTISE-MENT packets whose priority is 0	—
\<N\> change by command	Number of times that the "swap vrrp" command was executed	—
\<N\> change by interface down	Number of status transitions due to interface down	—
\<N\> change by receiving advertisement with high priority	Number of status transitions caused by receipt of a high-priority ADVERTISEMENT packet	—
\<N\> change by Master_Down_Timer timeout	Number of status transitions because the Master Down Timer timed out	—

Item	Meaning	Displayed detailed information
<N> master transition delay count	Number of times that the suppression timer has been started	—
track <track-number> {<interface name> [VRF <vrf id>]|<interface type> <interface number>} {Target-Address : <target-address>|line-protocol}	VRRP polling information assigned to a virtual router	<track-number>: Indicates the track number of the track assigned to a virtual router. <interface name>: Indicates the name of an interface that monitors failures. VRF <vrf id>: Indicates the VRF ID. When the destination for VRRP polling is a global network, this item is not displayed. [SL-L3A] <interface type> <interface number>: Indicates an interface that monitors for failures. Note that <interface number> is displayed without <switch no.>. • Ethernet interface • Port channel interface Target-Address : <target-address>: Indicates the destination IP address for VRRP polling. line-protocol: Applied to a fault monitoring interface.
VRRP Polling round-trip min/avg/max =<minimum>/<average>/<maximum> ms	Packet response time for VRRP polling	This item is not displayed if the IP address for VRRP polling has not been specified, or for a fault monitoring interface. <minimum>/<average>/<maximum>: Indicates the minimum value, average value, and maximum value.
<N> priority down by detected	Number of times that the priority has been decreased due to a track error	—

Example 4

Figure 36-5: Displaying the group information of a primary virtual router

```
> show vrrpstatus group name VRRPNAME1
Date 20XX/12/10 12:00:00 UTC
VLAN0010: VRID 1 VRF 2
    Virtual Router Name           : VRRPNAME1 (primary)
    Virtual Router Follow         : -
    Number of Follow virtual routers : 4
    Followed by virtual routers   :
        VLAN0020: VRID 1 VRF 2
        VLAN0030: VRID 1 VRF 2
        VLAN0040: VRID 1 VRF 2
        VLAN0050: VRID 1 VRF 2
```

Figure 36-6: Displaying the group information of a follower virtual router

```
> show vrrpstatus group interface vlan 10 vrid 1
Date 20XX/12/10 12:00:00 UTC
VLAN0010: VRID 1 VRF 2
    Virtual Router Name           : VRRPNAME2 (follow)
    Virtual Router Follow         : VRRPNAME1 (VLAN0010: VRID 1 VRF 2 )
    Number of Follow virtual routers : 0
    Followed by virtual routers   : -
```

Display items in Example 4

Table 36-4: Items displayed for the group information of virtual routers

Item	Meaning	Displayed detailed information
<interface name> : VRID <vrid> [VRF <vrf id>]	Name of the interface where a virtual router is running, and its VRID information	<interface name>: Indicates the name of the interface where the virtual router is running. <vrid>: Indicates the virtual router ID. VRF <vrf id>: Indicates the VRF ID. This is not displayed if the virtual router is running in a global network. [SL-L3A]
Virtual Router Name : <virtual router name> ({primary | follow})	Virtual router name	{primary	follow}: Type of virtual router
Number of Follow virtual routers : <N>	Number of follower virtual routers	—
Followed by virtual routers: <interface name> : VRID <vrid> [VRF <vrf id>]	List of follower virtual routers	A hyphen (-) is displayed for follower virtual routers. <interface name>: Indicates the name of the interface where the follower virtual router is running. <vrid>: Indicates the virtual router ID. VRF <vrf id>: Indicates the VRF ID. This is not displayed if the virtual router is running in a global network. [SL-L3A]

Impact on communication

None

Response messages

Table 36-5: List of response messages for the show vrrpstatus (IPv4) command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
no entries.	There are no applicable virtual routers.

Notes

None

clear vrrpstatus(IPv4)

Clears the counter for VRRP virtual router statistics.

Syntax

```
clear vrrpstatus [protocol ip] [{ name <virtual router name> | interface vlan <vlan id> [vrid
<vrid>]}]
```

Input mode

User mode and administrator mode

Parameters

protocol ip

Clears the IPv4 protocol virtual router statistics.

Behavior when this parameter is omitted:

Clears the statistics for both IPv4 and IPv6-protocol virtual routers.

{ name <virtual router name> | interface vlan <vlan id> [vrid <vrid>]}

name <virtual router name>

Specifies the name of a virtual router.

interface vlan <vlan id> [vrid <vrid>]

Specifies the interface that is used to configure the virtual router.

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

For vrid <vrid>, specify a virtual router ID. If it is omitted, statistics about all virtual routers for the specified interface is cleared.

Behavior when this parameter is omitted:

Clears the statistics on virtual routers for all interfaces.

Behavior when all parameters are omitted:

Clears the counter for all virtual router statistics.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 36-7: Clearing the counters for virtual router statistics

```
> clear vrrpstatus interface vlan 10 vrid 1
>
```

Display items

None

Impact on communication

None

Response messages

Table 36-6: List of response messages for the clear vrrpstatus (IPv4) command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
no entries.	There are no applicable virtual routers.

Notes

None

swap vrrp(IPv4)

Changes the device status when switchback is suppressed.

If the device is in the master status, it is changed to the backup status.

If the device is in the backup status, it is changed to the master status.

Syntax

```
swap vrrp [-f] { name <virtual router name> | interface vlan <vlan id> [vrid <vrid>] }
```

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.

{ name <virtual router name> | interface vlan <vlan id> [vrid <vrid>]}

    name <virtual router name>

        Specifies the name of a virtual router.

    interface vlan <vlan id> [vrid <vrid>]

        Specifies the interface that is used to configure the virtual router.

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

        For vrid <vrid>, specify a virtual router ID. If it is omitted, a confirmation message for individual virtual routers configured for the specified interface is displayed.

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows how to change VRID "1" and VRID "20" virtual routers that are configured for VLAN "10", which are currently operating as the master, to the backup status.

Figure 36-8: Performing switchback for virtual routers

```
> swap vrrp interface vlan 10
Exchange VRRP 1 OK? (y/n): y
Exchange VRRP 20 OK? (y/n): y
>
```

Display items

None

Impact on communication

Communication might stop temporarily because of status transitions in VRRP.

Response messages

Table 36-7: List of response messages for the swap vrrp (IPv4) command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Command execution cannot be performed to follow virtual router.	This command cannot be executed for follower virtual routers.
Command execution cannot be performed to owner's virtual router of an initial state.	This command cannot be executed for virtual routers in initial status.
Command execution cannot be performed to owner's virtual router.	This command cannot be executed for the virtual router of the address owner.
no entries.	There are no applicable virtual routers.

Notes

- If this command is executed from a virtual router that has lower or equal priority (including the default priority), the device status might not be changed to the master status.
- This command cannot be entered for an address owner, follower virtual router, or a device in initial status.
- If a switchback command is executed while switchback is suppressed, the command is given priority and switchback is performed.
- If the command is executed when switchback is not suppressed, switchback is performed, even though that does not seem to be the case because the status of the virtual router with the higher priority is changed to the master status by the automatic switchback function.
- When the command is executed, both virtual routers are swapped to the backup or master status temporarily, but they are changed back to the master or backup status automatically.
- When switchback cannot be performed due to a failure of other devices, if the command is executed, communication is suspended for four seconds by default.
- In a configuration where the "no vrrp preempt" and the "vrrp timers non-preempt-swap" configuration commands are set for all devices that make up the VRRP, if a switchback command is executed in the master device, all devices change to the backup status until the period set for the "vrrp timers non-preempt-swap" command elapses. To avoid this situation, do not set the "vrrp timers non-preempt-swap" command for at least one of the devices that makes up the VRRP. If all the devices are in backup status, you can make one of the devices the master device by executing the "swap vrrp" command and specifying the device.

The table below lists the results of executing this command. No status change in the following table indicates situation where it does not seem that switchback is performed.

Table 36-8: List of execution results for the swap vrrp (IPv4) command

—			This device is being suppressed		This device is not suppressed	
			Another device is being suppressed	Another device is not being suppressed	Another device is being suppressed	Another device is not being suppressed
This device (Master)	Comparison of the priority between this device and another device	High	Switched	Switched	No status change	No status change
		Equal	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.
		Low	Switchback	Switchback	Switchback	Switchback
This device (Backup)		High	Switchback	Switchback	Switchback	Switchback
		Equal	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.
		Low	No status change	No status change	No status change	No status change

Terms used in the above table:

- This device: A device in which the "swap vrrp" command is executed.

- Another device: A device other than this device.

- Switched: The priority of the master device is changed from high to low.

show vrrpstatus(IPv6)

Displays the status of VRRP virtual routers.

Syntax

```
show vrrpstatus [detail][statistics][group][protocol ipv6][{ name <virtual router name> | inter
face vlan <vlan id> [vrid <vrid>]}]
```

Input mode

User mode and administrator mode

Parameters

detail

　　Displays detailed information about the virtual router status.

　　Behavior when this parameter is omitted:

　　　　An overview of virtual routers is displayed.

statistics

　　Display statistics for virtual routers.

　　Behavior when this parameter is omitted:

　　　　Information about the virtual router status is displayed.

group

　　Displays group information.

　　Behavior when this parameter is omitted:

　　　　Information about the virtual router status is displayed.

protocol ipv6

　　Displays information about an IPv6 protocol virtual router.

　　Behavior when this parameter is omitted:

　　　　Displays information about both IPv4 and IPv6-protocol virtual routers.

{ name <virtual router name> | interface vlan <vlan id> [vrid <vrid>]}

　　name <virtual router name>

　　　　Specifies the name of a virtual router.

　　interface vlan <vlan id> [vrid <vrid>]

　　　　Specifies the interface that is used to configure the virtual router.

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

　　　　For vrid <vrid>, specify a virtual router ID. If it is omitted, information about all virtual routers for the specified interface is displayed.

　　Behavior when this parameter is omitted:

　　　　All virtual router information is displayed.

Behavior when all parameters are omitted:

　　A list of virtual routers, and information about their statuses are displayed.

Operation when a stack configuration is used

This command is not supported.

Example 1

Figure 36-9: Example of displaying the summary information about IPv6 protocol virtual routers

```
> show vrrpstatus protocol ipv6
Date 20XX/12/10 12:00:00 UTC
VLAN0010 VRID 1 VRF 2 MASTER virtual-ip 100:0:11::100 priority 150/150
VLAN0013 VRID 1 BACKUP virtual-ip 100:0:13::100 priority 100/100
>
```

Display items in Example 1

Table 36-9: Items displayed for the summary information about IPv6 protocol virtual routers

Item		Meaning	Displayed detailed information
<interface name> VRID <vrid> [VRF <vrf id>] <state> virtual-ip <virtual ip address> priority <priority>/<original priority>			
Summary information	<interface name>	Name of the interface where a virtual router is running	—
	VRID <vrid>	Virtual router ID	—
	VRF <vrf id> [SL-L3A]	VRF ID	This is not displayed if the virtual router is running in a global network.
	<state>	Current status of a virtual router	MASTER: Indicates that the virtual router is working as the master. BACKUP: Indicates that the virtual router is working as the backup. INITIAL: Indicates that the virtual router is in initial status.
	virtual-ip <virtual ip address>	Virtual IP address	—
	priority <priority>/<original priority>	Virtual router priority	<priority>: Indicates the current priority of the virtual router. <original priority>: Indicates the priority set in the configuration. If the configuration setting is omitted, the initial value, 100, is displayed.

Example 2

Figure 36-10: Displaying the detailed virtual router status

```
> show vrrpstatus detail interface vlan 10 vrid 3
Date 20XX/12/10 12:00:00 UTC
VLAN0010: VRID 3 VRF 2
   Virtual Router IP Address : fe80::1234
   Virtual MAC Address : 0000.5e00.0203
   Virtual Router Name : VRRPNAME1
   Current State : MASTER
   Admin State : enable
   Priority : 100/120
   IP Address Count : 1
   Master Router's IP Address : fe80::abcd
   Primary IP Address : fe80::abcd
   Authentication Type : SIMPLE TEXT PASSWORD(Disable)
```

```
    Authentication Key : ABCDEFG(Disable)
    Advertisement Interval : 1 sec
    Preempt Mode : ON
    Preempt Delay : 60
    Non Preempt swap timer :30
    Accept Mode : ON
    Virtual Router Up Time : Mon Dec  6 16:55:00 20XX
    track 10 VLAN0022 VRF 3 Status : (IF UP) Down Priority : 50
      Target Address : fe80::ba
      Vrrp Polling Status : reachable
    track 20 VLAN0023 Status : (IF UP) Down Priority : 40
    track 30 gigabitethernet 0/10  Status : (IF DOWN) Down Priority : 20
    track 40 port-channel 2 Status : (IF UP) Down Priority : 20
    IPv6 Advertisement Type :ietf-ipv6-spec-07-mode
>
```

Display items in Example 2

Table 36-10: Items displayed for the virtual router status

Item	Meaning	Displayed detailed information
<interface name> : VRID <vrid> [VRF <vrf id>]	Name of the interface where a virtual router is running, and its VRID information	<interface name>: Indicates the name of the interface where the virtual router is running. <vrid>: Indicates the virtual router ID. VRF <vrf id>: Indicates the VRF ID. This is not displayed if the virtual router is running in a global network. [SL-L3A]
Virtual Router IP Address : <ip address>[(ADDRESS OWNER)]	IP address of the virtual router	(ADDRESS OWNER): Displayed if the user is the owner of the address.
Virtual MAC Address : <mac address>	MAC address of the virtual router	—
Virtual Router Name : <virtual router name>	Virtual router name	—
Current State : <status>	Current status of a virtual router	MASTER: Indicates that the virtual router is working as the master. BACKUP: Indicates that the virtual router is working as the backup. INITIAL: Indicates that the virtual router is in initial status.
Admin State : [enable | disable<flag>]	Current behavior status of a virtual router	enable: Indicates that the virtual router is running. disable: Indicates that the virtual router is not running. <flag>: Indicates the reason why the virtual router is not running. (IF DOWN): Indicates that the status of the applicable interface is DOWN. (TRACK DOWN): The priority was set to 0 by the tracking function. (NOIP): The IP address of the applicable interface was not set. (NOJOIN): An attempt to join a multicast group failed. (S/W FAIL): An attempt to register a virtual MAC address in the hardware failed.
Priority : <priority> / <original priority>	Virtual router priority	<priority>: Indicates the current priority of the virtual router.

Item	Meaning	Displayed detailed information
		<original priority>: Indicates the priority set in the configuration. If the configuration setting is omitted, the initial value, 100, is displayed.
IP Address Count : <N>	Number of virtual router IP addresses	—
Master Router's IP Address : <ip address>	IP address of the router currently working as the master	—
Primary IP Address: <ip address>	IP address of an interface for which VRRP is configured	—
Authentication Type : <type>[(Disable)]	Packet authentication type	NONE: No packet authentication is performed. SIMPLE TEXT PASSWORD: Indicates a text password. (Disable): Indicates that the virtual router is disabled. This function is disabled if the router is not supported in VRRP running mode.
Authentication Key : <text>[(Disable)]	Text password	(Disable): Indicates that the virtual router is disabled. This function is disabled if the router is not supported in VRRP running mode.
Advertisement Interval : <second> sec	Sending interval for ADVERTISEMENT packets (in seconds)	1 to 255
Preempt Mode : {ON | OFF}	Automatic preemption setting	ON: Indicates that the automatic switchback function is enabled. OFF: Indicates that the automatic switchback function is suppressed.
Preempt Delay : <second> [(Now Waiting, <N>sec left)]	Suppression timer setting period (in seconds)	(Now Waiting, <N>sec left): Displays the remaining time until the state is changed to master while switching to the master status is suppressed by this setting. N: Indicates a value from 1 to 65535.
Non Preempt swap timer : <second> [(Now Waiting, <N>sec left)]	Preemption suppression time (in seconds) while automatic preemption is suppressed	(Now Waiting, <N>sec left): Displays the remaining time until the state is changed to master while switching to the master status is suppressed by this setting. N: Indicates a value from 1 to 65535.
Accept Mode : {ON | OFF}	Accept mode	ON: Indicates the accept mode. OFF: Indicates that accept mode is turned off. For an address owner, "-" is displayed regardless of the address mode setting.
Virtual Router Up Time : <time string>	Time when a virtual router is changed from the INITIAL state	This item is not displayed if the virtual router is in INITIAL state.

Item	Meaning	Displayed detailed information

track <track-number> {<interface name> [VRF <vrf id>]|<interface type><interface number>} Status : <status> {Down Priority|Critical Priority} : <priority>	Information about a track assigned to a virtual router	<track-number>: Indicates the track number of the track assigned to a virtual router.
		<interface name>: Indicates the interface name of the VLAN interface that monitors for failures.
		VRF <vrf id>: Indicates the VRF ID.
		When the destination for VRRP polling is a global network, this item is not displayed. [SL-L3A]
		<interface type> <interface number>: Indicates an interface that monitors for failures. Note that <interface number> is displayed without <switch no.>.
		• Ethernet interface
		• Port channel interface
		<status>: Indicates the current status of an interface that monitors failures.
		  (IF UP): Indicates that the interface is in UP status.
		  (IF DOWN): Indicates that the interface is in DOWN status.
		Method for changing priority
		Down Priority : <priority>: Indicates the priority is decreased if an interface that monitors failures is in DOWN status.
		Critical Priority : <priority>: Indicates the priority to be replaced when the interface that monitors failures is in DOWN status.

Target Address : <target-address> [(check reply interface)]	Destination address for VRRP polling	<target-address>: Indicates the target address for VRRP polling. This item is not displayed if the IP address for VRRP polling has not been specified, or for a fault monitoring interface. (check reply interface): This information is displayed if the "track check-reply-interface" configuration command has been used to configure this.

Vrrp Polling Status : <status>[<reason>]	VRRP polling information	This item is not displayed if the IP address for VRRP polling has not been specified, or for a fault monitoring interface.
		<status>: Indicates connectivity detected through VRRP polling.
		  reachable: Indicates that communication is possible.
		  unreachable: Indicates that communication is impossible.
		<reason>: Provides a detailed reason why communication is impossible.
		This information is displayed if <status> is unreachable.
		  (interface down): Indicates that the source interface for polling is in DOWN status.
		  (no response): Indicates that there were no responses from the polling destination.
		  (no route): Indicates that there are no routes to the polling destination.

Item	Meaning	Displayed detailed information
		(invalid response): When the "track check-reply-interface" configuration command is set, responses from the interface that sent the polling request and also from another interface were received.
IPv6 Advertisement Type: <type>	Type of sending ADVERTISEMENT packets	Type of sending ADVERTISEMENT packets ietf-ipv6-spec-02-mode: Sends ADVERTISEMENT packets according to draft-ietf-vrrp-ipv6-spec-02. ietf-ipv6-spec-07-mode: Sends ADVERTISEMENT packets according to draft-ietf-vrrp-ipv6-spec-07.

Example 3

Figure 36-11: Displaying the virtual router statistics

```
> show vrrpstatus statistics interface vlan 10 vrid 3
Date 20XX/12/10 12:00:00 UTC
VLAN0010: VRID 3 VRF 2
  1 times transitions to master
  247 advertisement received
        0 with bad advertisement interval
        0 with authentication failed
        0 with bad ipv6 hoplimit
        0 with priority zero
        0 with invalid type
        0 with bad ipv6 address
        0 with bad authentication type
        0 with authentication type mismatch
        0 with packet length error
        0 with different VRRP version
        0 with low priority
  1747 advertisement sent
        0 with priority zero
  0 change by command
  0 change by interface down
  0 change by receiving advertisement with high priority
  0 change by Master_Down_Timer timeout
  0 master transition delay count
  track 10  VLAN0022 VRF 3 Target-Address : fe80::ba
    VRRP Polling round-trip min/avg/max = 0.266/0.274/0.286 ms
    1 priority down by detected
>
```

Display items in Example 3

Table 36-11: Items displayed for the virtual router statistics

Item	Meaning	Displayed detailed information
<interface name> : VRID <vrid> [VRF <vrf id>]	Name of the interface where a virtual router is running, and its VRID information	<interface name>: Indicates the name of the interface where the virtual router is running. <vrid>: Indicates the virtual router ID. VRF <vrf id>: Indicates the VRF ID. This is not displayed if the virtual router is running in a global network. [SL-L3A]
<number of packets> times transitions to master	Number of transitions to the master status	—
<number of packets> advertisement received	Number of received ADVERTISEMENT packets	—

Item	Meaning	Displayed detailed information
\<number of packets> with bad advertisement interval	Number of received ADVERTISEMENT packets that have invalid packet-sending intervals	—
\<number of packets> with authentication failed	Number of received ADVERTISEMENT packets of which authentication failed	—
\<number of packets> with bad ipv6 hoplimit	Number of received ADVERTISEMENT packets whose HopLimit for the IPv6 header was not 255	—
\<number of packets> with priority zero	Number of received ADVERTISEMENT packets whose priority is 0	—
\<number of packets> with invalid type	Number of received ADVERTISEMENT packets that had an invalid value in the type field	—
\<number of packets> with bad ipv6 address	Number of received ADVERTISEMENT packets that have invalid virtual router IPv6 addresses	—
\<number of packets> with bad authentication type	Number of received ADVERTISEMENT packets with invalid packet authentication types	—
\<number of packets> with authentication type mismatch	Number of received ADVERTISEMENT packets whose packet authentication type did not match the local setting.	—
\<number of packets> with packet length error	Number of received ADVERTISEMENT packets whose packet length was invalid	—
\<number of packets> with different VRRP version	Number of received packets whose version of ADVERTISEMENT packets and that of VRRP running mode do not match	—
\<number of packets> with low priority	Number of received ADVERTISEMENT packets with lower priority	—
\<number of packets> advertisement sent	Number of sent ADVERTISEMENT packets	—
\<number of packets> with priority zero	Number of sent ADVERTISEMENT packets whose priority is 0	—
\<N> change by command	Number of times that the "swap vrrp" command was executed	—
\<N> change by interface down	Number of status transitions due to interface down	—

Item	Meaning	Displayed detailed information
\<N> change by receiving advertisement with high priority	Number of status transitions caused by receipt of a high-priority ADVERTISEMENT packet	—
\<N> change by Master_Down_-Timer timeout	Number of status transitions because the Master Down Timer timed out	—
\<N> master transition delay count	Number of times that the suppression timer has been started	—
track \<track-number> {\<interface name> [VRF \<vrf id>]|\<interface type> \<interface number>} {Target-Address : \<target-ad­dress>|line-protocol}	VRRP polling information assigned to a virtual router	\<track-number>: Indicates the track number of the track assigned to a virtual router. \<interface name>: Indicates the name of an interface that monitors failures. VRF \<vrf id>: Indicates the VRF ID. When the destination for VRRP polling is a global network, this item is not displayed. [SL-L3A] \<interface type> \<interface number>: Indicates an interface that monitors for failures. Note that \<interface number> is displayed without \<switch no.>. • Ethernet interface • Port channel interface Target-Address : \<target-address>: Indicates the target address for VRRP polling. line-protocol: Applied to a fault monitoring interface.
VRRP Polling round-trip min/avg/max =\<minimum>/\<aver­age>/\<maximum> ms	Packet response time for VRRP polling	This item is not displayed if the IP address for VRRP polling has not been specified, or for a fault monitoring interface. \<minimum>/\<average>/\<maximum>: Indicates the minimum value, average value, and maximum value.
\<N> priority down by detected	Number of times that the priority has been decreased due to a track error	—

Impact on communication

None

Response messages

Table 36-12: List of response messages for the show vrrpstatus (IPv6) command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
no entries.	There are no applicable virtual routers.

Notes

None

clear vrrpstatus(IPv6)

Clears the counter for VRRP virtual router statistics.

Syntax

```
clear vrrpstatus [protocol ipv6] [{ name <virtual router name> | interface vlan <vlan id> [vrid
<vrid>]}]
```

Input mode

User mode and administrator mode

Parameters

protocol ipv6

    Clears the counter for IPv6-protocol virtual router statistics.

    Behavior when this parameter is omitted:

        Clears the statistics for both IPv4 and IPv6-protocol virtual routers.

{ name <virtual router name> | interface vlan <vlan id> [vrid <vrid>]}

    name <virtual router name>

        Specifies the name of a virtual router.

    interface vlan <vlan id> [vrid <vrid>]

        Specifies the interface that is used to configure the virtual router.

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

        For vrid <vrid>, specify a virtual router ID. If it is omitted, statistics about all virtual routers for the specified interface is cleared.

    Behavior when this parameter is omitted:

        Clears the statistics on virtual routers for all interfaces.

Behavior when all parameters are omitted:

    Clears the counter for all virtual router statistics.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 36-12: Clearing the counters for virtual router statistics

```
> clear vrrpstatus interface vlan 10 vrid 3
>
```

Display items

None

Impact on communication

None

Response messages

Table 36-13: List of response messages for the clear vrrpstatus (IPv6) command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
no entries.	There are no applicable virtual routers.

Notes

None

swap vrrp(IPv6)

Changes the device status when switchback is suppressed.

If the device is in the master status, it is changed to the backup status.

If the device is in the backup status, it is changed to the master status.

Syntax

```
swap vrrp [-f] { name <virtual router name> | interface vlan <vlan id> [vrid <vrid>] }
```

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.

{ name <virtual router name> | interface vlan <vlan id> [vrid <vrid>]}

 name <virtual router name>

  Specifies the name of a virtual router.

 interface vlan <vlan id> [vrid <vrid>]

  Specifies the interface that is used to configure the virtual router.

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

  For vrid <vrid>, specify a virtual router ID. If it is omitted, a confirmation message for individual virtual routers configured for the specified interface is displayed.

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows how to switch VRID "3" and VRID "40" virtual routers configured for VLAN "10", which are currently operating as the master, to the backup status.

Figure 36-13: Performing switchback for virtual routers

```
> swap vrrp interface vlan 10
Exchange VRRP 3 OK? (y/n): y
Exchange VRRP 40 OK? (y/n): y
>
```

Display items

None

Impact on communication

Communication might stop temporarily because of status transitions in VRRP.

Response messages

Table 36-14: List of response messages for the swap vrrp (IPv6) command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Command execution cannot be performed to follow virtual router.	This command cannot be executed for follower virtual routers.
Command execution cannot be performed to owner's virtual router of an initial state.	This command cannot be executed for virtual routers in initial status.
Command execution cannot be performed to owner's virtual router.	This command cannot be executed for the virtual router of the address owner.
no entries.	There are no applicable virtual routers.

Notes

- If this command is executed from a virtual router that has lower or equal priority (including the default priority), the device status might not be changed to the master status.

- This command cannot be entered for an address owner, follower virtual router, or a device in initial status.

- If a switchback command is executed while switchback is suppressed, the command is given priority and switchback is performed.

- If the command is executed when switchback is not suppressed, switchback is performed, even though that does not seem to be the case because the status of the virtual router with the higher priority is changed to the master status by the automatic switchback function.

- When the command is executed, both virtual routers are swapped to the backup or master status temporarily, but they are changed back to the master or backup status automatically.

- When switchback cannot be performed due to a failure of other devices, if the command is executed, communication is suspended for four seconds by default.

- In a configuration where the "no vrrp preempt" and the "vrrp timers non-preempt-swap" configuration commands are set for all devices that make up the VRRP, if a switchback command is executed in the master device, all devices change to the backup status until the period set for the "vrrp timers non-preempt-swap" command elapses. To avoid this situation, do not set the "vrrp timers non-preempt-swap" command for at least one of the devices that makes up the VRRP. If all the devices are in backup status, you can make one of the devices the master device by executing the "swap vrrp" command and specifying the device.

The table below lists the results of executing this command. No status change in the following table indicates situation where it does not seem that switchback is performed.

Table 36-15: List of execution results for the swap vrrp (IPv6) command

—			This device is being suppressed		This device is not suppressed	
			Another device is being suppressed	Another device is not being suppressed	Another device is being suppressed	Another device is not being suppressed
This device (Master)	Comparison of the priority between this device and another device	High	Switched	Switched	No status change	No status change
		Equal	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.
		Low	Switchback	Switchback	Switchback	Switchback
This device (Backup)		High	Switchback	Switchback	Switchback	Switchback
		Equal	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.
		Low	No status change	No status change	No status change	No status change

Terms used in the above table:

- This device: A device in which the "swap vrrp" command is executed.

- Another device: A device other than this device.

- Switched: The priority of the master device is changed from high to low.

show track(IPv4)

Displays VRRP track information.

Syntax

```
show track <track number> [detail]
show track [detail]
    {[protocol ip] [interface vlan <vlan id>]
     | [interface <interface type> <interface number>]}
```

Input mode

User mode and administrator mode

Parameters

<track number>

Specify the track number.

detail

Displays detailed statistics.

Behavior when this parameter is omitted:

A track overview is displayed.

{[protocol ip] [interface vlan <vlan id>] | [interface <interface type> <interface number>]}

protocol ip

Displays track information set for the IPv4 protocol IP interface.

interface vlan <vlan id>

Specifies a VLAN interface for which a track is configured.

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

interface <interface type> <interface number>

Specifies the interface that monitors failures.

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

• Port channel interface

Behavior when this parameter is omitted:

All track information is displayed.

Behavior when all parameters are omitted:

A list of tracks and track information are displayed.

Operation when a stack configuration is used

This command is not supported.

Example

- The following figure shows an example of displaying the list of IPv4 protocol tracks.

Figure 36-14: Displaying the IPv4 protocol track information

```
> show track protocol ip
Date 20XX/12/10 12:00:00 UTC
track : 10  interface : VLAN0022  Mode : (interface)
track : 20  interface : VLAN0031 VRF 10 Mode : (polling)
>
```

- The following figure shows an example of displaying the detailed track information.

Figure 36-15: Displaying the detailed track information

```
> show track detail interface vlan 31
Date 20XX/12/10 12:00:00 UTC
track : 20  interface : VLAN0031 VRF 10 Mode : (polling)
   Target Address : 170.10.10.10
   Assigned to :
     VLAN0010: VRID 1
     VLAN0100: VRID 100 VRF 20
>
```

Display items

Table 36-16: Information displayed by the show track (IPv4) command

Item	Meaning	Displayed detailed information

track : <track-number> interface : { <interface name> [VRF <vrf id>]|<interface type> <interface number>} Mode : <mode>	Summary information about track settings	<track-number>: Indicates the track number of the track assigned to a virtual router.
		 interface : <interface name> [VRF <vrf id>]|<interface type> <interface number>: Information about the interface for which failure monitoring is performed.
		 "(not assigned)" is displayed if the "track interface" configuration command is not set.
		 <interface name>: Indicates the interface name of the VLAN interface that monitors for failures.
		 VRF <vrf id>: Indicates the VRF ID.
		 This item is not displayed if the VLAN interface that monitors failures is a global network. [SL-L3A]
		 <interface type> <interface number>: Indicates an interface that monitors for failures.
		 • Ethernet interface
		 • Port channel interface
		 Mode : <mode>: Indicates the monitoring mode of the track.
		 This item is not displayed if the "track interface" configuration command is not set.
		   (interface): Monitors the interface status.
		   (polling): Monitors the polling status.

Target Address : <target_address>	Destination IP address for VRRP polling	This item is not displayed if it has not been set.
check_status_interval : <seconds>	Interval (in seconds) between VRRP polling attempts	This item is not displayed if it has not been set. Initial value: 6
check_trial_times : <count>	Number of attempts until the status is changed by VRRP polling	This item is not displayed if it has not been set. Initial value: 4

Item	Meaning	Displayed detailed information
failure_detection_interval : <seconds>	Interval (in seconds) between VRRP polling attempts when a failure is detected	This item is not displayed if it has not been set. Initial value: 2
failure_detection_times : <count>	Number of attempts until the status is changed when VRRP polling detects a failure	This item is not displayed if it has not been set. Initial value: 3
recovery_detection_interval : <seconds>	Interval (in seconds) between attempts when VRRP polling detects a failure	This item is not displayed if it has not been set. Initial value: 2
recovery_detection_times : <count>	Number of attempts until the status is changed when VRRP polling detects restoration	This item is not displayed if it has not been set. Initial value: 3
check_reply_interface : on	Whether to check if the interface sent by VRRP polling and the interface that received the response match	This item is not displayed if it has not been set.
Assigned to : <interface name>: VRID <vrid> [VRF <vrf id>]	List of virtual routers to which a track is assigned	This item is not displayed if no tracks are assigned to a virtual router. <interface name>: Indicates the name of an interface for which a virtual router, to which a track is assigned, is configured. <vrid>: Indicates the virtual router ID of a virtual router to which a track is assigned. VRF <vrf id>: Indicates the VRF ID. This is not displayed if the virtual router is running in a global network. [SL-L3A]

Impact on communication

None

Response messages

Table 36-17: List of response messages for the show track (IPv4) command

Message	Description
no entries.	There are no applicable tracks.

Notes

None

show track(IPv6)

Displays VRRP track information.

Syntax

```
show track <track number> [detail]
show track [detail]
    {[protocol ipv6][interface vlan <vlan id>]
     |[interface <interface type> <interface number>]}
```

Input mode

User mode and administrator mode

Parameters

<track number>

Specify the track number.

detail

Displays detailed statistics.

Behavior when this parameter is omitted:

A track overview is displayed.

{[protocol ipv6][interface vlan <vlan id>]|[interface <interface type> <interface number>]}

protocol ipv6

Displays track information set for the IPv6 protocol IP interface.

interface vlan <vlan id>

Specifies a VLAN interface for which a track is configured.

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

interface <interface type> <interface number>

Specifies the interface that monitors failures.

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
- Port channel interface

Behavior when this parameter is omitted:

All track information is displayed.

Behavior when all parameters are omitted:

A list of tracks and track information are displayed.

Operation when a stack configuration is used

This command is not supported.

Example

- The following figure shows an example of displaying the list of IPv6 protocol tracks.

Figure 36-16: Displaying the IPv6 protocol track information

```
> show track protocol ipv6
Date 20XX/12/10 12:00:00 UTC
track : 10  interface : VLAN0022  Mode : (interface)
track : 30  interface : VLAN0032 VRF 10 Mode : (polling)
>
```

- The following figure shows an example of displaying the detailed track information.

Figure 36-17: Displaying the detailed track information

```
> show track detail interface vlan 32
Date 20XX/12/10 12:00:00 UTC
track : 30  interface : VLAN0032 VRF 10 Mode : (polling)
   Target Address : 100::6789
   Assigned to :
     VLAN0010: VRID 3
     VLAN0100: VRID 200 VRF 20
>
```

Display items

Table 36-18: Information displayed by the show track (IPv6) command

Item	Meaning	Displayed detailed information
track : <track-number> interface : {<interface name> [VRF <vrf id>]|<interface type> <interface number>} Mode : <mode>	Summary information about track settings	<track-number>: Indicates the track number of the track assigned to a virtual router. interface : <interface name> [VRF <vrf id>]|<interface type> <interface number>: Information about the interface for which failure monitoring is performed. "(not assigned)" is displayed if the "track interface" configuration command is not set. <interface name>: Indicates the interface name of the VLAN interface that monitors for failures. VRF <vrf id>: Indicates the VRF ID. This item is not displayed if the VLAN interface that monitors failures is a global network. [SL-L3A] <interface type> <interface number>: Indicates an interface that monitors for failures. • Ethernet interface • Port channel interface Mode : <mode>: Indicates the monitoring mode of the track. This item is not displayed if the "track interface" configuration command is not set. (interface): Monitors the interface status. (polling): Monitors the polling status.
Target Address : <target_address>	Destination IP address for VRRP polling	This item is not displayed if it has not been set.
check_status_interval : <seconds>	Interval (in seconds) between VRRP polling attempts	This item is not displayed if it has not been set. Initial value: 6

Item	Meaning	Displayed detailed information
check_trial_times : <count>	Number of attempts un-til the status is changed by VRRP polling	This item is not displayed if it has not been set. Initial value: 4
failure_detection_interval : <sec-onds>	Interval (in seconds) be-tween VRRP polling at-tempts when a failure is detected	This item is not displayed if it has not been set. Initial value: 2
failure_detection_times : <count>	Number of attempts un-til the status is changed when VRRP polling de-tects a failure	This item is not displayed if it has not been set. Initial value: 3
recovery_detection_interval : <sec-onds>	Interval (in seconds) be-tween attempts when VRRP polling detects a failure	This item is not displayed if it has not been set. Initial value: 2
recovery_detection_times : <count>	Number of attempts un-til the status is changed when VRRP polling de-tects restoration	This item is not displayed if it has not been set. Initial value: 3
check_reply_interface : on	Whether to check if the interface sent by VRRP polling and the interface that received the re-sponse match	This item is not displayed if it has not been set.
Assigned to : <interface name>: VRID <vrid> [VRF <vrf id>]	List of virtual routers to which a track is as-signed	This item is not displayed if no tracks are as-signed to a virtual router. <interface name>: Indicates the name of an inter-face for which a virtual router, to which a track is assigned, is configured. <vrid>: Indicates the virtual router ID of a virtual router to which a track is assigned. VRF <vrf id>: Indicates the VRF ID. This is not displayed if the virtual router is running in a glob-al network. [SL-L3A]

Impact on communication

None

Response messages

Table 36-19: List of response messages for the show track (IPv6) command

Message	Description
no entries.	There are no applicable tracks.

Notes

None

37 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.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example 1

The following figure shows an example of displaying the information about the uplink redundancy function.

Figure 37-1: Example of displaying the information about the uplink redundancy function

```
> show switchport-backup
Date 20XX/04/04 16:48:07 UTC
startup active port selection: primary only
Switchport Backup pairs                      Preemption   Flush
 Primary     Status    Secondary  Status     Delay Rest   VLAN  Update  Reset
 Port 1/0/1  Forwarding Port 2/0/24 Blocking   -     -    4093     -      -
 Port 1/0/10 Down      ChGr 4      Forwarding  -     -     -       1      -
*Port 1/0/11 Down      Port 2/0/15 Blocking    -     -     10      -      -
```

```
*Port 1/0/20 Down       Port 2/0/21 Down          -    -    -    -     3s
>
```

Display items in Example 1

Table 37-1: Items displayed for the 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 pairs	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.
	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.

Example 2

The following figure shows an example of displaying the detailed information about the uplink redundancy function.

Figure 37-2: 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 pairs                          Preemption  Flush
 Primary     Status    Secondary  Status     Delay  Rest   VLAN  Update  Reset
 Port 1/0/1  Forwarding Port 2/0/24 Blocking      -     -    4093     -      -
  VLAN                        : 4051-4094
  MAC Address update Exclude-VLAN : -
  Last change factor          : primary down
  Last change time            : 20XX/04/03 16:52:21 UTC
  Last Flush Tx time          : 20XX/04/03 16:52:22 UTC
  Last MAC Address update Tx time : -
  Last port reset time        : -
Switchport Backup pairs                          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 UTC
  Last Flush Tx time          : -
  Last MAC Address update Tx time : 20XX/04/03 09:52:22 UTC
  Last port reset time        : -
Switchport Backup pairs                          Preemption  Flush
 Primary     Status    Secondary  Status     Delay  Rest   VLAN  Update  Reset
*Port 1/0/11 Down      Port 2/0/15 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 pairs                          Preemption  Flush
 Primary     Status    Secondary  Status     Delay  Rest   VLAN  Update  Reset
*Port 1/0/20 Down      Port 2/0/21 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 UTC
>
```

Display items in Example 2

Table 37-2: 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.

Item		Meaning	Displayed detailed information
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.
	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.

Item	Meaning	Displayed detailed information
Last change factor	Last factor that de-termined 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 per-formed. 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:sec-ond 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:sec-ond 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 com-mand.
Last MAC Address update Tx time	The date and time when the MAC ad-dress update frame was last sent.	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:sec-ond This item displays the last time when the MAC address up-date 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 com-mand.
Last port reset time	Date and time when port resetting was last executed	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:sec-ond 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 execut-ed. 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

Response messages

Table 37-3: List of response messages for the show switchport-backup command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Uplink Redundant program.	Communication with the uplink redundancy program failed. Re-execute the command.
No operational Port.	There are no available ports or channel groups. Make sure the specified parameter is correct, and then try again.

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.

Operation when a stack configuration is used

The command can be executed only on the master switch.

Example

The following figure shows an example of switching the standby port to the active port.

Figure 37-3: 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.

Response messages

Table 37-4: List of response messages for the set switchport-backup active command

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.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Uplink Redundant program.	Communication with the uplink redundancy program failed. Re-execute the command.
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.

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} restart uplink-redundant [-f] [core-file]
```

Example

Figure 37-4: Example of restarting uplink redundancy

```
> restart uplink-redundant
Uplink Redundant restart OK? (y/n): y
>
```

Display items

None

Impact on communication

All VLANs temporarily become unable to send or receive data.

Response messages

Table 37-5: List of response messages for the restart uplink-redundant command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Uplink Redundant program failed to be restarted.	An attempt to restart the uplink redundancy program by this command failed. Re-execute the command.

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

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} dump protocols uplink-redundant
```

Example

The following figure is an example of outputting detailed event trace information and control table information to a file.

Figure 37-5: Outputting the detailed event trace information and control table information

```
> dump protocols uplink-redundant
>
```

Display items

None

Impact on communication

None

Response messages

Table 37-6: List of response messages for the dump protocols uplink-redundant command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

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.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example

Figure 37-6: 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 2/0/24
  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 37-7: 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

Response messages

Table 37-8: List of response messages for the show switchport-backup statistics command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Uplink Redundant program.	Communication with the uplink redundancy program failed. Re-execute the command.
No operational Port.	There are no available ports or channel groups. Make sure the specified parameter is correct, and then try again.

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.

Operation when a stack configuration is used

The command can clear information only from the master switch.

Example

Figure 37-7: Example of clearing the uplink redundancy statistics

```
> clear switchport-backup statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 37-9: List of response messages for the clear switchport-backup statistics command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Uplink Redundant program.	Communication with the uplink redundancy program failed. Re-execute the command.

Notes

If a port or channel group is specified, the uplink redundancy statistics on the paired port or channel group are also cleared.

38 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.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example

The following figure shows an example of displaying L2 loop detection information.

Figure 38-1: 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:32(U)    100
  CH:1     Up          trap                0             -   -
  CH:32    Up          uplink              -             -   1/0/5       100
>
```

Display items

Table 38-1: 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

Response messages

Table 38-2: List of response messages for the show loop-detection command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Loop Detection program.	Communication with the L2 loop detection program failed. Re-execute the command.
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.

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.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example

The following figure shows an example of displaying L2 loop detection statistics.

Figure 38-2: 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:32        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 38-3: 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

Response messages

Table 38-4: List of response messages for the show loop-detection statistics command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Loop Detection program.	Communication with the L2 loop detection program failed. Re-execute the command.
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.

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

Operation when a stack configuration is used

The command can display information only for the master switch.

Example

The following figure shows an example of displaying log information about the received L2 loop detection frames.

Figure 38-3: 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:32    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:32    Source: 1/0/12   Vlan: 12    Uplink
20XX/09/05 00:00:00  CH:32    Source: 1/0/12   Vlan: 12    Uplink
>
```

Display items

Table 38-5: 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.

Item	Meaning	Displayed detailed information
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.
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

Response messages

Table 38-6: List of response messages for the show loop-detection logging command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Loop Detection program.	Communication with the L2 loop detection program failed. Re-execute the command.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the function has not been enabled. Check the configuration.

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.

Operation when a stack configuration is used

The command can clear information only from the master switch.

Example

The following figure shows an example of clearing L2 loop detection statistics.

Figure 38-4: Clearing the L2 loop detection statistics

```
> clear loop-detection statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 38-7: List of response messages for the clear loop-detection statistics command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Loop Detection program.	Communication with the L2 loop detection program failed. Re-execute the command.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the function has not been enabled. Check the configuration.

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

Operation when a stack configuration is used

The command can clear information only from the master switch.

Example

The following figure show an example of clearing the log information for received L2 loop detection frames.

Figure 38-5: Clearing the log information for received L2 loop detection frames

```
> clear loop-detection logging
>
```

Display items

None

Impact on communication

None

Response messages

Table 38-8: List of response messages for the clear loop-detection logging command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Loop Detection program.	Communication with the L2 loop detection program failed. Re-execute the command.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the function has not been enabled. Check the configuration.

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} restart loop-detection [-f] [core-file]
```

Example

The following figure shows an example of restarting the L2 loop detection program.

Figure 38-6: 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

Response messages

Table 38-9: List of response messages for the restart loop-detection command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
L2 Loop Detection doesn't seem to be running.	The L2 loop detection program has not been started. Check the configuration.

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

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} dump protocols loop-detection
```

Example

The following figure is an example of outputting detailed event trace information and control table information to a file.

Figure 38-7: Outputting the detailed event trace information and control table information

```
> dump protocols loop-detection
>
```

Display items

None

Impact on communication

None

Response messages

Table 38-10: List of response messages for the dump protocols loop-detection command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

Message	Description
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the function has not been enabled. Check the configuration.

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.

39 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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} show sflow [detail]
```

Example

Figure 39-1: Displaying the setting status and behavior status of sFlow statistics

```
> show sflow
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
```

Figure 39-2: 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 39-1: 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.[1] 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[2]
Configured sFlow egress ports	Ports for which "sflow forward egress" is set in the configuration and on which sFlow statistics are collected[2]
Received sFlow samples	Total number of packets which were sampled correctly[3]
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.[3] (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[3]

Item	Displayed information
Couldn't export sFlow samples	Total number of sample packets contained in UDP packets that could not be sent[#3]
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.[#4] 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[#3]
Send failed packets	Number of UDP packets that could not be sent to the collector[#3]
Send CounterSample UDP packets	Number of UDP packets for counter samples sent to the collector[#3]
Max packet size	Maximum sFlow packet size
Packet information type	Basic data format for flow samples
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.[#4] 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

#1

In the stack configuration:

- The backup switch displays 0:00:00.
- When the backup switch is switched over to the master switch, the elapsed time after the switching is displayed.

#2

If no configured port exists, ---- is displayed.

#3

In the stack configuration:

- All packets are counted on the master switch. The backup switch displays 0.

- When the backup switch is switched over to the master switch, the count starts from 0.

#4

The information about the specified member switch is displayed.

Impact on communication

None

Response messages

Table 39-2: List of response messages for the show sflow command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} clear sflow statistics
```

Example

```
>clear sflow statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 39-3: List of response messages for the clear sflow statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} restart sflow [-f] [core-file]
```

Example

```
>restart sflow
sflow program restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Response messages

Table 39-4: List of response messages for the restart sflow command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

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.

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

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} dump sflow
```

Example

```
>dump sflow
>
```

Display items

None

Impact on communication

None

Response messages

Table 39-5: List of response messages for the dump sflow command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

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.

40 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 ports 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.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example 1

The following figure shows an example of displaying brief information related to the IEEE 802.3ah/OAM configuration.

Figure 40-1: Displaying the brief IEEE 802.3ah/OAM configuration information

```
> show efmoam
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
1/0/4     Down(uni-link)   detection       unknown
>
```

Display items in Example 1

Table 40-1: Items displayed for the brief 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. 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.
Dest MAC	MAC address of the port on the partner device	"unknown" is displayed if no information has been received from the partner device. If a bidirectional link is confirmed, "*" is displayed on the left of the MAC address.

Example 2

The following figure shows an example of displaying detailed information related to the IEEE 802.3ah/OAM configuration by specifying the detail parameter.

Figure 40-2: 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 in Example 2

Table 40-2: 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. Disabled: Indicates that the IEEE 802.3ah/OAM function is disabled.

Item	Meaning	Displayed detailed information
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

Response messages

Table 40-3: List of response messages for the show efmoam command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
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.
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.

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.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example

The following figure shows an example of displaying statistics for all configured IEEE 802.3ah/OAM ports.

Figure 40-3: 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 40-4: 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. 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

Item	Meaning	Displayed detailed information
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

Response messages

Table 40-5: List of response messages for the show efmoam statistics command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
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.
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.

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.

Operation when a stack configuration is used

The command can clear information only from the master switch.

Example

Figure 40-4: Clearing the IEEE 802.3ah/OAM statistics

```
> clear efmoam statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 40-6: List of response messages for the clear efmoam statistics command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.

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.
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.

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.

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} restart efmoam [-f] [core-file]
```

Example

Figure 40-5: 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

Response messages

Table 40-7: List of response messages for the restart efmoam command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

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, if this command is executed after the master switch substitutes for the backup switch when a stack is configured or when the statuses of multiple VLANs are 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

Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the "remote command" command.

```
remote command {<switch no.> | all} dump protocols efmoam
```

Example

Figure 40-6: Taking a dump for IEEE 802.3ah/OAM

```
> dump protocols efmoam
>
```

Display items

None

Impact on communication

None

Response messages

Table 40-8: List of response messages for the dump protocols efmoam command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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 IEEE 802.3ah/OAM.
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.

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.

41 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.

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of executing the "l2ping" command.

Figure 41-1: 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 41-1: 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.

Item	Meaning	Displayed detailed information
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
Lost Frame	Percentage of lost frames (%)	—
Round-trip Min/Avg/Max	Minimum, average, and maximum response times	—

Impact on communication

None

Response messages

Table 41-2: List of response messages for the l2ping command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
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.

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.

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of executing the "l2traceroute" command.

Figure 41-2: 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 41-3: 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

Response messages

Table 41-4: List of response messages for the l2traceroute command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
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.
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.

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.

Operation when a stack configuration is used

This command is not supported.

Example 1

The following figure shows an example of displaying the CFM configuration information.

Figure 41-3: 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
      CH12(Up)    Enable   MAC:0012.e220.00b2
>
```

Display items in Example 1

Table 41-5: 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.

Item	Meaning	Displayed detailed information
		• 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.
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.

Item	Meaning	Displayed detailed information
		"-" 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.
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 41-4: 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 41-6: 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

Response messages

Table 41-7: List of response messages for the show cfm command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
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 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.

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>] [detail]
```

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.

Operation when a stack configuration is used

This command is not supported.

Example 1

The following figure shows an example of displaying remote MEP information.

Figure 41-5: Example of displaying the remote MEP information

```
>show cfm remote-mep
Date 20XX/03/20 18:05:12 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
        ID:15    Status:-           MAC:0012.e200.005a  Time:20XX/03/20 18:04:54
   MA 200   Name(str) : Tokyo_to_Nagoya
     MEP ID:8012  CH1 (Up)    Enable   Status:-
        RMEP Information  Counts:  2
        ID:8003  Status:-           MAC:0012.e20a.1241  Time:20XX/03/20 12:12:20
        ID:8004  Status:-           MAC:0012.e20d.12a1  Time:20XX/03/20 12:12:15
  >
```

Display items in Example 1

Table 41-8: Items displayed for the 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.

Item	Meaning	Displayed detailed information
		• RDI: Indicates a CCM reporting failure detection was received. "-" is displayed if no failure has been detected.
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

Example 2

The following figure shows an example of displaying detailed remote MEP information.

Figure 41-6: 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 in Example 2

Table 41-9: Items displayed for the detailed remote MEP information

Item	Meaning	Displayed detailed information
Total RMEP Counts	Total number of remote MEPs	—

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.
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.
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.

Item	Meaning	Displayed detailed information
		• 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. • 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.

Item	Meaning	Displayed detailed information
		• 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

Response messages

Table 41-10: List of response messages for the show cfm remote-mep command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
No such Remote MEP.	The specified remote MEP is unknown. Make sure the specified parameter is correct, and then try again.
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 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.

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.

Operation when a stack configuration is used

This command is not supported.

Example 1

The following figure shows an example of displaying summary information about CFM failures.

Figure 41-7: 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 41-11: 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 41-8: 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 41-12: 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.	—

Item	Meaning	Displayed detailed information
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. -: 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

Response messages

Table 41-13: List of response messages for the show cfm fault command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

Message	Description
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 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.

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.

Operation when a stack configuration is used

This command is not supported.

Example 1

The following figure shows an example of displaying route information in the linktrace database.

Figure 41-9: Example of displaying the linktrace database information

```
> show cfm l2traceroute-db
Date 20XX/03/15 10:05:30 UTC
L2traceroute to MP:0012.e220.00a3 on Level:7  MA:1000  MEP:1020  VLAN:1000
Time:20XX/03/14 17:42:20
254  0012.e220.00c0  Forwarded
253  0012.e210.000d  Forwarded
252  0012.e220.00a3  NotForwarded  Hit

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
62   0012.e220.10c8  NotForwarded
>
```

Display items in Example 1

Table 41-14: Items displayed for the 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.

Example 2

The following figure shows an example of displaying detailed linktrace database information.

Figure 41-10: 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 in Example 2

Table 41-15: 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.
Chassis ID	Chassis ID of the replying MP	The chassis ID of the MP that sent a linktrace reply.

Item	Meaning	Displayed detailed information
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.

Item	Meaning	Displayed detailed information
		• NoVLAN: Indicates that there is no VLAN setting for linktrace messages. "-" is displayed if this information is not found in the received linktrace reply.

Impact on communication

None

Response messages

Table 41-16: List of response messages for the show cfm l2traceroute-db command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

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.

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of displaying CFM statistics.

Figure 41-11: 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 41-17: 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.

Item		Meaning	Displayed detailed information
	Rx	Number of linktrace messages that have been received	—
	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

Response messages

Table 41-18: List of response messages for the show cfm statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

Message	Description
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 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.

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.

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of clearing remote MEP information.

Figure 41-12: Example of clearing the remote MEP information

```
> clear cfm remote-mep
>
```

Display items

None

Impact on communication

None

Response messages

Table 41-19: List of response messages for the clear cfm remote-mep command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

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.

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of clearing CFM failure information.

Figure 41-13: Example of clearing the CFM failure information

```
> clear cfm fault
>
```

Display items

None

Impact on communication

None

Response messages

Table 41-20: List of response messages for the clear cfm fault command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

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

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of clearing CFM linktrace database information.

Figure 41-14: Example of clearing the CFM linktrace database information

```
> clear cfm l2traceroute-db
>
```

Display items

None

Impact on communication

None

Response messages

Table 41-21: List of response messages for the clear cfm l2traceroute-db command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

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.

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of clearing CFM statistics.

Figure 41-15: Example of clearing the CFM statistics

```
> clear cfm statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 41-22: List of response messages for the clear cfm statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

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.

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of restarting the CFM program.

Figure 41-16: Example of restarting the CFM program

```
> restart cfm
CFM program restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Response messages

Table 41-23: List of response messages for the restart cfm command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
CFM doesn't seem to be running.	The CFM program is not running. Check the configuration.

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

Operation when a stack configuration is used

This command is not supported.

Example

The following figure shows an example of taking a dump of the CFM program.

Figure 41-17: Example of taking a dump of the CFM program

```
> dump protocols cfm
>
```

Display items

None

Impact on communication

None

Response messages

Table 41-24: List of response messages for the dump protocols cfm command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.

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.

42 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.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example 1

The following figure shows an example of displaying the LLDP configuration information in a simplified format.

Figure 42-1: 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:10)  Link: Up     Neighbor Counts:    2
1/0/2            Link: Down    Neighbor Counts:    0
2/0/3            Link: Down    Neighbor Counts:    0
>
```

Display items in Example 1

Table 42-1: 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.
Chassis ID	Chassis ID of the Switch	—
Type	Subtype 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 42-2: 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 AX3660S AX-3660-24T4XW [AX3660S-24T4XW] Switching software Ver.12.1
.G [OS-L3M]
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:10)
  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  2/0/3
  Link: Up      PortEnabled: TRUE     AdminStatus: enabledRxTx
  Std Neighbor Counts:  0    Draft Neighbor Counts:   1
  Port ID: Type=MAC          Info=0012.e298.5cc1
  Port Description: GigabitEther 0/2
  Tag ID: Tagged=1,10-20,4094
  IPv4 Address: Tagged: 10      192.168.248.240
  IPv6 Address: Tagged: 20      2001:db8:811:ff01:200:8798:5cc0:e7f4
  Draft Neighbor 1     TTL: 100
    Chassis ID: Type=MAC          Info=0012.e268.2c21
    System Name: LLDP3
    System Description: ALAXALA AX6300S AX-6300-S08 [AX6308S] Switching software Ver. 11.9 [OS-
SE]
    Port ID: Type=MAC          Info=0012.e298.5cc4
    Port Description: GigabitEther 1/5
    Tag ID: Tagged=1,10-20,4094
    IPv4 Address: Tagged: 10      192.168.248.244
    IPv6 Address: Tagged: 20      2001:db8:811:ff01:200:8798:5cc0:e7f8
>
```

Display items in Example 2

Table 42-2: 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	Subtype 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

Item	Meaning	Displayed detailed information
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.
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.

Item	Meaning	Displayed detailed information
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	Subtype 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)# GigabitEther: Indicates a 1 Gbit/s or slower Ethernet. TenGigabitEther: Indicates a 10 Gbit/s Ethernet. FortyGigabitEther: Indicates a 40 Gbit/s Ethernet. HundredGigabitEther: Indicates a 100 Gbit/s Ethernet.

When running on IEEE Std 802.1AB

Item	Meaning	Displayed detailed information
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.#
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

Item	Meaning	Displayed detailed information
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.#

Item	Meaning	Displayed detailed information
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 42-3: 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	Subtype 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.
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	Subtype 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.

Item	Meaning	Displayed detailed information
		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 subtype
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.
Protocol VLAN ID	Port and Protocol VLAN ID of the neighboring device	This item is not displayed if it has not been reported.

Item	Meaning	Displayed detailed information
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.

When a switchover of the master switch occurs, the information on the neighboring device is cleared.

Table 42-4: 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	Subtype 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	Subtype 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.

Item	Meaning	Displayed detailed information
		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 subtype
Port Description	Port description of the neighboring device	This item is not displayed if it has not been reported.
Tag ID	List of VLAN IDs to which the neighboring device port belongs	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.

When a switchover of the master switch occurs, the information on the neighboring device is cleared.

Impact on communication

None

Response messages

Table 42-5: List of response messages for the show lldp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
LLDP is not configured.	LLDP has not been configured. Check the configuration.

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.

Operation when a stack configuration is used

The command can display information only for the master switch.

Example

Figure 42-3: 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
2/0/3     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 42-6: 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

Item	Meaning	Displayed detailed information
Statistics on IEEE Std 802.1AB		
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	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	—

Note that when a switchover of the master switch occurs, the statistics are cleared.

Impact on communication

None

Response messages

Table 42-7: List of response messages for the show lldp statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
LLDP is not configured.	LLDP has not been configured. Check the configuration.

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.

Operation when a stack configuration is used

The command can clear information only from the master switch.

Example

Figure 42-4: Example of executing the clear lldp command

```
> clear lldp
>
```

Display items

None

Impact on communication

None

Response messages

Table 42-8: List of response messages for the clear lldp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
LLDP is not configured.	LLDP has not been configured. Check the configuration.

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.

Operation when a stack configuration is used

The command can clear information only from the master switch.

Example

Figure 42-5: Example of executing the clear lldp statistics command

```
> clear lldp statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 42-9: List of response messages for the clear lldp statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
LLDP is not configured.	LLDP has not been configured. Check the configuration.

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.

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} restart lldp [-f] [core-file]
```

Example

Figure 42-6: Example of restarting LLDP

```
> restart lldp
LLDP restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Response messages

Table 42-10: List of response messages for the restart lldp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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

Operation when a stack configuration is used

Execute the command on all member switches that belong to the stack on the master switch.

You can also use the "remote command" command.

```
remote command {<switch no.> | all} dump protocols lldp
```

Example

Figure 42-7: Example of taking an LLDP dump

```
> dump protocols lldp
>
```

Display items

None

Impact on communication

None

Response messages

Table 42-11: List of response messages for the dump protocols lldp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to LLDP program.	Communication with the LLDP program failed. Re-execute the command. If the failure occurs frequently, use the "re-start 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 is not configured.	LLDP has not been configured. Check the configuration.

Message	Description
Switch <switch no.> was deleted from stack.	The member switch was deleted from the stack configuration. <switch no.>: Switch number

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.

43 OADP

show oadp

Shows OADP/CDP configuration information and neighboring device information.

Syntax

```
show oadp [port <port list>] [channel-group-number <channel group list>] [device-id <device id>
] [detail]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Displays neighboring device information for the specified port.

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.>.

Behavior when this parameter is omitted:

The neighboring device information for all ports is displayed.

channel-group-number <channel group list>

Displays neighboring device information 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:

The neighboring device information for all channel groups is displayed.

device-id <device id>

Displays neighboring device information for the specified device ID.

Behavior when this parameter is omitted:

All neighboring device information is displayed.

detail

Displays the OADP/CDP configuration information for the Switch and the neighboring device information in detail.

Behavior when this parameter is omitted:

The OADP/CDP configuration information for the Switch and the neighboring device information are displayed in a simplified format.

Behavior when all parameters are omitted:

The OADP/CDP configuration information for the Switch and all neighboring device information are displayed in a simplified format.

Operation when a stack configuration is used

This command is not supported.

Example 1

The following figure shows an example of displaying OADP/CDP configuration information in a simplified format.

Figure 43-1: Example of displaying the OADP configuration information and neighboring device information in a simplified format

```
> show oadp
Date 20XX/11/09 19:50:20 UTC
OADP/CDP status: Enabled/Disabled   Device ID: OADP-1
Interval Time: 60   Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 0/1-5,16,20
              CH 10

Total Neighbor Counts=2
Local     VID Holdtime Remote   VID Device ID        Capability Platform
0/1        0        35 0/8        0 OADP-2           RS         AX3640S-24T2XW
0/16       0         9 0/1        0 OADP-3           S          AX2430S-48T

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
>

> show oadp port 0/1
Date 20XX/11/09 19:50:30 UTC
OADP/CDP status: Enabled/Disabled   Device ID: OADP-1
Interval Time: 60   Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 0/1-5,16,20
              CH 10

Total Neighbor Counts=1
Local     VID Holdtime Remote   VID Device ID        Capability Platform
0/1        0        35 0/8        0 OADP-2           RS         AX3640S-24T2XW

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
>

> show oadp device-id OADP-3
Date 20XX/11/09 19:50:40 UTC
OADP/CDP status: Enabled/Disabled   Device ID: OADP-1
Interval Time: 60   Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 0/1-5,16,20
              CH 10

Total Neighbor Counts=1
Local     VID Holdtime Remote   VID Device ID        Capability Platform
0/16       0         9 0/1        0 OADP-3           S          AX2430S-48T

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
>
```

Display items in Example 1

Table 43-1: Items displayed for the OADP configuration information and neighboring device information in a simplified format

Item	Meaning	Displayed detailed information
OADP/CDP status	Status of the OADP/CDP function of the Switch	Enabled: The OADP/CDP function is enabled. Disabled: The OADP/CDP function is disabled. Paused: The OADP transmission/CDP reception function is being paused.
Interval Time	Sending interval for OADP frames that has been set on the Switch (in seconds)	5 to 254
Hold Time	OADP frame retention time to be reported to neighboring devices (in seconds)	10 to 255

Item	Meaning	Displayed detailed information
ignore vlan	VLANs that ignore OADP PDUs	VLAN ID list
Enabled Port	Information about ports where the OADP function is enabled on the Switch	<NIF number>/<port number>, <channel group number>
Total Neighbor Counts	Number of items of information on neighboring devices that is retained by the Switch	0 to 100
Local	Port number of the port on which frames are received	<NIF number>/<port number>, <channel group number>
VID	VLAN ID of the IEEE 802.1Q VLAN Tag attached to the receive frame	VLAN ID
Holdtime	Remaining retention time for neighboring device information (in seconds)	OADP: 0 to 255 CDP: Time set for a Cisco device on the sending side
Remote	Port number of the port from which a neighboring device sent frames	<NIF number>/<port number>, <channel group number>
VID	VLAN ID set for the VLAN ID TLV sent from a neighboring device	VLAN ID
Device ID	Device ID of the neighboring device	Device identifier
Capability	Functions of neighboring devices	R: Indicates a router. T: Indicates a transparent bridge. B: Indicates a source-route bridge. S: Indicates a switch. H: Indicates a host. I: Indicates that no IGMP reports are sent. r: Indicates a repeater.
Platform	Name of the neighboring device	Device name

Example 2

The following figure shows an example of displaying OADP information when the detail parameter is specified.

Figure 43-2: Example of displaying the detailed OADP configuration and neighboring device information

```
> show oadp detail
Date 20XX/11/09 19:55:52 UTC
OADP/CDP status: Enabled/Disabled    Device ID: OADP-1
Interval Time: 60   Hold Time: 180
ignore vlan: 2-4,10                                                   1
Enabled Port: 0/1-5,16,20

Total Neighbor Counts=2
--------------------------------------------------------
Port: 0/1      VLAN ID: 0                                            2
Holdtime     : 6(sec)
Port ID      : 0/8  VLAN ID(TLV): 0
Device ID    : OADP-2
Capabilities : Router,Switch
Platform     : AX3640S-48T2XW
Entry address(es):                                                   3
    IP address  : 192.16.170.87
    IPv6 address: fe80::200:4cff:fe71:5d1c
IfSpeed      : 1G   Duplex    : FULL
```

```
Version      : ALAXALA AX3640S AX-3640-48T2XWE-ZX [AX3640S-48T2XW] ┐
Switching software Ver. 11.6 [OS-L3A]                               ┘1

-----------------------------------------------------
Port: 0/16    VLAN ID: 0                                           ┐2
Holdtime    : 10(sec)                                              ┘
Port ID     : 0/1  VLAN ID(TLV): 0                                 ┐
Device ID   : OADP-3                                               │
Capabilities : Switch                                              │
Platform    : AX2430S-48T                                          │
Entry address(es):                                                 │3
    IP address  : 192.16.170.100                                   │
IfSpeed     : 1G   Duplex    : FULL                                │
Version      : ALAXALA AX2430S AX-2430S-48T [AX2430S-48T] Swit     │
ching software Ver. 11.6 [OS-L2]                                   ┘
-----------------------------------------------------
>
```

1. Configuration information of the Switch

2. Information about the Switch's port

3. Information about neighboring devices

Display items in Example 2

Table 43-2: Items displayed for the detailed OADP configuration information and neighboring device information

Item	Meaning	Displayed detailed information
OADP/CDP status	Status of the OADP/CDP function of the Switch	Enabled: The OADP/CDP function in enabled. Disabled: The OADP/CDP function is disabled. Paused: The OADP transmission/CDP reception function is being paused.
Interval Time	Sending interval for OADP frames that has been set on the Switch (in seconds)	5 to 254
Hold Time	OADP frame retention time to be reported to neighboring devices (in seconds)	10 to 255
ignore vlan	VLANs that ignore OADP PDUs	VLAN ID list
Enabled Port	Information about ports where the OADP function is enabled on the Switch	<NIF number>/<port number>, <channel group number>
Total Neighbor Counts	Number of items of information on neighboring devices that is retained by the Switch	0 to 100
Port	Port number of the port on which frames are received	<NIF number>/<port number>, <channel group number>
VLAN ID	VLAN ID of the IEEE 802.1Q VLAN Tag attached to the receive frame	VLAN ID
Holdtime	Remaining retention time for neighboring device information (in seconds)	OADP: 0 to 255 CDP: Time set for a Cisco device on the sending side
Port ID	Port number of the port from which a neighboring device sent frames	<NIF number>/<port number>, <channel group number>

Item	Meaning	Displayed detailed information
VLAN ID(TLV)	VLAN ID set for the VLAN ID TLV sent from a neighboring device	VLAN ID
Device ID	Device ID of the neighboring device	Device identifier
Capability	Functions of neighboring devices	Functions
Platform	Name of the neighboring device	Device name
Entry address	Addresses related to ports from which neighboring devices sent frames	IPv4 address, IPv6 address
ifSpeed	Line speed of a port from which a neighboring device sent frames	Example: 10M: 10Mbit/s, 1G: 1Gbit/s
Duplex	Duplex information for a port from which a neighboring device sent frames	FULL
Version	Version information about neighboring devices	Version information

Impact on communication

None

Response messages

Table 43-3: List of response messages for the show oadp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to OADP.	Communication with the OADP program failed. Re-execute the command. If the failure occurs frequently, use the "restart oadp" command to restart the OADP program.
OADP is not configured.	OADP has not been configured. Check the configuration.

Notes

None

show oadp statistics

Shows OADP/CDP statistics.

Syntax

```
show oadp statistics [port <port list>] [channel-group-number <channel group list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Displays OADP 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". Note that you specify <port list> without <switch no.>.

Behavior when this parameter is omitted:

OADP statistics for all ports are displayed.

channel-group-number <channel group list>

Displays OADP statistics for the specified channel group numbers in list format.

For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

OADP statistics for all channel group numbers are displayed.

Behavior when all parameters are omitted:

Statistics for all OADP/CDP frames are displayed by port.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 43-3: Example of displaying the OADP/CDP statistics

```
> show oadp statistics
Date 20XX/11/09 23:12:23 UTC
Port Counts: 3
Port 0/6   OADP PDUs  : Tx  =          9 OADP/CDP PDUs   : Rx    =        14
           RX PDUs    : OADP=          6 CDPv1 =         0 CDPv2  =         8
           Discard/ERR: Head=          0 cksum =         0 capacity=        0
Port 0/7   OADP PDUs  : Tx  =         10 OADP/CDP PDUs   : Rx    =        18
           RX PDUs    : OADP=          9 CDPv1 =         0 CDPv2  =         9
           Discard/ERR: Head=          0 cksum =         0 capacity=        0
Port 0/8   OADP PDUs  : Tx  =          0 OADP/CDP PDUs   : Rx    =         0
           RX PDUs    : OADP=          0 CDPv1 =         0 CDPv2  =         0
           Discard/ERR: Head=          0 cksum =         0 capacity=        0
>
```

Display items

Table 43-4: Items displayed for the OADP/CDP statistics

Item	Meaning	Displayed detailed information
Port counts	Number of ports subject to this statistics	—
Port	Port number	NIF number/port number of the port whose information is to be displayed
OADP PDUs Tx	Number of sent OADP PDUs	0 to 4294967295
OADP/CDP PDUs Rx	Number of received OADP/CDP PDUs	0 to 4294967295
Rx PDUs	Statistics for receive frames	—
OADP	Number of OADP PDUs	0 to 4294967295
CDPv1	Number of CDP version 1 PDUs	0 to 4294967295
CDPv2	Number of CDP version 2 PDUs	0 to 4294967295
Discard/ERR	Statistics for error frames	—
Head	Number of header error PDUs	0 to 4294967295
cksum	Number of checksum error PDUs	0 to 4294967295
capacity	Number of PDUs exceeding the accommodation limit	0 to 4294967295

Impact on communication

None

Response messages

Table 43-5: List of response messages for the show oadp statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to OADP.	Communication with the OADP program failed. Re-execute the command. If the failure occurs frequently, use the "restart oadp" command to restart the OADP program.
OADP is not configured.	OADP has not been configured. Check the configuration.

Notes

None

clear oadp

Clears OADP neighboring device information.

Syntax

```
clear oadp [port <port list>] [channel-group-number <channel group 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". Note that you specify <port list> without <switch no.>.
>
> Behavior when this parameter is omitted:
>
> > Clears neighboring device information for all ports.

channel-group-number <channel group list>

> Clears neighboring device information for the specified channel group number in list format.
>
> For details about how to specify <channel group list>, see "Specifiable values for parameters".
>
> Behavior when this parameter is omitted:
>
> > The neighboring device information for all channel group numbers is cleared.

Behavior when all parameters are omitted:

> Information about all neighboring devices retained on the Switch is cleared.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 43-4: Example of executing the clear oadp command

```
> clear oadp
>
```

Display items

None

Impact on communication

None

Response messages

Table 43-6: List of response messages for the clear oadp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to OADP.	Communication with the OADP program failed. Re-execute the command. If the failure occurs frequently, use the "restart oadp" command to restart the OADP program.
OADP is not configured.	OADP has not been configured. Check the configuration.

Notes

None

clear oadp statistics

Clears OADP/CDP statistics.

Syntax

```
clear oadp statistics [port <port list>] [channel-group-number <channel group list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Clears OADP/CDP statistics for the specified port.

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.>.

Behavior when this parameter is omitted:

OADP/CDP statistics for all ports are cleared.

channel-group-number <channel group list>

Clears OADP/CDP statistics for the specified channel group numbers in list format.

For details about how to specify <channel group list>, see "Specifiable values for parameters".

Behavior when this parameter is omitted:

OADP/CDP statistics for all channel group numbers are cleared.

Behavior when all parameters are omitted:

All OADP/CDP statistics for the Switch are cleared.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 43-5: Example of executing the clear oadp statistics command

```
> clear oadp statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 43-7: List of response messages for the clear oadp statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to OADP.	Communication with the OADP program failed. Re-execute the command. If the failure occurs frequently, use the "restart oadp" command to restart the OADP program.
OADP is not configured.	OADP has not been configured. Check the configuration.

Notes

None

restart oadp

Restarts the OADP program.

Syntax

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

Input mode

User mode and administrator mode

Parameters

-f

Restarts the OADP 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 OADP program is restarted.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 43-6: Example of restarting OADP

```
> restart oadp
OADP restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Response messages

Table 43-8: List of response messages for the restart oadp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
OADP doesn't seem to be running.	This command failed because the OADP program is not started. Wait until the OADP program restarts, and then re-execute the command.

Notes

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

Storage directory: /usr/var/core/

Core file: oadpd.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 oadp

Dumps detailed event trace information and control table information collected by the OADP program to a file.

Syntax

```
dump protocols oadp
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

This command is not supported.

Example

Figure 43-7: Example of taking an OADP dump

```
> dump protocols oadp
>
```

Display items

None

Impact on communication

None

Response messages

Table 43-9: List of response messages for the dump protocols oadp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to OADP.	Communication with the OADP program failed. Re-execute the command. If the failure occurs frequently, use the "restart oadp" command to restart the OADP program.
File open error.	An attempt to open or access a dump file failed. Re-execute the command later.
OADP is not configured.	OADP has not been configured. Check the configuration.

Notes

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

    Storage directory: /usr/var/oadp/

    File: oadpd_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 PTP

show ptp

Displays the PTP information and the status of ports.

Syntax

```
show ptp [port <port list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

>Displays PTP information for the specified port. For details about how to specify <port list> and the specifiable range of values, see the topic about a command applicable to a stack configuration in "Specifiable values for parameters".

>Behavior when this parameter is omitted:

>>The PTP information for all ports is displayed.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 44-1: Displaying the PTP information

```
> show ptp
Date 20XX/09/01 12:00:00 UTC
Clock types: E2E-TC
PTP profile information
  Profile name: AlaxalA PTP profile for AX3660S
  Profile version: 1.0
  Profile identifier: 0012.e200.0100
Clock description
  Manufacturer identity: 00-12-E2
  Product description: AlaxalA xxxxxxxxxxxxxxxx
  Revision data: 1.0;1.0;1.0
  User description: E2E-TC NODE 101
  Profile identity: 0012.e200.0100
Transport mechanism protocol: IPv4
Source interface: VLAN 1000 (100.100.100.1)
Primary domain: 0
Port counts: 4
  Port     Port Identity
  1/0/1    0012.e2ff.fe00.0100:100
  1/0/2    0012.e2ff.fe00.0100:101
  1/0/10   0012.e2ff.fe00.0100:109
  1/0/20   0012.e2ff.fe00.0100:119
>
```

Display items

Table 44-1: Display items for the PTP information

Item	Meaning	Displayed detailed information
Clock types	PTP communication function	E2E-TC: End-to-end transparent clock
PTP profile information	PTP profile information	—
Profile name	Profile name	—
Profile version	Profile version	—
Profile identifier	Profile ID	—
Clock description	Clock Description information	—
Manufacturer identity	Manufacturer Identity information	—
Product description	Product Description information	—
Revision data	PTP revision information	Product version Hardware version Software version
User description	Supplementary explanation on PTP	"-" is displayed when the "ptp description" configuration command is not set.
Profile identity	Profile ID	—
Transport mechanism protocol	Transfer mode	IPv4: Transport mode IPv4
Source interface	Source interface	Source VLAN The IP address set for the applicable VLAN is displayed in parentheses. "-" is displayed when the source interface is not set in the configuration.
Primary domain	Primary domain	0
Port counts	Number of ports	These items are applicable to ports where the "ptp enable" configuration command is set.
Port	Port number	
Port Identity	Port ID	—

Impact on communication

None

Response messages

Table 44-2: List of response messages for the show ptp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to PTP program.	Communication with the PTP program failed. Re-execute the command. If the failure occurs frequently, use the "restart ptp" command to restart the PTP program.
No operational Port.	There is no port on which this command can be executed. Make sure the specified parameter is correct, and then try again.
PTP is not configured.	PTP has not been configured. Check the configuration.

Notes

None

restart ptp

Restarts the PTP program.

Syntax

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

Input mode

User mode and administrator mode

Parameters

-f

Restarts the PTP program without displaying a confirmation message.

Behavior when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the PTP program's core files when the PTP program is restarted.

Behavior when this parameter is omitted:

A core file is not output.

Behavior when all parameters are omitted:

After the confirmation message is output, the PTP program is restarted.

Operation when a stack configuration is used

This command is not supported.

Example

Figure 44-2: Example of restarting the PTP program

```
> restart ptp
PTP program restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Response messages

Table 44-3: List of response messages for the restart ptp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
PTP doesn't seem to be running.	The PTP program is not running. Check the configuration.

Notes

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

   - Storage directory: /usr/var/core/
   - Core file: ptpd.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 ptp

Dumps detailed event trace information and control table information collected by the PTP program to a file.

Syntax

```
dump protocols ptp
```

Input mode

User mode and administrator mode

Parameters

None

Operation when a stack configuration is used

This command is not supported.

Example

Figure 44-3: Example of taking a PTP dump

```
> dump protocols ptp
>
```

Display items

None

Impact on communication

None

Response messages

Table 44-4: List of response messages for the dump protocols ptp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to PTP program.	Communication with the PTP program failed. Re-execute the command. If the failure occurs frequently, use the "restart ptp" command to restart the PTP program.
PTP is not configured.	PTP has not been configured. Check the configuration.

Notes

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

   • Storage directory: /usr/var/ptp/
   • File: ptpd_dump.tgz

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

Appendix

A. List of operation commands that support the remote command command

When a stack configuration is used, you can execute the "remote command" command to execute an operation command for a member switch that was specified from the master switch. The following table lists the operation commands that support the "remote command" command.

Table A-1: Operation commands that support the remote command command

Chapter	Operation command
Configurations and File Operations	ls, dir, cat, cp, mkdir, mv, rm, rmdir, delete, undelete, squeeze
Stack	show switch, dump stack
Management Port	inactivate mgmt 0, activate mgmt 0
Login Security and RADIUS/TACACS+	show sessions (who), killuser
SSH	show ssh logging, clear ssh logging
Time Settings and NTP	show clock, restart ntp
Utilities	diff, grep, tail, hexdump
Device Management	show version, show system, clear control-counter, show environment, reload, show tech-support, backup, restore
Checking Internal Memory and Memory Cards	show mc, format mc, show flash
Resource Information	show cpu, show processes, show memory, df, du
Dump Information	erase dumpfile, show dumpfile
Software Management	ppupdate, set license, show license, erase license
Power Saving Functions	show power, clear power
Log	show logging, clear logging, show logging console, set logging console
Advanced Script	pyflakes, show script installed-file, show event manager history, clear event manager, restart script-manager, restart event-manager, dump script-user-program, dump script-manager, dump event-manager
Ethernet	show interfaces, clear counters, show port, activate, inactivate
Link Aggregation	show channel-group statistics, restart link-aggregation, dump protocols link-aggregation
MAC Address Table	show mac-address-table
VLAN	restart vlan, dump protocols vlan
VXLAN	show vxlan mac-address-table, show vxlan statistics, clear vxlan statistics, restart overlay, dump protocols overlay
Spanning Tree Protocols	restart spanning-tree, dump protocols spanning-tree
Ring Protocol	restart axrp, dump protocols axrp

Chapter	Operation command
IGMP/MLD snooping	restart snooping, dump protocols snooping
Filters	show access-filter, clear access-filter
QoS	show qos-flow, clear qos-flow, show qos queueing, clear qos queueing
GSRP	restart gsrp, dump protocols gsrp
Uplink Redundancy	restart uplink-redundant, dump protocols uplink-redundant
L2 Loop Detection	restart loop-detection, dump protocols loop-detection
sFlow Statistics	show sflow, clear sflow statistics, restart sflow, dump sflow
IEEE 802.3ah/UDLD	restart efmoam, dump protocols efmoam
LLDP	restart lldp, dump protocols lldp
IPv4, ARP, ICMP	show netstat (netstat), clear netstat, clear tcp
Policy-based Routing	dump policy, restart policy, dump protocols track-object, restart track-object
IPv4 Multicast Routing Protocols	restart ipv4-multicast, dump protocols ipv4-multicast, erase protocol-dump ipv4-multicast
Routing Protocol Common to IPv4 and IPv6	restart unicast, debug protocols unicast, no debug protocols unicast, dump protocols unicast, erase protocol-dump unicast
IPv6, NDP, ICMPv6	show netstat (netstat), clear netstat, clear tcp
IPv6 DHCP Relays	restart ipv6-dhcp relay, dump protocols ipv6-dhcp relay