AX2500S Software Manual

Operation Command Reference

For Version 3.5

AX25S-S004X-70

AlaxalA

Relevant products

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

Export restrictions

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

Trademarks

Ethernet is a registered trademark of Xerox Corporation.
Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and other countries.
Windows is a registered trademark of Microsoft Corporation in the United States and other countries.
RSA and RSA SecurID are trademarks or registered trademarks of RSA Security Inc. in the United States and other countries.
sFlow is a registered trademark of InMon Corporation in the United States and other countries.
Wake-on-LAN is a registered trademark of IBM Corporation.
MagicPacket is a registered trademark of Advanced Micro Devices,Inc.
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 equipment, carefully read the manual and make sure that you understand all safety precautions. After reading the manual, keep it in a convenient place for easy reference.

Notes

Information in this document is subject to change without notice.

Editions history

January 2013 (Edition 8) AX25S-S004X-70

Copyright

History of Amendments

Ver. 3.5 (Edition 8)

Summary of amendments

Location and title	Changes
1. Reading the Manual	Descriptions of AX2530S-24TD, AX2530S-48TD, and AX2530S-24S4XD series switches were added.
5. Login Security and RADIUS	The description of the `show sessions (who)` command was changed.
13. Ethernet	The descriptions of the following commands were changed: ● show interfaces ● show port ● no test interfaces
15. MAC Address Table	The description of the `show mac-address-table` command was changed.
19. IGMP/MLD Snooping	A parameter was added to the `show mld-snooping` command.
20. IPv4, ARP, and ICMP	The descriptions of the following commands were changed: ● ping ● traceroute
26. IEEE 802.1X	The description of the `show dot1x` command was changed. The list of operation log messages of the `show dot1x logging` command was changed.
27. Web Authentication	The `show web-authentication redirect target` command was added. The descriptions of the following commands were changed: ● show web-authentication login ● show web-authentication login select-option ● show web-authentication The list of operation log messages of the `show web-authentication logging` command was changed.
28. MAC-based Authentication	The descriptions of the following commands were changed: ● show mac-authentication login ● show mac-authentication login select-option The list of operation log messages of the `show mac-authentication logging` command was changed.
29. Multistep Authentication	The description of the `show authentication multi-step` command was changed.
32. GSRP	The description of the `show gsrp aware` command was changed.
33. Uplink Redundancy	The description of the `show switchport backup-statistics` command was changed.
34. SML (Split Multi Link) [OS-L2A]	A parameter was added to the `show sml channel group` command.

Location and title	Changes
37. L2 Loop Detection	The descriptions of the following commands were changed: ● show loop-detection ● show loop-detection statistics ● show loop-detection logging
41. LLDP	A parameter was added to the `show lldp` command. The description of the `show lldp statistics` command was changed.

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

Ver. 3.4 (Edition 7)

Summary of amendments

Location and title	Changes
Terminals and Remote Operations	The descriptions of the following commands were changed: ● set exec-timeout ● set terminal pager
Login Security and RADIUS	The descriptions of the following commands were changed: ● adduser ● rmuser ● show users
Checking Software Versions and Device Statuses	The descriptions of the following commands were changed: ● show system ● show environment
Log	The following commands were added: ● show critical-logging ● show critical-logging summary ● clear critical-logging
Ethernet	A parameter was added to the `show port` command.
Spanning Tree Protocols	A description of the `show spanning-tree` command was changed.
Web Authentication	The list of operation log messages of the `show web-authentication logging` command was changed.
sFlow	This chapter was added.

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

Ver. 3.3 (Edition 6)

Summary of amendments

Location and title	Changes
Terminals and Remote Operations	Parameters were added to the following commands: ● telnet ● ftp ● tftp The descriptions of the following commands were changed: ● set exec-timeout ● set terminal pager
Checking Software Versions and Device Statuses	The descriptions of the following commands were changed: ● show system ● backup ● restore
Ethernet	A parameter was added to the `show port` command.

Location and title	Changes
VLANs	The description of the `show vlan` command was changed.
Spanning Tree Protocols	The descriptions of the following commands were changed: ● show spanning-tree ● show spanning-tree statistics
Ring Protocol	The following commands were added: ● clear axrp ● clear axrp preempt-delay The description of the `show axrp` command was changed.
IPv4, ARP, and ICMP	The following commands were added: ● show ip-dual interface ● clear arp-cache Parameters were added to the following commands: ● ping ● traceroute The descriptions of the following commands were changed: ● show ip interface ● show ip arp
IPv6, NDP, and ICMPv6	This chapter was added.
IEEE 802.1X	The list of operation log messages of the `show dot1x logging` command was changed.
LLDP	The description of the `show lldp` command was changed.

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

Ver. 3.2 (Edition 5)

Summary of amendments

Location and title	Changes
Terminals and Remote Operations	The `tftp` command was added.
Configurations and File Operations	The response message to the `copy` command was added.
Checking Software Versions and Device Statuses	Parameters were added to the following commands: ● show tech-support ● backup ● restore
Ethernet	The descriptions of the following commands were changed: ● show interfaces ● show port ● no test interfaces
VLANs	The description of the `show vlan` command was changed.

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

Ver. 3.2 (Edition 4)

Summary of amendments

Location and title	Changes
Reading the Manual	The descriptions of AX2530S-24T4X and AX2530S-48T2X series switches were added.
Checking Software Versions and Device Statuses	The descriptions of the following commands were changed: ● show version ● show system ● show environment
Ethernet	The description of the `no test interfaces` command was changed.
Filters	The description of the `show access-filter` command was changed.
QoS	The description of the `show qos-flow` command was changed.

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

Ver. 3.1 (Edition 3)

Summary of amendments

Location and title	Changes
Login Security and RADIUS	The descriptions of the following commands were changed: ● adduser ● show users ● password
Time Settings and NTP	The execution example of the `set clock` command was changed. The `show clock` command was added.
Checking Software Versions and Device Statuses	The description of the `show environment` command was changed.
Log	The parameter was added to the `show logging` command.
Ethernet	The descriptions of the following commands were changed: ● show interfaces ● show port ● test interfaces
IGMP/MLD Snooping	The description of the `show access-filter` command was changed.
Common to Layer 2 Authentication	The parameter was added to the `show authentication logging` command.
Web Authentication	The description of the `show web-authentication` command was changed.

Location and title	Changes
MAC-based Authentication	The description of the `show mac-authentication` command was changed.
SNMP	This chapter was added.

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

Ver. 3.1 (Edition 2)

Summary of amendments

Location and title	Changes
Reading the Manual	A description of AX2530S-24S4X series switches was added.
Checking Software Versions and Device Statuses	The parameter was added to the `show environment` command.
Software Management	The response message to the `ppupdate` command was added.
Ethernet	The descriptions of the following commands were changed: ● show interfaces ● show port Parameters were added to the following commands: ● clear counters ● activate ● inactivate ● test interfaces ● no test interfaces
Filters	The description of the `show access-filter` command was changed.
QoS	The description of the `show qos-flow` command was changed.
IEEE 802.1X	The list of operation log messages of the `show dot1x logging` command was changed.
Web Authentication	The list of operation log messages of the `show web-authentication logging` command was changed.
MAC-based Authentication	The list of operation log messages of the `show mac-authentication logging` command was changed.
DHCP Snooping	The descriptions of the following commands were changed: ● show ip dhcp snooping ● show ip dhcp snooping binding ● show ip dhcp snooping statistics

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

Preface

Applicable products and software versions

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

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

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

[24T]:

The description applies to the AX2530S-24T switch.

[24T4X]:

The description applies to the AX2530S-24T4X switch.

[48T]:

The description applies to the AX2530S-48T switch.

[48T2X]:

The description applies to the AX2530S-48T2X switch.

[24S4X]:

The description applies to the AX2530S-24S4X switch.

[24TD]:

The description applies to the AX2530S-24TD switch.

[48TD]:

The description applies to the AX2530S-48TD switch.

[24S4XD]:

The description applies to the AX2530S-24S4XD switch.

[10G model]:

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

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

[OS-L2A]:

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

Corrections to the manual

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

Intended readers

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

Readers must have an understanding of the following:

- The basics of network system management

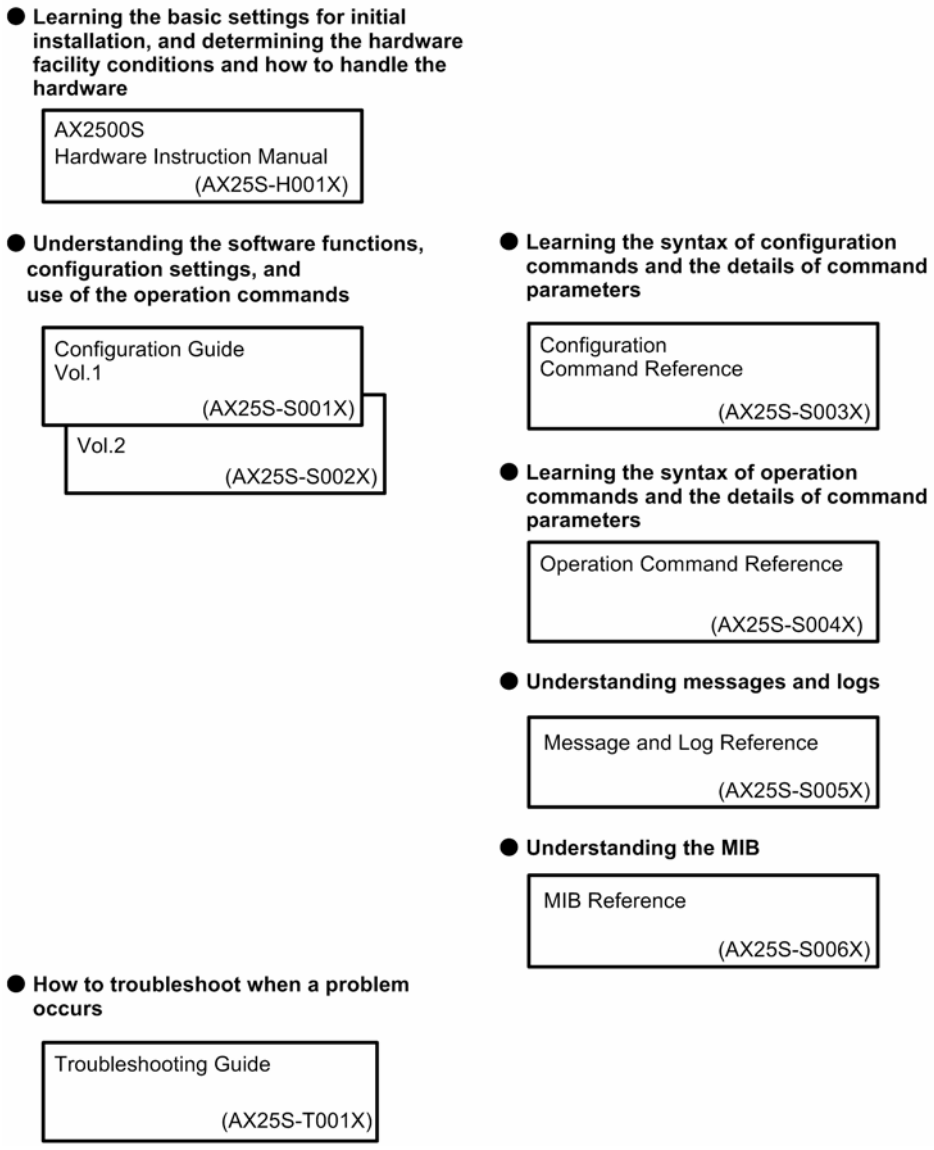
Manual URL

You can view this manual on our website at:

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

Reading sequence of the manuals

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



Abbreviations used in the manual

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second (can also appear as bps)
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol

E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU

LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	packets per second (can also appear as pps)
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode

PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PoE	Power over Ethernet
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SFP+	Enhanced Small Form factor Pluggable
SML	Split Multi Link
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier

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

Conventions: The terms "Switch" and "switch"

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

- AX2500S series switch

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

Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

1 KB (kilobyte) is 1024 bytes.

1 MB (megabyte) is 1024^2 bytes.

1 GB (gigabyte) is 1024^3 bytes.

1 TB (terabyte) is 1024^4 bytes.

Contents

1. Reading the Manual

Command description format
Specifiable values for parameters
List of character codes
Error messages displayed by the entry-error location detection functionality

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 input mode (administrator mode, or user mode and administrator mode) that can be used for 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 *Operation when all parameters are omitted*.

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

Example

Provides examples of appropriate command usage.

Display items

Describes the display items generated by the example.

The following table describes the Date display items displayed immediately after the command in the example is executed.

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

Item	Displayed information
Date	*yyyy*/*mm*/*dd hh*:*mm*:*ss timezone* year/month/day hour:minute:second time zone

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 execution of the command.

Note that error messages displayed by entry-error location detection functionality are not described here. For details on these messages, see *42. Error Messages Displayed When Editing the Configuration* in the manual *Configuration Command Reference*.

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 1-2 Specifiable values for parameters

Parameter type	Description	Input example
Any character string	See *List of character codes.*	hostname L2_switch_1
Access list name QoS flow list name	See *List of character codes*. The first character must be an alphabetical character. Subsequent characters can be alphanumeric characters, hyphens (-), underscores (_), and periods (.). It is possible to enter other characters, but use only the characters mentioned above. In addition, do not specify a character string, `resequence`, or a character string beginning with `resequence`.	mac access-list extended list101
QoS queue list name DHCP address pool name	See *List of character codes.* Alphabetic characters can be used for the first character, and alphanumeric characters, hyphens (-), underscores (_), and periods (.) can be used for the other characters. Any other characters can be entered, but specify the above type characters.	ip dhcp pool floorA
File name[#1]	You can use alphanumeric characters, hyphens (-), underscores (_), and periods (.). See also *The file name used on the RAMDISK or on the memory card*.	backup mc backup.cnf
File name filename	Specify a file name or a file name with the path name[#2]. You can use a forward slash (/) as the path delimiter.	backup mc my_dir/backup.cnf
Directory name[#3]	Specify a directory name or a directory name with the path name[#2]. You can use a forward slash (/) as the path delimiter.	mkdir my_dir
Base name	Specify only the file name. You cannot use a forward slash (/).	rename mc my_dir/backup.cnf bup.cnf
Host name	You can use alphanumeric characters, hyphens (-), and periods (.). However, you cannot specify the following characters: ● Period (.) for the first character ● Successive periods (..) ● Only with numerics and periods (.) Note that the maximum of 63 characters can be entered between periods (.).	telnet host-1

Parameter type	Description	Input example
MAC address, MAC address mask	Specify these items in hexadecimal format, separating 2-byte hexadecimal values by periods (`.`).	1234.5607.08ef 0000.00ff.ffff
IPv4 address, IPv4 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
IPv6 address with an interface name (for a link-local address only)	Specify a percent (%) between an IPv6 address and an interface name. Only link-local IPv6 addresses can be used as this parameter type.	fe80::200:87ff:fe5a:13c7%VLAN0001

#1: When you specify a file name (for example, when using the `copy` command), add the file extension.

(Example: `xx.dat`, `xx.txt`)

If you do not use a file extension when specifying a file name, a command execution error might occur.

#2: A forward slash is used as the path delimiter. A path name beginning with a forward slash is not allowed.

Also, a path name meeting any of the following conditions is not allowed:

- The path name contains two successive periods (`..`).
- The path name contains a period (`.`). The only exception is a path name that consists only of one period.
- The path name contains successive forward slashes.

  (Example: `foo//baa`)
- The path name ends with a forward slash.

  (Example: `foo/`)

#3: If the total number of characters in a directory name and its subordinate file name exceeds 64 characters, the character string will not be displayed correctly by some commands (for example, `show mc-file` or `show ramdisk-file`).

Therefore, specify *<Directory name>* in which the total number of characters, including the subordinate file name, does not exceed the maximum allowed number of characters. Keep this in mind especially when using the `mkdir` command to create a directory.

<IF#> Parameter range

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

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

Table 1-3 Range of <IF#> values

#	Model	Ethernet type	Range of values
1	AX2530S-24T/AX2530S-24TD	gigabitethernet	0/1 to 0/28

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

How to specify <Port# list> or <port list> and the range of the specifiable values

If *<Port# list>* or *<port list>* is written in the parameter input format, use a hyphen (`-`) or commas (,) in the *<IF#>* format to specify multiple ports. You can also specify one port, as when *<IF#>* is written as the parameter input format. The range of permitted values is the same as the range of *<IF#>* values in the above table.

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

```
0/1-3,0/5
```

How to specify <VLAN ID list> or <vlan id list>

If *<VLAN ID list>* or *<vlan id list>* is written in the parameter input format, use a hyphen (`-`) or commas (`,`) to specify multiple VLAN IDs. You can also specify one VLAN ID, as when *<VLAN ID>* is written as the parameter input format. 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 commas (`,`):

```
1-3,5,10
```

How to specify <Channel group# list> or <channel group list>

If *<Channel group# list>* or *<channel group list>* is written in the parameter input format, use a hyphen (`-`) or commas (`,`) to specify multiple channel group numbers. You can also specify one channel group number. The range of permitted values for the channel group number is all the channel group numbers set by the configuration command.

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

```
1-3,5
```

The file name used on the RAMDISK or on the memory card

For details about the parameter range specifiable for each command, see the description for each command or *Specifiable values for parameters.*

The following limitations exist for parameters outside the specifiable range for parameters:

- The file names are not case sensitive.
- A file name or a directory name ended with a period (`.`) cannot be used.

The file name used on the FTP, TFTP servers

For details about the parameter range specifiable for each command, see the description

for each command or *Specifiable values for parameters.*

Some server-dependent limitations other than the specifiable range for parameters might exist. For details, see the specifications of the server.

When using the Switch as an FTP server, the descriptions in above *The file name used on the RAMDISK or on the memory card* are applied.

List of character codes

Character codes are listed in the following table.

Table 1-4 List of character codes

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

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

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

Error messages displayed by the entry-error location detection functionality

For error messages output by the entry-error location detection functionality (see *5.2.3 Entry-error location detection functionality* in the *Configuration Guide Vol. 1*), see *42. Error Messages Displayed When Editing the Configuration* in the manual *Configuration Command Reference*.

2. Switching the Command Input Mode

enable
disable
exit
logout
configure

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 input from user mode.

Syntax

```
enable
```

Input mode

User mode

Parameters

None

Example

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

```
> enable Press the Enter key.
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
Sorry.	The mode cannot be changed to administrator mode because a password entry error occurred.

Notes

- Initially (at the time the Switch is first installed), no password is set. To ensure better security, we recommend that you use the `password` command to set the password.
- Help for this command is also displayed in administrator mode. Although you enter this command in administrator mode, the command input mode will not change.

disable

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

Syntax

```
disable
```

Input mode

Administrator mode

Parameters

None

Example

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

```
#  disable Press the Enter key.
>
```

Display items

None

Impact on communication

None

Response messages

None

Notes

None

exit

Ends the current command input mode as follows:

1. If you are in user mode or administrator mode, you are logged out from the device.
2. The configuration command mode ends, and you are returned to administrator mode.

Syntax

```
exit
```

Input mode

User mode and administrator mode

Parameters

None

Example

1. Ends administrator mode and logs out from the device.

   `# exit` Press the **Enter** key.

2. Ends configuration command mode.

   `(config)# exit` Press the **Enter** key.

   ```
   #
   ```

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.

Syntax

```
logout
```

Input mode

User mode and administrator mode

Parameters

None

Example

In administrator mode, logs out from the command input mode.

```
# logout Press the Enter key.
login:
```

Display items

None

Impact on communication

None

Response messages

None

Notes

None

configure

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

Syntax

```
configure [terminal]
```

Input mode

Administrator mode

Parameters

terminal

Enables editing of the running configuration during operation.

Example

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

```
# configure Press the Enter key.
(config)#
```

Display items

None

Impact on communication

None

Response messages

None

Notes

The device starts operation at power up based on the settings in the startup configuration file. To change the settings, you can use this configuration command, which immediately applies a settings change. Note that if you do not save the settings configured by using the configuration command to the startup configuration file, the configuration settings will be lost when the device is restarted. We recommend that you execute the `save` configuration command or the `copy` operation command to save the settings to the startup configuration file.

3. Terminals and Remote Operations

set exec-timeout
set terminal pager
telnet
ftp
tftp

set exec-timeout

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

Syntax

```
set exec-timeout <Minutes>
```

Input mode

User mode and administrator mode

Parameters

<Minutes>

Specifies the idle time for auto-logout in minutes.

Specifiable values

0 to 60 (If 0 is specified, auto-logout does not apply.)

Operation when this command is not used:

The auto-logout time is set to 60 minutes.

Example

- Sets the auto-logout value to 10 minutes.

  `> set exec-timeout 10` Press the **Enter** key.

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.	The command could not be executed. Re-execute the command.

Notes

- When the `set terminal pager` command has been executed with the `enable` parameter specified, if "`Press any key to continue (Q to quit)`" is displayed and the display halts temporarily, you will be returned to the prompt after the set time elapses and thereafter be logged out from the device.
- The following shows the objects that are the target of the auto-logout functionality.

Target	set exec-timeout	Default logout time
Console	Y (0 to 60 minutes)	60 minutes
Telnet server	Y (0 to 60 minutes)	60 minutes
FTP server	N	30 minutes

Legend Y: Supported; N: Not supported

- Executing the `show running-config` command does not display this command setting.
- 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.

set terminal pager

Specifies whether to perform paging (see *5.2.6 Paging* in the *Configuration Guide Vol. 1*). 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.

disable

Paging is not performed.

Operation when this parameter is omitted:

Paging is performed.

Example

- Paging is not performed.

  `> set terminal pager disable` Press the **Enter** key.

- Paging is performed.

  `> set terminal pager enable` Press the **Enter** key.

Display items

None

Impact on communication

None

Response messages

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

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

Notes

- Executing the `show running-config` command does not display this command setting.
- 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.

telnet

Connects via Telnet, as a Telnet client, to the remote host that has the specified IP address.

Syntax

```
telnet [<host> [{/ipv4 | /ipv6}]]
```

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.

Specifiable values

Host name: 1 to 255 characters can be specified. For details about the characters that can be specified, see *Specifiable values for parameters*.

IPv4 unicast address

1.0.0.0 to 126.255.255.255, 128.0.0.0 to 223.255.255.255

IPv6 global unicast addresses

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

IPv6 link local unicast address

fe80:0000:0000:0000:0000:0000:0000:0000: to fe80:0000:0000:0000:ffff:ffff:ffff:ffff

Operation when this parameter is omitted:

This parameter cannot be omitted.

{/ipv4 | /ipv6}

/ipv4

Establishes a connection via IPv4 only.

/ipv6

Establishes a connection via IPv6 only.

Operation when this parameter is omitted:

Establishes a connection via IPv4 or IPv6.

Operation when all parameters are omitted:

This parameter cannot be omitted.

Example

1. Accesses the remote host whose IP address is `192.168.0.1` via Telnet.

   `> telnet 192.168.0.1` Press the **Enter** key.

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

   ```
   Trying 192.168.0.1 ...
   ```

2. After the connection is established with the remote host, you can enter the login

name and password.

`login: username` Press the **Enter** key.

`Password: ********` Press the **Enter** key.

3. Accesses the remote operation terminal whose IPv6 address is `100::2` via Telnet.

```
> telnet 100::2
Trying 100::2 ...
```

Display items

None

Impact on communication

None

Response messages

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

Message	Description
aborted.	DNS request is aborted.
<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
Can't assign requested address.	The interface of the link-local address is invalid.
Trying *<host>*...	Trying to connect to *<host>*. *<host>*: Remote host

Notes

- To interrupt the processing while `Trying...` is displayed, press the **Ctrl**+**C**, **Ctrl**+**Shift**+**6** keys and then the **X** key in sequence. The process is interrupted by any of those commands.
- To break the attempted connection, press the **Ctrl**+**Shift**+**6** keys and then the **B** key.
- This command sends the input key codes to the login destination host without making any modifications. Therefore, the key code used on the terminal on which this command is entered must be the same as the key code recognized by the destination host. If they are different, the command will not operate correctly. For example, as the input key code for the **Enter** key, some terminals generate only **CR**, whereas other terminals generate **CR** and **LF**. Also, when a destination device recognizes the **Enter** key, some devices only recognize **CR**, whereas other devices recognize **CR** and **LF**. Check the settings of the input terminal and the login destination device beforehand.

ftp

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

Syntax

```
ftp <host> [{/ipv4 | /ipv6}]
```

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.

Specifiable values

Host name: 1 to 255 characters can be specified. For details about the characters that can be specified, see *Specifiable values for parameters*.

IPv4 unicast address

1.0.0.0 to 126.255.255.255, 128.0.0.0 to 223.255.255.255

IPv6 global unicast addresses

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

IPv6 link local unicast address

fe80:0000:0000:0000:0000:0000:0000:0000: to fe80:0000:0000:0000:ffff:ffff:ffff:ffff

Operation when this parameter is omitted:

This parameter cannot be omitted.

{/ipv4 | /ipv6}

/ipv4

Establishes a connection via IPv4 only.

/ipv6

Establishes a connection via IPv6 only.

Operation when this parameter is omitted:

Establishes a connection via IPv4 or IPv6.

Operation when all parameters are omitted:

This parameter cannot be omitted.

Example

Logs in to the remote operation terminal whose IP address is `192.168.0.1`.

```
> ftp 192.168.0.1
```
Press the **Enter** key.

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 mode returns to operation command mode.

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 following table describes the parameters that can be specified for file transfer.

Parameter type	Description	Number of characters
<Local file>	You can use alphanumeric characters, hyphens (`-`), underscores (`_`), and periods (`.`). See *Base name* under *Fine name* in *Specifiable values for parameters*.	1 to 64 characters
<Local files> mget *<Remote files>*	You can use alphanumeric characters, hyphens (`-`), underscores (`_`), periods (`.`), asterisks (`*`), and question marks (`?`). If the character string includes a question mark (`?`), enclose the entire character string in double quotation marks (`"`). See *Base name* under *Fine name* in *Specifiable values for parameters*.	1 to 64 characters
<Remote file> mdelete *<Remote files>* *<From name>* *<To name>* *<Remote directory>* *<Directory name>*	See *Any character string* in *Specifiable values for parameters*.	1 to 1024 characters
<Mode>	See *Any character string* in *Specifiable values for parameters*.	1 to 64 characters

#: File names that end with a period (.) cannot be used.

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.

If *<Remote file>* does not meet the input conditions for *<Local file>* (number of characters and character type), make sure you specify *<Local file>*.

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>*.

chmod *<Mode>* *<Remote file>*

Changes the attribute of the file specified for *<Remote file>* on the remote operation terminal to the attribute specified for *<Mode>*.

delete *<Remote file>*

Deletes *<Remote file>* on the remote operation terminal.

help [*<Command>*]

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

lols

Lists the contents of the RAMDISK on the Switch.

ls [*<Remote directory>*]

Lists the contents of *<Remote directory>* (current directory if *<Remote directory>* is not specified) on the remote operation terminal.

mdelete [*<Remote files>*]

Deletes *<Remote files>* on the remote operation terminal. Use this command when multiple files must be deleted. Enter the command in the format `mdelete *.txt`.

mkdir *<Directory name>*

Creates a directory on the remote operation terminal.

passive

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

prompt

Enables (on) or disables (off) interactive mode for the `mget`, `mput`, and `mdelete` commands.

If this mode is enabled (on), files can be selected separately.

The following table shows the display format and describes the options.

<Command name> *<File name>* `[y/n/a/q/?]?`

Display	Description
y	Executes the file.
n	Skips the file.
a	Executes all subsequent files.
q	Ends command execution.
?	Displays Help.

If the mode is off, all files are transferred or deleted unconditionally.

The default is enabled (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 display of the detailed response information from the FTP server. The default is enabled (on).

Display items

None

Impact on communication

None

Response messages

Table 3-4 List of response messages for the ftp command

Message	Description
aborted.	File transfer is aborted. DNS request is aborted.
Can't assign requested address.	The interface of the link-local address is invalid.
Connecting...	Connection to the FTP server is in progress.
Error: Can't get file names.	A file list could not be acquired when the `mget`, `mput`, or `mdelete` command was executed.
Error: Can't open "*<File name>*".	A file could not be opened. *<File name>*: The specified file name

Message	Description
Error: Command send failed.	A communication error occurred.
Error: Connect failed.	An attempt to connect to the FTP server failed.
Error: Data accept failed.	A communication error occurred.
Error: Data connect failed.	A communication error occurred.
Error: Data receive failed.	A communication error occurred.
Error: Data send failed.	A communication error occurred.
Error: File not found "*<File name>*".	The specified file could not be found. *<File name>*: The specified file name
Error: File read failed.	A file could not be read.
Error: File write failed.	Writing to a file failed.
Error: Invalid file name "*<File name>*".	The file name is invalid (for example, an invalid character string was used). *<File name>*: The specified file name
Error: Is a directory "*<File name>*".	The specified *<File name>* is a directory. *<File name>*: The specified file name
Error: Reply receive failed.	A communication error occurred.
Error: Too long file name.	The file name is too long. (In the file name list of the `mput`, `mget`, or `mdelete` command)
Error: Too much file entries.	There are too many files. (In the file name list of the `mput`, `mget`, or `mdelete` command)
No address associated with hostname.	The connection to the host could not be established because the address could not be resolved.
Passive: off	Passive mode has been disabled.
Passive: on	Passive mode has been enabled.
Prompting: off	Interactive mode for the `mput`, `mget`, or `mdelete` command has been disabled.
Prompting: on	Interactive mode for the `mput`, `mget`, or `mdelete` command has been enabled.
Type: ascii	The type for sending and receiving files has been set to ASCII.
Type: binary	The type for sending and receiving files has been set to binary.
Verbose: off	Display of a detailed response has been disabled.

Message	Description
Verbose: on	Display of a detailed response has been enabled.

Notes

- A user ID whose password is not set on the destination terminal might not be able to log in via FTP. If this occurs, set the password on the destination terminal, and then execute the `ftp` command again.
- If commands cannot be input, enter the **Ctrl**+**C** keys to exit.
- A local directory on the Switch can be moved only to `/ramdisk`.
- A local file on the Switch can be sent to or received from `/ramdisk` only.
- If the default file transfer format is ASCII, you will need to execute the `binary` command to enable the transfer of binary files.
- If you press **Ctrl**+**C** while a file is being transferred with a `get` or `put` command, the file transfer is immediately interrupted. The interruption is reported to the remote operation terminal and a response is waited for. Therefore, if some communication failures occur between the Switch and the remote operation terminal, you might not see any `ftp` prompts even if you press **Ctrl**+**C**. In this case, press **Ctrl**+**C** again.

tftp

Transfers files between the Switch and a connected remote operation terminal by using UDP. This functionality is used for transferring update files to TFTP servers.

Syntax

```
tftp [<host> [{/ipv4 | /ipv6}]]
```

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.

Specifiable values

Host name: 1 to 255 characters can be specified. For details about the characters that can be specified, see *Specifiable values for parameters*.

IPv4 unicast address

1.0.0.0 to 126.255.255.255, 128.0.0.0 to 223.255.255.255

IPv6 global unicast addresses

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

IPv6 link local unicast address

fe80:0000:0000:0000:0000:0000:0000:0000: to fe80:0000:0000:0000:ffff:ffff:ffff:ffff

Operation when this parameter is omitted:

Displays the `tftp` prompt. 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.

Operation when this parameter is omitted:

Establishes a connection via IPv4 or IPv6.

Operation when all parameters are omitted:

Displays the `tftp` prompt. In this state, a connection to the remote operation terminal has not been established. Use the `connect` command to establish the connection.

Example

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

`> tftp 192.168.0.1` Press the **Enter** key.

After executing the `tftp` command, 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, 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 following table describes the parameters that can be specified for file transfer.

Parameter type	Description	Number of characters
<local-file>	You can use alphanumeric characters, hyphens (`-`), underscores (_), and periods (`.`). See *Base name* under *Fine name* in *Specifiable values for parameters*.	1 to 64 characters
<remote-file>	See *Any character string* in *Specifiable values for parameters*.	1 to 256 characters

   #: File names that end with a period (.) cannot be used.

   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.

   If *<remote file>* does not meet the input conditions for *<local-file>* (number of characters and character type), make sure you specify *<local-file>*.

   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>*

   Connects to the TFTP server with the specified address.

   quit

   Ends the `tftp` command.

   binary

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

   ascii

   Sets ascii (netascii) as the file transfer format.

   help [*<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 3-5 List of response messages for the tftp command

Message	Description
Aborted.	File transfer is aborted. DNS request is aborted.
Can't assign requested address.	The interface of the link-local address is invalid.
Can't execute.	The command could not be executed. Re-execute the command.
Error code *<number>*: *<message>*	Displaying other TFTP error messages: *<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.
Error: Invalid file name "*<File name>*".	The file name is invalid (for example, an invalid character string was used). *<File name>*: The specified file name
File access error.	An attempt to read from or write to a local file (RAMDISK) failed.
getting from *<host>*:*<remote-file>* to *<local-file>* [*<mode>*]	Receiving *<remote-file>* on *<host>* as *<local-file>* (the transfer mode is *<mode>*). *<host>*: Remote host *<remote-file>*: Remote file name *<local-file>*: Local file name *<mode>*: File transfer mode
mode set to netascii	The type for sending and receiving files has been set to ascii (netascii).
mode set to octet	The type for sending and receiving files has been set to binary (octet).
No address associated with hostname.	The connection to the host could not be established because the address could not be resolved.
No target machine specified, Use connect command.	The connection destination has not been set. Use the `connect` command to set it.

Message	Description
Protocol error: *<description>*	An invalid message was received from the server. *<description>*: Detailed description
putting *<local-file>* to *<host>*:*<remote-file>* [*<mode>*]	Sending *<local-file>* to *<host>* as *<remote-file>* (the transfer mode is *<mode>*). *<local-file>*: Local file name *<host>*: Remote host *<remote-file>*: Remote file name *<mode>*: File transfer mode
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. When the `get` or `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 input, enter the **Ctrl**+**C** keys to exit.
- A local file on the Switch can be sent to or received from `/ramdisk` only.

4. Configurations and File Operations

show running-config
show startup-config
copy
erase startup-config
rename
del
mkdir
rmdir

show running-config

Displays the running configuration.

Syntax

```
show running-config
```

Input mode

Administrator mode

Parameters

None

Example

None

Display items

None

Impact on communication

None

Response messages

Table 4-1 List of response messages for the show running-config command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
CAUTION!!! This configuration list is too big!!! (xxxxxxx byte) *x*: Indicates the size of `running-config`.	The `running-config` list is too large. The `running-config` list exceeds 1 MB, so it cannot be saved to `startup-config`. Review the configuration.

Notes

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

show startup-config

Displays the startup configuration file used at device startup.

Syntax

```
show startup-config
```

Input mode

Administrator mode

Parameters

None

Example

None

Display items

None

Impact on communication

None

Response messages

None

Notes

None

copy

Copies the specified file or directory.

Syntax

```
copy startup-config ramdisk {<File name> | <Directory name>}
copy running-config startup-config
copy running-config mc {<File name> | <Directory name>}
copy mc {<File name> | <Directory name>} mc {<File name> | <Directory name>}
copy mc {<File name> | <Directory name>} ramdisk {<File name> | <Directory name>}
copy ramdisk <File name> startup-config
copy ramdisk {<File name> | <Directory name>} ramdisk {<File name> | <Directory name>}
copy ramdisk {<File name> | <Directory name>} mc {<File name> | <Directory name>}
copy auto-log mc {<File name> | <Directory name>}
copy auto-log ramdisk {<File name> | <Directory name>}
```

Input mode

User mode and administrator mode for the following commands

```
copy mc {<File name> | <Directory name>} mc {<File name> | <Directory name>}
copy mc {<File name> | <Directory name>} ramdisk {<File name> | <Directory name>}
copy ramdisk {<File name> | <Directory name>} mc {<File name> | <Directory name>}
copy ramdisk {<File name> | <Directory name>} ramdisk {<File name> | <Directory name>}
```

For all other commands, only administrator mode is available.

Parameters

`startup-config`: Startup configuration file

`running-config`: Running configuration

`auto-log`: The device status information collected automatically after the device starts

{*<File name>* | *<Directory name>*}

<File name>

Specifies the name of a file at the copy source or copy destination.

Specify the file name with 64 or fewer characters. The file name is not case sensitive.

For the characters that can be specified, see *Specifiable values for parameters.*

<Directory Name>

Specifies the directory name at the copy source or copy destination.

Specify the directory name so that the total number of characters used in the directory name and its subordinate file name is no more than 64. The file name is not case sensitive.

For the characters that can be specified, see *Specifiable values for parameters.*

startup-config ramdisk {*<File name>* | *<Directory name>*}

Copies the startup configuration file to the RAMDISK.

running-config startup-config

Copies the running configuration to the startup configuration file.

running-config mc {*<File name>* | *<Directory name>*}

Copies the running configuration to the memory card.

mc {*<File name>* | *<Directory name>*} mc {*<File name>* | *<Directory name>*}

Copies a file or directory on the memory card to the memory card.

mc {*<File name>* | *<Directory name>*} ramdisk {*<File name>* | *<Directory name>*}

Copies a file or directory on the memory card to the RAMDISK.

ramdisk *<File name>* startup-config

Copies a file on the RAMDISK to the startup configuration file.

A directory on the RAMDISK cannot be specified.

ramdisk {*<File name>* | *<Directory name>*} mc {*<File name>* | *<Directory name>*}

Copies a file or directory on the RAMDISK to the memory card.

ramdisk {*<File name>* | *<Directory name>*} ramdisk {*<File name>* | *<Directory name>*}

Copies a file or directory on the RAMDISK to the RAMDISK.

auto-log mc {*<File name>* | *<Directory name>*}

Copies the auto-log information to the memory card.

auto-log ramdisk {*<File name>* | *<Directory name>*}

Copies the auto-log information to the RAMDISK

Example

- Copy the running configuration to the startup configuration file. (If the copy destination is the startup configuration file, a confirmation message is displayed.)

```
# copy running-config startup-config
Do you wish to copy from running-config to startup-config? (y/n): y
```

- Copy a file on the RAMDISK to the startup configuration file. (If the copy destination is the startup configuration file, a confirmation message is displayed.)

```
# copy ramdisk config1.txt startup-config
Do you wish to copy from RAMDISK to startup-config? (y/n): y
```

Display items

None

Impact on communication

If a file on the RAMDISK is copied to the startup configuration file, you must restart the device to apply the file to the running configuration. Restart the device by executing the `reload` operation command, or by turning it off and then on again.

Response messages

Table 4-2 List of response messages for the copy command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command. The possible causes are as follows: ● The file name is incorrect. ● The file was not found. ● The memory card might be damaged. ● The file system might be damaged.

Message	Description
Can't access to MC by write protection.	Make sure the memory card's protect switch is not set to ▼Lock. If the switch is set to ▼Lock, move it to the opposite side, and then insert the memory card again. Make sure there is no dust in the memory card slot. If there is dust, remove it with a dry cloth and then insert the memory card again.
Can't copy subdirectory.	Subdirectories cannot be copied.
File format error.	The file format is invalid. Make sure the name of the specified file is correct.
File name length exceeds the limit.	The file name or the directory, including its path name, exceeds 64 characters.
File size too big.	The source file size is too large. Reduce the file size less than 1 MB.
MC is not inserted.	A memory card was not inserted.
Not enough space on device.	Capacity at the write destination is insufficient.
Source and destination are identical.	The source and destination files for a transfer exist at the same location.

Notes

- Editing the startup configuration file has no effect on the running configuration or communication.
- If a file on the RAMDISK is copied to the startup configuration file, you must restart the device to apply the file to the running configuration. Restart the device by executing the `reload` command, or by turning it off and then on again.
- If the copy destination is the startup configuration file, the copy processing is performed even if there is an error in the specified configuration file. After the device is restarted, execute the `show logging` command to make sure the operation log does not indicate an inconsistent configuration.
- If there is insufficient free space for storing files, a configuration cannot be copied. Use the `show mc` command and the `show ramdisk` command to check the unused capacity. 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 1MB of free capacity is required for a maximum-size configuration file.
- If a file on the memory card is specified, the command can be executed only when the memory card is inserted.
- If a file on the memory card is specified, the ACC LED on the device is on while the command is being executed. Do not remove or insert the memory card while the ACC LED is on.
- Note that the file copied to the RAMDISK will be deleted when the device restarts.
- Specify the file name with 64 or fewer characters. If the file name is too long, it will not be displayed correctly when the `show mc-file` or `show ramdisk-file` command is executed.
- If you create the configuration file on your PC and save it to the memory card used for operation, specify the file name with 64 or fewer characters.

- You cannot view the `auto-log` file because it is a binary file that the manufacturer uses for failure analysis.
- If the source and destination files for a copy operation are the same, an error occurs as follows:

  When both the copy source and the copy destination are the memory card and the file names (including their path names) are the same

  When both the copy source and the copy destination are the RAMDISK and the file names (including their path names) are the same

  `Example: When the mc <File name> mc <File name> command is executed.`

  ```
  copy mc aaa        mc aaa Not allowed
  copy mc bbb/xxx    mc bbb/xxx Not allowed
  copy mc bbb/xxx    mc bbb/yyy OK
  ```

- If there are any subdirectories in the copy source directory, an error occurs.
- If the name of a directory at the copy destination is the same as the name of the source directory, the source file is copied to that directory or overwrites a file in that directory.

erase startup-config

Deletes the contents of the startup configuration file.

Syntax

```
erase startup-config
```

Input mode

Administrator mode

Parameters

None

Example

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

Display items

None

Impact on communication

None

Response messages

None

Notes

If you restart the device after executing this command, the contents of the startup configuration file will be deleted. In such cases, you will not be able to log in via the network.

rename

Renames a file on the memory card or the RAMDISK.

Syntax

```
rename {mc | ramdisk} {<File name> | <Directory name>} <Base name>
```

Input mode

User mode and administrator mode

Parameters

{mc | ramdisk}

mc

Specifies a file on the memory card.

ramdisk

Specifies a file on the RAMDISK.

Operation when this parameter is omitted:

This parameter cannot be omitted.

{*<File name>* | *<Directory name>*}

<File name>

Specifies the old file name.

Specify the file name with 64 or fewer characters.

For the characters that can be specified, see *Specifiable values for parameters.*

<Directory name>

Specifies the old directory name.

Specify the directory name with 64 or fewer characters.

For the characters that can be specified, see *Specifiable values for parameters.*

Operation when this parameter is omitted:

This parameter cannot be omitted.

<Base name>

Specifies the new file name or directory name.

Specify the name with 64 or fewer characters.

For the characters that can be specified, see *Specifiable values for parameters.*

Example

- Rename a file on the memory card.

  `# rename mc abc/showtech.txt shotech_01.txt` Press the **Enter** key.
- Rename a directory on the memory card.

  `# rename mc abc efg` Press the **Enter** key.

Display items

None

Impact on communication

None

Response messages

Table 4-3 List of response messages for the rename command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command. The possible causes are as follows: ● The file name is incorrect. ● The file was not found. ● The memory card might be damaged. ● The file system might be damaged.
MC is not inserted.	A memory card was not inserted.
Can't access to MC by write protection.	Make sure the memory card's protect switch is not set to ▼Lock. If the switch is set to ▼Lock, move it to the opposite side, and then insert the memory card again. Make sure there is no dust in the memory card slot. If there is dust, remove it with a dry cloth and then insert the memory card again.
Resultant name exceeds the maximum length.	The new file name or directory, including its path name, exceeds 64 characters. If the old file name or directory name includes a path name, specify *<Base name>* with no more characters than the value of 64 minus the number of characters in the path name.

Notes

- If a file on the memory card is specified, the command can be executed only when the memory card is inserted.
- If a file on the memory card is specified, the ACC LED on the device is on while the command is being executed. Do not remove or insert the memory card while the ACC LED is on.
- This command cannot move a file from a directory to another directory.
- When you rename a directory, you can specify a maximum of 64 characters. However, if you do so, you might not be able to use a long name in the `show` and `copy` commands as shown by the following example:

  Example:

  Old directory name: *short-dir* (20 characters)

  Old file name: *long-file* (40 characters)

  New directory name: *long-dir* (30 characters)

  `rename ramdisk` *short-dir long-dir*

  In this case, the total number of characters for the directory name and the file name becomes 70, which exceeds the limit of 64. Therefore, you cannot use these names in the `show` and `copy` commands.

del

Deletes a file on the memory card or the RAMDISK.

Syntax

```
del {mc | ramdisk} <File name>
```

Input mode

User mode and administrator mode

Parameters

{mc | ramdisk}

mc

Specifies a file on the memory card.

ramdisk

Specifies a file on the RAMDISK.

Operation when this parameter is omitted:

This parameter cannot be omitted.

<File name>

Specifies the name of the file to be deleted.

Example

- Delete the file `showtech_01` on the memory card.

  `> del mc abc/showtech_01.txt` Press the **Enter** key.

Display items

None

Impact on communication

None

Response messages

Table 4-4 List of response messages for the del command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command. The possible causes are as follows: ● The file name is incorrect. ● The file was not found. ● The memory card might be damaged. ● The file system might be damaged. ● The specified name is the name of a directory.
MC is not inserted.	A memory card was not inserted.

Message	Description
Can't access to MC by write protection.	Make sure the memory card's protect switch is not set to ▼Lock. If the switch is set to ▼Lock, move it to the opposite side, and then insert the memory card again. Make sure there is no dust in the memory card slot. If there is dust, remove it with a dry cloth and then insert the memory card again.

Notes

- If a file on the memory card is specified, the command can be executed only when the memory card is inserted.
- If a file on the memory card is specified, the ACC LED on the device is on while the command is being executed. Do not remove or insert the memory card while the ACC LED is on.
- Even if this command is not executed, all files on the RAMDISK are deleted when the device restarts.
- Attempting to delete a directory by using this command results in error. For details about deleting a directory, see the description of the `rmdir` command.

mkdir

Creates a new directory.

Syntax

```
mkdir {mc-dir | ramdisk} <Directory name>
```

Input mode

User mode and administrator mode

Parameters

{mc-dir | ramdisk}

mc-dir

Creates a directory on a memory card.

ramdisk

Creates a directory on the RAMDISK.

<Directory name>

Specifies the name of the directory to be created.

Specify the directory name with 64 or fewer characters.

For the characters that can be specified, see *Specifiable values for parameters.*

Example

- Create the directory `newdir` on the memory card.

  `> mkdir mc-dir newdir` Press the **Enter** key.

- Create the directory `newdir` on the RAMDISK.

  `> mkdir ramdisk newdir` Press the **Enter** key.

Display items

None

Impact on communication

None

Response messages

Table 4-5 List of response messages for the mkdir command

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

Message	Description
Can't access to MC by write protection.	Make sure the memory card's protect switch is not set to ▼Lock. If the switch is set to ▼Lock, move it to the opposite side, and then insert the memory card again. Make sure there is no dust in the memory card slot. If there is dust, remove it with a dry cloth and then insert the memory card again.
MC is not inserted.	A memory card was not inserted.

Notes

- The `mc-dir` parameter cannot be used when a memory card is not inserted.
- 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.
- You can specify a maximum of 64 characters for a directory name, but if you do so, you might not be able to use a long name in the `show` and `copy` commands.

rmdir

Deletes a specified empty directory.

Syntax

```
rmdir {mc-dir | ramdisk} <Directory name>
```

Input mode

User mode and administrator mode

Parameters

{mc-dir | ramdisk}

mc-dir

Deletes a directory on the memory card.

ramdisk

Deletes a directory on the RAMDISK.

<Directory name>

Specifies the name of the directory to be deleted.

Example

- Delete the directory `deldir` on the memory card.

  `> rmdir mc-dir deldir` Press the **Enter** key.

- Delete the directory `deldir` on the RAMDISK.

  `> rmdir ramdisk deldir` Press the **Enter** key.

Display items

None

Impact on communication

None

Response messages

Table 4-6 List of response messages for the rmdir command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Can't access to MC by write protection.	Make sure the memory card's protect switch is not set to ▼Lock. If the switch is set to ▼Lock, move it to the opposite side, and then insert the memory card again. Make sure there is no dust in the memory card slot. If there is dust, remove it with a dry cloth and then insert the memory card again.
MC is not inserted.	A memory card was not inserted.

Notes

- The `mc-dir` parameter cannot be used when a memory card is not inserted.
- 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.
- If there is a file in the specified directory, an error occurs. For details about deleting a file, see the description of the `del` command.

5. Login Security and RADIUS

adduser
rmuser
show users
password
clear password
show sessions (who)
show radius-server
clear radius-server
show radius-server statistics
clear radius-server statistics

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. Set 1 to 16 characters for the user name. For the user name, alphabetic characters can be used for the first character, and alphanumeric characters can be used for the second and subsequent characters.

no-flash

Does not store the CLI environment information of the new account into the internal flash memory.

Operation when this parameter is omitted:

Stores the CLI environment information of the new account into the internal flash memory.

Example

1. Add a new login user `user1`.

   `# adduser user1` Press the **Enter** key.

   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 user1.
   ```

   `New password:********` Press the **Enter** key.

   If the password configuration is interrupted (press the **Ctrl** + **C** 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:********` Press the **Enter** key.

   ```
   # exit
   >
   ```

Display items

None

Impact on communication

None

Response messages

Table 5-1 List of response messages for the adduser command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
User: '*<user name>*' is not a valid login name.	This user name cannot be used. *<user name>*: User name
Mismatch; try again.	The new password and the re-entered password are not the same. Re-enter the password.
Password unchanged.	The password change was canceled.
Password: system error.	A system error occurred in an attempt to write to the internal flash memory file system.
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.
User: already a '*<user name>*' user.	The specified user has already been registered. *<user name>*: User name
User: Cannot add new user because the maximum number is already set.	No more entries can be registered because maximum number of users are registered.
User: system error.	A system error occurred in an attempt to write to the internal flash memory file system.

Notes

- To abort password configuration, press the **Ctrl**+**C** keys. If the **Ctrl**+**C** keys are pressed while retyping, the input prompt (`Mismatch; try again.`) is displayed. If this happens, press the **Ctrl**+**C** keys again. If password configuration is aborted, a new login user with no password is created.
- A login user name that has already been registered cannot be added.
- 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. 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.
- If you create an account with the `adduser` command and specify the `no-flash` parameter then configure settings using the `set exec-timeout`, or `set terminal pager` commands, they revert to the default settings when the device is restarted.

rmuser

Deletes the account of a login user registered by the `adduser` command.

Syntax

`rmuser` *<user name>*

Input mode

Administrator mode

Parameters

<user name>

Specifies the registered login user name.

Example

1. Delete the user registration of the login user named `operator`.

   `# rmuser operator` Press the **Enter** key.

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 5-2 List of response messages for the rmuser command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
User: No such user '*<user name>*'.	The specified user has not been registered. *<user name>*: User name
User: Permission denied.	The account cannot be deleted as the specified user is logged in.
User: Remove myself?	The account of the user executing this command cannot be deleted.
User: system error.	A system error occurred in an attempt to write to the internal flash memory file system.

Notes

- 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.
- The default user (`operator`) provided at the time the Switch is first installed can be deleted.
- The accout cannot be deleted if the specified user is logged in. Therefore, the deletion target user should be logged out by the `logout` command or `exit` command beforehand.

show users

Displays the effective user information set on the Switch.

Syntax

```
show users
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 5-1 Displaying information about valid users

```
> show users

Date 2011/02/23 02:16:59 UTC
<aaa methods>
  authentication login default   : group "12345"
  authentication end-by-reject   : disable

<login authentication>
 * terminals
  console  : local
  remote   : group "12345"

 * local (users)
  No   Name              Password    Exec timeout  Terminal pager  Flash
   1   operator          ****        60(min)       disabled        saved
   2   admin             ****        30(min)       enabled         saved
   3   user              not set     never         disabled        no saved

<enable authentication>
 * terminals
  console  : local (Fixed)
  remote   : local (Fixed)

 * local (enable)
  Password : not set

>
```

Display items

Table 5-3 Item displayed for information about valid users

Item	Meaning	Displayed detailed information
<aaa methods>	Authentication method information	--

Item	Meaning	Displayed detailed information
authentication login default	Default login authentication method on the Switch	`Local`: Indicates local authentication `radius`: Indicates RADIUS authentication `radius` *<Group name>*: RADIUS server group name `local` is displayed when this item is not set. The authentication methods are applied in order in which they are configured.
authentication login end-by-reject	Operation when login authentication is rejected	`enable`: Authentication is quitted due to unsuccessful login authentication. `disable`: If the authentication fails due to an abnormality, such as an inability to communicate, the next authentication method specified by the `aaa authentication login` command is used to perform authentication. `disable` is displayed when this item is not set.
<login authentication>	Display of login authentication	--
* terminals	Information by terminal	--
console	Login authentication from the console	`Local`: Indicates local authentication (Fixed)
remote	Login authentication from the remote terminal	`Local`: Indicates local authentication `radius`: Indicates RADIUS authentication `radius` *<Group name>*: RADIUS server group name `local` is displayed when this item is not set. `(not defined)` is displayed after the group name if the RADIUS server group name that has been set is invalid.
* local (users)	Local setting for login authentication	--
No	Registration number	1 to 3 Up to three users, including the default configured `operator`, can be registered.
Name	Login user name	--
Password	Login user password setting status	`not set`: The password has not been set. `****`: The password has been set
Exec timeout	Auto-logout time	`1` to `60`: Auto-logout time (minutes) never: Auto-logout disabled.
Terminal pager	Paging	`Enabled`: Paging is performed. `Disabled`: Paging is not performed.

Item	Meaning	Displayed detailed information
Flash	Auto-logout time, storage status of paging into the internal flash memory	`saved`: Stored into the internal flash memory `no saved`: Not stored into the internal flash memory (restored to the default after device restart)
<enable authentication>	Display of enable authentication	--
* terminals	Information by terminal	--
console	enable authentication on the console	`local (Fixed)`: Indicates local authentication (Fixed)
remote	Enable authentication in the remote terminal	`local (Fixed)`: Indicates local authentication (Fixed)
* local (enable)	Local setting for enable authentication	--
Password :	enable password setting status	`not set`: The password has not been set. `****`: The password has been set

Impact on communication

None

Response messages

None

Notes

None

password

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

1. In user mode, only the login user password can be changed.
2. In administrator mode, the login user password 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 user name.

Operation when this parameter is omitted:

Changes the password of the current login user.

enable-mode

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

Example

- Change the password of the login user name `operator`. Administrator mode

  ```
  # password operator
  Changing local password for operator
  New password:********
  Retype new password:********
  #
  ```

  `Changing local password for operator` ... The login user name is displayed.

  `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). User mode

  ```
  > password
  Changing local password for xxxxxxx
  Old password:********
  New password:********
  Retype new 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 5-4 List of response messages for the password command

Message	Description
Mismatch; try again.	The new password and the re-entered password are not the same. Re-enter both passwords.
Password unchanged.	The password change was canceled.
Password: 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 a password 6 to 128 characters in length.
Password: unknown user '*<user name>*'.	The specified user has not been registered. *<user name>*: User name

Notes

- 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:`).
- To abort password configuration, press the **Ctrl**+**C** keys. If the **Ctrl**+**C** keys are pressed while retyping, the input prompt (`Mismatch; try again.`) is displayed. If this happens, press the **Ctrl**+**C** keys again.
- 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. We recommend that you use upper-case alphabetic characters, numbers, and symbols in addition to lower-case alphabetic characters. If a password consists of only lower-case alphabetic characters, an error is displayed. Note, however, that if you re-enter the same password, it will be accepted.

clear password

Clears the password of a login user. The operation differs 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 user name.

Operation when this parameter is omitted:

Clears the password of the current login user.

enable-mode

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

If the `enable-mode` parameter is not specified, only the login user password is deleted.

Example

- Clear the password of the login user name `operator`. Administrator mode

```
# clear password operator
Changing local password for operator ...The login user name is displayed.
Password cleared.
#
```

- Clear the password of the current login user (with no parameters). User mode

```
> 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 5-5 List of response messages for the clear password command

Message	Description
Password unchanged.	The password deletion was canceled.
Permission denied.	Deletion of the password is not allowed.
Password: unknown user '*<user name>*'.	The specified user has not been registered. *<user name>*: User name

Notes

The password of other login users cannot be deleted in modes other than administrator mode. When the password of other login users is deleted, the prompt (`Old password:`) is not displayed.

show sessions (who)

Displays the users currently logged in to the Switch.

Syntax

```
show sessions
who
```

Input mode

User mode and administrator mode

Parameters

None

Example

Displays the users currently logged in to the Switch.

```
> show sessions

Date 2011/02/15 21:09:13 UTC
 Username          Type     Login                Source
*operator          console  2011/02/15 21:04:57  -
 abc1234567890     vty0     2011/02/15 21:08:09  192.168.10.1
 operator          ftp      2011/02/15 21:05:41  192.168.10.2

>
```

Display items

Table 5-6 Information displayed for logged-in users

Item	Meaning	Displayed detailed information
Username	User name	An asterisk (`*`) precedes the name of the user who is executing the command.
Type	Connection type	`console`, `vty0` to `vty15`, or `ftp`
Login	Login time	The time the user successfully logged in.
Source	IP address	IP address of the device on which the Telnet or FTP client is running. A hyphen (`-`) is always displayed for `console`.

Impact on communication

None

Response messages

None

Notes

None

show radius-server

Displays the effective RADIUS server information set on the Switch.

Syntax

```
show radius-server
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 5-2 Displaying the RADIUS server information

```
> show radius-server

Date 2012/02/01 09:45:52 UTC
 <common>
   [Authentication]
    * IP address: 192.168.100.254
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -
      IP address: 2001::fe
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -
   [Accounting]
    * IP address: 192.168.100.254
         Port:  1813  Timeout:  5  Retry:  3  Remain:    -
      IP address: 2001::fe
         Port:  1813  Timeout:  5  Retry:  3  Remain:    -
 <dot1x>
   [Authentication]
    * IP address: 2001::fe
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -
      IP address: 192.168.100.254
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -
   [Accounting]
    * IP address: 2001::fe
         Port:  1813  Timeout:  5  Retry:  3  Remain:    -
      IP address: 192.168.100.254
         Port:  1813  Timeout:  5  Retry:  3  Remain:    -
 <mac-auth>
   [Authentication]
      IP address: 192.168.101.254
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -
      IP address: 2000::fe
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -
    * hold down                                        591
   [Accounting]
    * IP address: 192.168.101.254
         Port:  1813  Timeout:  5  Retry:  3  Remain:    -
      IP address: 2000::fe
         Port:  1813  Timeout:  5  Retry:  3  Remain:    -
 <web-auth>
   [Authentication]
    * IP address: 192.168.100.254
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -
      IP address: 2001::fe
```

```
          Port:  1812  Timeout:  5  Retry:  3  Remain:    -
    [Accounting]
     * IP address: 192.168.100.254
          Port:  1813  Timeout:  5  Retry:  3  Remain:    -
       IP address: 2001::fe
          Port:  1813  Timeout:  5  Retry:  3  Remain:    -
  <Group1>
    [Authentication]
     * IP address: 192.168.100.254
          Port:  1812  Timeout:  5  Retry:  3  Remain:    -
       IP address: 2001::fe
          Port:  1812  Timeout:  5  Retry:  3  Remain:    -

>
```

Display items

Table 5-7 Information displayed for the RADIUS server

Item	Meaning	Displayed detailed information
<*server*>	Server type	`common`: General-use RADIUS server `dot1x`: RADIUS server using IEEE 802.1X authentication only `mac-auth`: RADIUS server using MAC-based authentication only `Web-auth`: RADIUS server using Web authentication only A group name: RADIUS server group
[Authentication]	Authentication information	--
IP address	IP addresses	--
Port	Authentication port number	--
Timeout	Timeout period (in minutes)	--
Retry	Number of re-transmissions	--
Remain	Time remaining until automatic restoration (in seconds)	A hyphen (`-`) is displayed if not applicable.
* hold down	All servers are unavailable.	Displayed only when all servers are unavailable.
[Accounting]	Accounting information	--
IP address	IP addresses	--
Port	Accounting port number	--
Timeout	Timeout period (in minutes)	--
Retry	Number of re-transmissions	--
Remain	Time remaining until automatic restoration (in seconds)	A hyphen (`-`) is displayed if not applicable.

Item	Meaning	Displayed detailed information
* hold down	All servers are unavailable.	Displayed only when all servers are unavailable.

Impact on communication

None

Response messages

Table 5-8 List of response messages for the show radius-server command

Message	Description
RADIUS Server is not configured.	A RADIUS server has not been configured.

Notes

- An asterisk (`*`) indicates the RADIUS server to which the next request will be submitted.

  A request to the RADIUS server is submitted in the order that hosts are set in `radius-server`.

  If no response is received from the first RADIUS server, a request is submitted to the next RADIUS server. This operation is repeated, and an asterisk (`*`) precedes the name of the RADIUS server that finally responds.

  If no response is received from all RADIUS servers, `* hold down` is displayed.

  If you want to submit a request to the first RADIUS server, execute the `clear radius-server` command.

clear radius-server

Restores the primary RADIUS server as the RADIUS server to which the Switch submits a request.

Syntax

```
clear radius-server [{common | dot1x | mac-authentication | web-authentication | group <Group name>}] [-f]
```

Input mode

User mode and administrator mode

Parameters

{common | dot1x | mac-authentication | web-authentication | group *<Group name>*}

common

Only a general-use RADIUS server can be restored as the primary RADIUS server.

dot1x

Only a RADIUS server used for IEEE 802.1X authentication only is restored as the primary RADIUS server.

mac-authentication

Only a RADIUS server used for only MAC-based authentication is restored as the primary RADIUS server.

web-authentication

Only a RADIUS server used for only Web authentication is restored as the primary RADIUS server.

group *<Group name>*

Only a RADIUS server in the specified RADIUS group is restored as the primary RADIUS server.

Operation when this parameter is omitted:

All the RADIUS servers restored as the primary RADIUS server by server type.

-f

A return to the primary RADIUS server is done without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

Figure 5-3 Example of the display when returning to the primary RADIUS server

- When a confirmation message is displayed:

```
> clear radius-server
Do you wish to clear priority of RADIUS server? (y/n): y

>
```

- When a confirmation message is not displayed:

```
> clear radius-server -f
```

```
>
```

Display items

None

Impact on communication

None

Response messages

Table 5-9 List of response messages for the clear radius-server command

Message	Description
RADIUS Server is not configured.	A RADIUS server has not been configured.

Notes

- Executing this command does not clear statistics. To clear statistics, use the command `clear radius-server statistics`.
- Executing this command restores the primary RADIUS server as the RADIUS server to which an authentication request is submitted and accounting information is sent.

show radius-server statistics

Displays statistics about the effective RADIUS server set on the Switch.

Syntax

```
show radius-server statistics [summary]
```

Input mode

User mode and administrator mode

Parameters

summary

Displays summary information about the RADIUS server.

Operation when this parameter is omitted:

Statistics about the RADIUS server are displayed.

Example 1

Figure 5-4 Displaying statistics about the RADIUS server

```
> show radius-server statistics

Date 2012/02/01 09:45:57 UTC
  IP address: 192.168.100.254
   [Authentication]     Current Request:          0
    [Tx] Request  :           2  Error  :          0
         Retry    :           0  Timeout:          0
    [Rx] Accept   :           1  Reject :          1  Challenge  :          0
         Malformed:           0  BadAuth:          0  UnknownType:          0
   [Accounting]         Current Request:          0
    [Tx] Request  :           0  Error  :          0
         Retry    :           0  Timeout:          0
    [Rx] Responses:           0
         Malformed:           0  BadAuth:          0  UnknownType:          0
  IP address: 192.168.101.254
   [Authentication]     Current Request:          0
    [Tx] Request  :           1  Error  :          0
         Retry    :           3  Timeout:          4
    [Rx] Accept   :           0  Reject :          0  Challenge  :          0
         Malformed:           0  BadAuth:          0  UnknownType:          0
   [Accounting]         Current Request:          0
    [Tx] Request  :           0  Error  :          0
         Retry    :           0  Timeout:          0
    [Rx] Responses:           0
         Malformed:           0  BadAuth:          0  UnknownType:          0
  IP address: 2000::fe
   [Authentication]     Current Request:          0
    [Tx] Request  :           1  Error  :          0
         Retry    :           3  Timeout:          4
    [Rx] Accept   :           0  Reject :          0  Challenge  :          0
         Malformed:           0  BadAuth:          0  UnknownType:          0
   [Accounting]         Current Request:          0
    [Tx] Request  :           0  Error  :          0
         Retry    :           0  Timeout:          0
    [Rx] Responses:           0
         Malformed:           0  BadAuth:          0  UnknownType:          0
  IP address: 2001::fe
   [Authentication]     Current Request:          0
```

```
     [Tx] Request  :          2  Error  :          0
          Retry    :          0  Timeout:          0
     [Rx] Accept   :          1  Reject :          0  Challenge  :          1
          Malformed:          0  BadAuth:          0  UnknownType:          0
    [Accounting]         Current Request:          0
     [Tx] Request  :          0  Error  :          0
          Retry    :          0  Timeout:          0
     [Rx] Responses:          0
          Malformed:          0  BadAuth:          0  UnknownType:          0

>
```

Display items in Example 1

Table 5-10 Statistics displayed for the RADIUS server

Item	Meaning	Displayed detailed information
IP address	IP addresses	--
[Authentication]	Authentication information	--
Current Request	Number of authentication requests being submitted	--
[Tx]	Information on sent requests	--
Request	Total number of sent Access-Request packets	Retries are excluded.
Error	Number of errors during sending	Most of these occur when the port used to connect to the RADIUS server is down (0 fixed)
Retry	Total number of Access-Request retries	--
Timeout	Number of timeouts	--
[Rx]	Information about received responses	--
Accept	Total number of received Access-Accept packets	--
Reject	Total number of received Access-Reject packets	--
Challenge	Total number of received Access-Challenge packets	--
Malformed	Number of received invalid data format replies	--
BadAuth	Number of received replies with invalid authenticators	--
UnknownType	Number of invalid packet types received	--

Item	Meaning	Displayed detailed information
[Accounting]	Accounting information	--
Current Request	Number of accounting requests	--
[Tx]	Information on sent requests	--
Request	Total number of sent Accounting-Request packets	Retries are excluded.
Error	Number of errors during sending	Most of these occur when the port used to connect to the RADIUS server is down (0 fixed)
Retry	Total number of Accounting-Request retries	--
Timeout	Number of timeouts	--
[Rx]	Information about received responses	--
Responses	Number of sent and received Accounting-Response packets	--
Malformed	Number of received invalid data format replies	--
BadAuth	Number of received replies with invalid authenticators	--
UnknownType	Number of invalid packet types received	--

Example 2

Figure 5-5 Displaying a summary of the RADIUS server

```
> show radius-server statistics summary

Date 2012/02/01 09:46:02 UTC
192.168.100.254 [Tx]Timeout: 0 [Rx]Accept/Reject: 1/1
192.168.101.254 [Tx]Timeout: 4 [Rx]Accept/Reject: 0/0
2000::fe [Tx]Timeout: 4 [Rx]Accept/Reject: 0/0
2001::fe [Tx]Timeout: 0 [Rx]Accept/Reject: 1/0

>
```

Display items in Example 2

Table 5-11 Display of the RADIUS server summary

Item	Meaning	Displayed detailed information
<ip address>	IP addresses	--

Item	Meaning	Displayed detailed information
[Tx]	Information on sent requests	--
Timeout	Number of timeouts	--
[Rx]	Information about received responses	--
Accept	Total number of received Access-Accept packets	--
Reject	Total number of received Access-Reject packets	--

Impact on communication

None

Response messages

Table 5-12 List of response messages for the show radius-server statistics command

Message	Description
RADIUS Server is not configured.	A RADIUS server has not been configured.

Notes

None

clear radius-server statistics

Clears the RADIUS server statistics.

Syntax

```
clear radius-server statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 5-6 Clearing the RADIUS server statistics

```
> clear radius-server statistics

>
```

Display items

None

Impact on communication

None

Response messages

None

Notes

None

6. Time Settings and NTP

set clock
show clock
set clock ntp
show ntp-client

set clock

Displays 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 in the range from 00 to 38 (for example, 00 means the year 2000).

MM

Specifies the month in the range from 01 to 12.

DD

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

HH

Specifies the hour in the range from 00 to 23.

MM

Specifies the minute in the range from 00 to 59.

SS

Specifies the second in the range from 00 to 59.

Operation when all parameters are omitted:

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

Example

To set the date and time as February 22, 2011 at 15:30, enter the following command:

```
> set clock 1102221530
Tue Feb 22 15:30:00 UTC 2011
>
```

Impact on communication

None

Response messages

Table 6-1 List of response messages for the set clock command

Message	Description
illegal time format.	The input format of the time is incorrect.

Notes

- The specification range is from January 1, 2000, at 00:00:00 to January 17, 2038, at

23:59:59.

- If you change the Switch's clock, in the statistics on CPU usage collected by the Switch, only the data displayed in seconds will be cleared to zero.

show clock

Displays the current date and time.

Syntax

```
show clock
```

Input mode

User mode and administrator mode

Parameters

None

Displays the current time.

Example

Enter the following command to display the current time.

```
> show clock Press the Enter key.
Tue Feb 22 15:30:00 UTC 2011
>
```

Display items

None

Impact on communication

None

Response messages

None

Notes

None

set clock ntp

Manually obtains the time from the NTP server.

Syntax

```
set clock ntp [<Server IP>]
```

Input mode

User mode and administrator mode

Parameters

<Server IP>

Specifies the NTP server address.

Operation when this parameter is omitted:

The NTP server address that is set by using the `ntp server` configuration command (primary address) is used. If the time cannot be obtained by using the primary address, the secondary address that is set by using the `ntp server` command is used.

Example

```
> set clock ntp
  Executed > Please check a result by 'show ntp-client'.

>
```

Impact on communication

None

Response messages

Table 6-2 List of response messages for the set clock ntp command

Message	Description
Failure > Please specify a NTP server address.	Set the NTP server address.
Failure > Busy.	The command is already being executed. Wait a while, and then retry the operation.
Can't execute.	The command could not be executed. Re-execute the command.
Executed > Please check a result by 'show ntp-client'.	To check the execution result, execute the `show ntp-client` command.

Notes

- You can execute this command even if the `ntp server` configuration command has not been set. If the `ntp client server` command has not been set, use this command to specify the NTP server address.
- The result is displayed within about 30 seconds after execution of this command.

show ntp-client

Displays the NTP client information.

Syntax

```
show ntp-client
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 6-1 Displaying the NTP client information

```
> show ntp-client

Date 2010/08/03 19:52:48 UTC
 Last NTP Status
  NTP-Server : 192.1.0.254, Source-Address : ---
  Mode : Unicast, Lapsed time : 104(s), Offset : 1(s)

 Activate NTP Client
  NTP-Server : 192.1.0.254, Source-Address : ---
  Mode : Unicast, Interval : 120(s)

 NTP Execute History(Max 10 entry)
  NTP-Server      Source-Address  Mode      Set-NTP-Time          Status
  192.1.0.254     ---             Unicast   2010/08/03 19:51:05        1
  192.1.0.254     ---             Unicast   2010/08/03 19:49:05        1
  192.1.0.254     ---             Unicast   2010/08/03 19:47:05        1
  192.1.0.254     ---             Unicast   2010/08/03 19:45:05        1
  192.1.0.254     ---             Unicast   2010/08/03 19:43:05        1
  192.1.0.254     ---             Unicast   2010/08/03 19:41:05        1
  192.1.0.254     ---             Unicast   2010/08/03 19:39:05        1
  192.1.0.254     ---             Command   2010/08/03 19:38:27       -2
  192.2.0.254     ---             Unicast   2010/08/03 19:37:30  Timeout
  192.1.0.254     ---             Unicast   2010/08/03 19:37:18  Timeout

>
```

Display items

Table 6-3 Information displayed by the show ntp-client command

Item	Displayed information	Displayed detailed information
Last NTP Status	The last information when it was possible to obtain the time from the NTP server	--
NTP-Server	The last accessed NTP server address	--
Source-Address	The specified source IP address	This item is displayed in unicast mode, but `---` is always displayed because the source IP address is not specified.

Item	Displayed information	Displayed detailed information
Mode	NTP client acquisition mode	`Unicast`, `Broadcast`, or `Command`
Lapsed time	The amount of time that has elapsed since the time was obtained from the NTP server	From 0 to 4294967295 (seconds)
Offset	Time lag with the NTP server	The range of values is from -2147483648 to 2147483647 (seconds).
Activate NTP Client	Information about the mode of the currently operating NTP client	--
NTP-Server	NTP server address	This item is displayed only in unicast mode.
Source-Address	The specified source IP address	This item is displayed in unicast mode, but `---` is always displayed because the source IP address is not specified.
Mode	NTP client acquisition mode	`Unicast` or `Broadcast`
Interval	The value registered by using the `ntp interval` command	If nothing is registered, `3600` is displayed by default. This item is displayed only in unicast mode. The range of values is from 120 to 604800 (seconds).
NTP Execute History(Max 10 entry)	History information on the executed NTP client operations	A maximum of 10 histories, which are the latest, are displayed.
NTP-Server	NTP server address	`Unicast`: Values set by configuration `Broadcast`: NTP server address of the acquisition source `Command`: `---` is displayed if the command has not been configured.
Source-Address	The specified source IP address	This item is displayed in unicast mode, but `---` is always displayed because the source IP address is not specified.
Mode	NTP client acquisition mode	`Unicast`, `Broadcast`, or `Command`
Set-NTP-Time	Set NTP time	If a timeout occurs or if the time cannot be acquired, the current time on the Switch is displayed.
Status	Offset value or status	Offset value: From -2147483648 to 2147483647 (seconds) If the time has been obtained normally, the offset value is displayed. For all other cases, see *Status display*[#1].

#1 Status display

#	Display	Status	Unicast	Broadcast	Operation commands
1	Offset value	Time has been updated normally.	Y	Y	Y
2	Timeout	Timeout	Y	--	Y
3	Cancel	An operation command was executed while the time was being obtained.	Y	--	--
4	30sRule	The time was changed again within 30 seconds of the previous change.	Y	Y	Y
5	Error	An error occurs due to a condition other than the above.	Y	--	Y

Impact on communication

None

Response messages

None

Notes

1. The following assumptions apply to the NTP client:

- The obtained time is basically used for the setting time. However, if an attempt is made to update the time within 30 seconds of the last update, the time will not be updated. (An exception occurs when the `set clock ntp` operation command is executed.)
- When a broadcast is received, the NTP version information is not checked. (Versions 1 to 3 are all received.)
- When a broadcast is received, NTP authentication is not checked. (Data sent from the server must not be authenticated.)

7. Checking Software Versions and Device Statuses

show version
show system
show environment
reload
show tech-support
backup
restore

show version

Displays the software version and hardware revision installed on the Switch.

Syntax

```
show version
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 7-1 Example of executing the command show version

```
> show version

Date 2010/08/06 17:38:02 UTC
Model: AX2530S-48T
S/W: OS-L2B Ver. 3.0 (Build:yy)
H/W: AX-2530-48T-B [SSSSSSSSSSSSSSSSSSSSS:R]

>
```

Display items

Table 7-1 Information displayed by the show version command

Item	Display format	Meaning
Model	Device model	Displays the device model. ● AX2530S-24T ● AX2530S-24T4X ● AX2530S-48T ● AX2530S-48T2X ● AX2530S-24S4X ● AX2530S-24TD ● AX2530S-48TD ● AX2530S-24S4XD
S/W	Software information	Displays software information. *x.x*: Software version *yy*: Build
	OS-L2B-A/OS-L2B Ver. *xx* (Build: *yy*)	L2 basic software
	OS-L2A-A/OS-L2A Ver. *xx* (Build: *yy*)	L2 advanced software The following functionalities are included. ● RSA SecurID linkage (one-time password authentication) ● Secure Wake-on-LAN ● SML (Split Multi Link)

Item	Display format	Meaning
H/W	Hardware information AX-2530-hhhhh[*SSS....SSS:R*]	Displays hardware information. *hhhhh*: Hardware model *SSS....SSS*: Serial information *R*: Manufacturer information

Impact on communication

None

Response messages

None

Notes

None

show system

Displays operating status.

Syntax

```
show system
```

Input mode

User mode and administrator mode

Parameters

None

Example 1

Figure 7-2 Example of displaying information in normal operation status

```
> show system

Date 2012/07/08 03:06:44 UTC
System: AX2530S-24T Ver. 3.4 (Build:xx)
    Name         : -
    Contact      : -
    Locate       : -
    Machine ID   : 0012.e262.3f8e
    Boot Date    : 2012/07/08 02:58:12
    Elapsed time : 0 days 00:08:32
    LED
       ST1 LED   : Green
       ST2 LED   : Light off
       Brightness mode : normal

Environment
    Power redundancy-mode : check is not executed
    Fan           :      -     Speed   : -
    PS            : active
    EPU           : notconnect EPU Fan : -
    Current wattage     : 22.50 W
    Accumulated wattage : 0.11 kWh
    Temperature  : normal
    Accumulated running time
       total     : 69 days and 6 hours
       critical  : 0 days and 0 hours

File System
    < RAMDISK information >
       used       168,960 byte
       free    31,288,320 byte
       total   31,457,280 byte
    < RAMDISK files >
    File Date               Size Name
    2012/07/08 03:06       1,024 Config_File/
    2012/07/08 03:02       4,648 Test_Config.txt
    2012/07/08 03:06       6,196 Config_File/12Floor_Config.txt
    2012/07/08 03:02      14,964 Config_File/11Floor_Config.txt
    < MC information >
    MC : enable
    Manufacture ID : 00000003
       used      9,108,992 byte
```

```
   free    116,801,536 byte
   total   125,910,528 byte
< MC files >
File Date              Size Name
2012/07/06 18:12   8,990,720 K.IMG
2012/07/08 03:05      16,384 Config_File/
2012/06/20 12:08       4,648 Test_Config.txt
2012/05/04 10:30       6,196 Config_File/12Floor_Config.txt
2012/07/05 20:17      14,964 Config_File/11Floor_Config.txt

               :
               :
```

Display items in Example 1

Table 7-2 Information displayed by the show system command

Item	Displayed information	Displayed detailed information
System	Device model	Device model name
	Software information	Version
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
Machine ID	Switch MAC addresses	--
Boot Data	Startup date and time	--
Elapsed time	Operating time	--
LED	LED status for ST1 and ST2	`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.
Brightness mode	LED brightness status	`normal`: Normal brightness `economy`: Power saving brightness `off`: The LED is off. `auto(`*xxx*`)`: Automatic brightness adjustment *xxx*: `normal`, `economy`, or `off`
Environment	Environment display	--
Power redundancy-mode	Power mode	`check is executed`: A check of whether the power is in a redundant configuration is performed. `check is not executed`: A check of whether the power is in a redundant configuration is not performed.

Item	Displayed information	Displayed detailed information
Fan	FAN operating status	`-`: No FAN `active`: Running `fault`: A fault has occurred.
Speed	The rotational speed of the FAN	`-`: No FAN `normal`: Normal rotation `stop`: Stopped rotation
PS	Installation status of the input power supply unit.	`active`: Supplied normally `fault`: No power is being supplied or there is an abnormal voltage.
EPU	Installation status of the external input power supply unit.	`active`: Supplied normally `fault`: No power is being supplied or there is an abnormal voltage. `notconnect`: Not installed
EPU Fan	EPU FAN operating status	`-`: EPU Fan is not connected. `active`: Running `fault`: A fault has occurred.
Current wattage	Current power consumption	Unit: [W]
Accumulated wattage	Accumulated power consumption	Unit: [kWh]
Temperature	Temperature environment status	`normal`: Normal `caution`: Outside the normal range `fault`: High temperature detection For the temperature value, see the description of the `show environment` command.
Accumulated running time	Cumulative operating time of the device	`total`: Total device run time since startup `critical`: Run time in the `caution` state
File System	File system	--
RAMDISK Information	RAMDISK status	--
used	Used capacity	Capacity being used by the RAMDISK file system
free	Unused capacity	Capacity not being used by the RAMDISK file system
total	Total capacity	Total capacity being used and not being used by the RAMDISK file system
RAMDISK files	List of files saved on the RAMDISK	Timestamp, size, and name of each file
MC information	Memory card status	--

Item	Displayed information	Displayed detailed information
MC	Memory card status	`enabled`: The memory card can be accessed. `not connect`: The memory card is not installed. `write protect`: Writing to the memory card is not allowed.
Manufacture ID	Type#1	Memory card production ID number
used	Used capacity#1	Capacity in use in the memory card file system
free	Unused capacity#1	Capacity not in use in the memory card file system
total	Total capacity#1	Total of capacity in use and capacity not in use for the memory card file system
MC files	List of files saved on the memory card	Timestamp, size, and name of each file

#1: Those items are displayed when the memory card status is `enabled` or `write protect`.

Example 2

The following is an example of displayed resource information.

Figure 7-3 Example of displaying resource information

```
> show system

Date 2012/07/08 07:06:44 UTC
System: AX2530S-24T Ver. 3.4 (Build:xx)

                   :
                   :

Device Resources
    IPv4 Routing Entry(static)    :     5(max entry=128)
    IPv4 Routing Entry(connected) :    22(max entry=128)
    IP Interface Entry            :     4(max entry=128)
    IPv4 ARP Entry                :    11(max entry=2048)
    IPv6 NDP Entry                :     7(max entry=256)
    MAC-address Table Entry       :    35(max entry=32768)

    System Layer2 Table Mode  : 1
    Flow detection mode : layer2-2
      Used resources for filter(Used/Max)
                                MAC      IPv4
        Port 0/1-28        :       -     2/256
        VLAN               :       -     2/256
      Used resources for QoS(Used/Max)
                                MAC      IPv4
        Port 0/1-28        :       -     1/128
        VLAN               :       -     1/128
      Used resources for TCP/UDP port detection pattern
        Resources(Used/Max):  0/16
    Flow detection out mode: layer2-2-out
      Used resources for filter outbound(Used/Max)
                                MAC      IPv4
```

```
  Port 0/1-28        :       -     2/128             |
  VLAN               :       -     2/128             |
```

```
System Layer2 Table Mode  : 1
Flow detection mode : layer2-3                       |
  Used resources for filter(Used/Max)                |
                            MAC      IPv4      IPv6    |
    Port 0/1-28 , VLAN :      -     8/256     8/128    |
  Used resources for QoS(Used/Max)                   |
                            MAC      IPv4      IPv6    |2
    Port 0/1-28 , VLAN :      -     2/128      2/64    |
  Used resources for TCP/UDP port detection pattern  |
    Resources(Used/Max):  0/16                       |
Flow detection out mode: layer2-3-out                |
  Used resources for filter outbound(Used/Max)       |
                            MAC      IPv4      IPv6    |
    Port 0/1-28 , VLAN :   6/128     8/128     8/128    |
```

1. Example of Layer 2-1 and Layer2-2 flow detection mode
2. Example of Layer 2-3 flow detection mode

Display items in Example 2

Table 7-3 Information displayed by the show system command (Resource information)

Item	Displayed information	Displayed detailed information
Device Resources	Device resource	--
IPv4 Routing Entry(static)	Number of IPv4 routing entries (static settings interface)	--
IPv4 Routing Entry(connected)	Number of IPv4 routing entries (direct-connection interface)	--
IP Interface Entry	Number of IPv4/IPv6 interface entries	--
IPv4 ARP Entry	Number of ARP entries	--
IPv6 NDP Entry	Number of NDP entries	--
MAC-address Table Entry	Number of MAC address table entries	--
System Layer2 Table Mode	Search method for the Layer 2 hardware table	Displays the search method set by the `system 12-table mode` configuration command. (If nothing is set, `1` is displayed.) ● *x*: Fixed value setting (For details about the `system 12-table mode` configuration command, see *7. Device Management* in the manual *Configuration Command Reference*.)

Item	Displayed information	Displayed detailed information
Flow detection mode	Flow detection mode	For details, see *20 Flow Detection Mode* in the manual *Configuration Command Reference*.
Used resources for filter(Used/Max)	Number of entries currently registered as filter conditions on the target interface, and the maximum number of specifiable entries	The total of the implicit discard entries and the filter condition entries set during configuration is displayed as the number of setting entries.
Used resources for QoS(Used/Max)	The number of entries for QoS flow detection conditions and the operating information that are currently registered on the target interface, and the maximum number of specifiable entries	--
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 switch, 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.	--
Flow detection out mode	Sending-side flow detection mode for the filter functionality	layer2-1-out layer2-2-out layer2-3-out For details, see *20 Flow Detection Mode* in the manual *Configuration Command Reference*.

Impact on communication

None

Response messages

None

Notes

None

show environment

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

Syntax

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

Input mode

User mode and administrator mode

Parameters

temperature-logging

Displays the temperature history of the target switch.

Operation when this parameter is omitted:

The environmental status of the switch is displayed.

Example 1

The following shows an example of displaying the operating status.

Figure 7-4 Example of executing the command show environment

```
> show environment

Date 2012/07/27 18:12:36 UTC
Fan environment
    Fan     : active
    Speed   : normal
    Mode    : 1 (silent)
    EPU Fan : -

Power environment
    PS      : active
    EPU     : notconnect

Temperature environment
    Main          : 29  degrees C
    Warning level : normal

    Temperature-warning-level current status : 29/32 degrees C
    Temperature-warning-level average status : 28/30 degrees C period 30 day(s)

Accumulated running time
    total    : 320 days and 15 hours
    critical : 219 days and 6 hours

>
```

Display items in Example 1

Table 7-4 Information displayed by the show environment command

Item	Displayed information	Displayed detailed information
Fan environment	Fan environment display	--

Item	Displayed information	Displayed detailed information
Fan	FAN operating status	`-`: No FAN `active`: Running `fault`: A fault has occurred.
Speed	The rotational speed of the FAN	`-`: No FAN `normal`: Normal rotation `stop`: Stopped rotation
Mode	Fan operation mode	`-`: No FAN. `1 (silent)`: Reducing switch noise takes priority. `2 (cool)`: Keeping the switch cool takes priority.
EPU Fan	EPU FAN operating status	`-`: EPU Fan is not connected. `active`: Running `fault`: A fault has occurred.
Power environment	Power supply unit information	--
PS	Installation status of the input power supply unit.	`active`: Supplied normally `fault`: No power is being supplied or there is an abnormal voltage.
EPU	Installation status of the external 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 environment display	--
Main[#1]	Intake temperature information	Converted value of the internal temperature Note, however, it shows `-` for 60 minutes after the Switch starts.
Warning level[#2]	Operating condition level	`normal`: Normal `caution`: Outside the normal range `fault`: High temperature detection
Temperature-warning-level current status[#3]	Information of the temperature for outputting operation messages	*mm/nn* `degree C` *mm*: Current intake temperature (converted value of the internal temperature) *nn*: Temperature that is set with the `system temperature-warning-level` configuration command

Item	Displayed information	Displayed detailed information
Temperature-warning-level average status#4	Information of the average temperature for outputting operation messages	*mm/nn* `degrees C period` *xx* `day(s)` *mm*: Current intake average temperature (converted value of the internal average temperature) *nn*: Temperature that is set with the `system temperature-warning-level average` configuration command *xx*: Time period of calculating the average temperature#5
Accumulated running time	Cumulative operating time#6	`total`: Total device run time since startup `critical`: Run time in the `caution` state

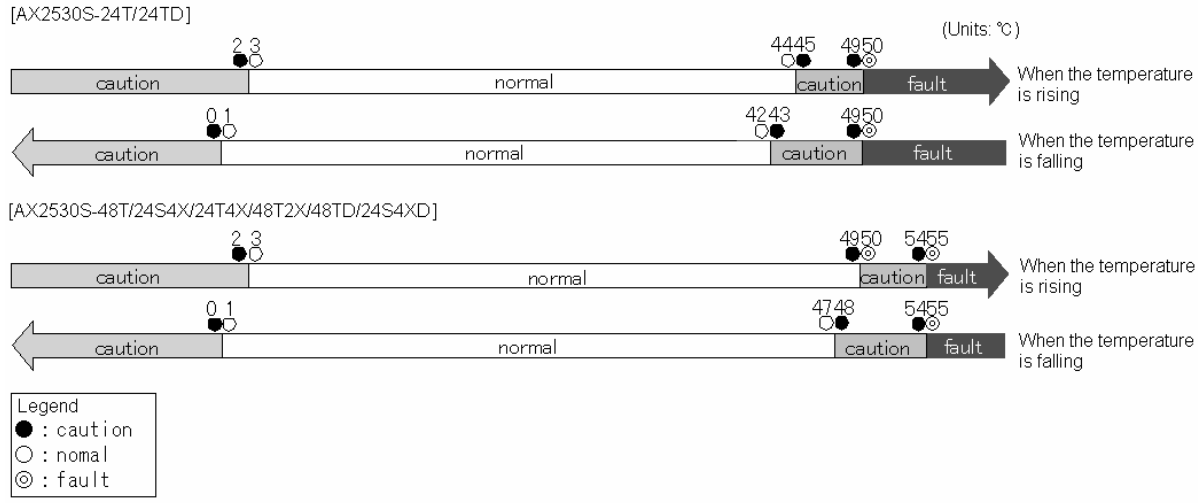
#1

The intake temperature is a converted value of the internal temperature. Therefore, the intake temperature might be quite different from the actual ambient temperature depending on the installation environment of the device, the number of the used ports, or the SFP type. When using the cooling fan monitoring and controlling functionality on the AX2530S-48T or AX2530S-48TD switch, the intake temperature might also be quite different from the actual ambient temperature depending on the ON or OFF status of the FAN.

#2

`Warning level` is displayed as a result of evaluating the changes in internal temperature.

Figure 7-5 Operating condition level and temperature



#3

When the configuration has not been set up yet, or when the temperature monitoring functionality does not work about 60 minutes after the device started, `-/-` appears.

#4

If the *<temperature>* parameter setting is omitted, the default average temperature appears.

When the configuration has not been set up yet, or the temperature logging data has not been collected for a day long, the following is displayed:

```
Temperature-warning-level average status : -/- degrees C period - day(s)
```

#5

When it is less than the number of days set, the number of days used for the calculation is displayed.

#6

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

At power-up (cumulative operating time = 0)

4 hours later (cumulative operating time = 4 hours, time written in the internal flash memory = 0 hours)

8 hours later (cumulative operating time = 8 hours, time written in the internal flash memory = 6 hours)

13 hours later (cumulative operating time = 13 hours, time written in the internal flash memory = 12 hours)

Example 2

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

Figure 7-6 Example of displaying temperature history information

```
> show environment temperature-logging

Date 2010/12/16 21:54:23 UTC
Date         0:00  6:00 12:00 18:00
2010/12/16   30.0  30.3  28.0  27.8
2010/12/15   31.0  32.0  29.8  31.1
2010/12/14      -     -  29.2  30.0

>
```

Display items in Example 2

Table 7-5 Information displayed by the show environment temperature-logging

Item	Displayed information	Displayed detailed information
Date	Date	--
0:00	Average temperature of the time period	Average temperature of the period from 18:00 (previous day) to 0:00
6:00		Average temperature of the period from 0:00 to 6:00
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 switch was not running. (Power was off or in sleep mode, 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

None

Notes

- The temperature history display is refreshed at the fixed times (0:00, 6:00, 12:00, and 18:00). The times might slightly change depending on the environment of the switch.
- For the display of temperature history, if the date of the switch 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.
- The average temperature displayed with this command is calculated using an intake temperature that is converted from the internal temperature, so it might be different from the actual ambient temperature depending on the connection port configurations or the surrounding environment.

reload

Restarts the switch.

Syntax

```
reload [-f]
```

Input mode

User mode and administrator mode

Parameters

-f

Executes the command without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

1. Restarts the switch.

   `>reload` Press the **Enter** key.

2. Display a confirmation message when the `reload` command is started.

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

   If `y` is entered, the device is restarted. If `n` is entered, restarting is canceled.

Display items

None

Impact on communication

Communication is interrupted while the device is being restarted.

Response messages

Table 7-6 List of response messages for the reload command

Message	Description
CAUTION!!! "running-config" is not saved!!!	Caution: The `running-config` setting was not saved.

Notes

- If the memory card has been installed, remove it before restarting the device.

show tech-support

Collects hardware and software status information required for technical support.

Syntax

```
show tech-support [{ page | ramdisk }] [layer-2]
```

Input mode

Administrator mode

Parameters

{ page | ramdisk }

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.

ramdisk

Directly save the information to the RAMDISK without displaying it on the console screen.

The file `showtech.txt` is generated on the RAMDISK for the saved information.

Operation when this parameter is omitted:

All information is displayed without being stopped partway. The information is not saved to the RAMDISK.

layer-2

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

Operation when this parameter is omitted:

Collects basic information about the hardware and software.

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 7-7 Example of displaying the collected information on the screen

```
# show tech-support

########## Tech-Support Log ##########
Date 2010/08/25 14:06:14 UTC
  :                          :
  :          (omitted)         :
  :                          :
Date 2010/08/25 14:18:32 UTC
########## End of Tech-Support Log ##########
```

Display items

Table 7-7 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>*: `Tech-Support Log`: Basic information that shows the hardware and software status. `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

Response messages

Table 7-8 Information displayed by the show tech-support command

Message	Description
Can't execute.	The command could not be executed. After deleting directories and files on the RAMDISK, execute the command again.
Can't execute for the maintenance mode. Please remove "page" and "ramdisk" option.	The `page` or `ramdisk` option cannot be used because the automatic restoration is disabled. Re-execute the command without specifying those options.
Executing.	Please wait a few minutes. Wait for several minutes because the Tech-Support log is being written to the RAMDISK.
Not enough space on device.	Capacity at the write destination is insufficient.

Notes

- Before executing the `show tech-support ramdisk` command, make sure there are no directories or files on the RAMDISK. If there are any directories or files on the RAMDISK, we recommend that you delete those files before executing this command.

- If `showtech.txt` already exists on the RAMDISK, it is overwritten and saved.
- This command operates regardless of the setting of the `set terminal pager` command.
- If the automatic restoration is disabled, the collected information cannot be stored on the RAMDISK. Also, you cannot use the `page` option to display the information page by page. In this case, use the capture function of the console terminal or another method to check the information on the screen.
- The following table shows the reference of the duration of time the command requires to complete its processing when the destination is set to RAMDISK.

Table 7-9 Reference for the execution time of show tech-support ramdisk

Model	Without layer-2 designation	With layer-2 designation
AX2530S-24T AX2530S-24T4X AX2530S-24S4X AX2530S-24TD AX2530S-24S4XD	3 minutes or longer	7 minutes or longer
AX2530S-48T AX2530S-48T2X AX2530S-48TD	4 minutes or longer	12 minutes or longer

If RAMDISK is not specified, the command needs several ten minutes to complete its processing.

Note that the execution time is different depending on the system configuration and/or network configuration.

backup

Saves information about the running software and device to a memory card, RAMDISK, or remote FTP server. The device information includes password information and the startup configuration file.

Syntax

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

Input mode

Administrator mode

Parameters

{mc | ramdisk | ftp *<ftp-server>*}

Specifies the backup destination.

mc

Specifies the memory card as the destination.

ramdisk

Specifies the RAMDISK as the destination.

The backup files can be transferred via FTP after backup is executed from a remote terminal.

ftp *<ftp-server>*

Specifies the remote FTP server as the destination. A host name of the server, IPv4 address, IPv6 address, or IPv6 link local unicast address with an interface name (only `fe80::/64`) can be specified in *<ftp-server>*.

<filename>

Specifies the name of a file at the copy source or copy destination.

Specify the file name with 64 or fewer characters for the memory card or RAMDISK. If a file with the same name already exists at the copy destination, it will be overwritten.

For the characters that can be specified, see *Specifiable values for parameters.*

Specify the file name with 1024 or fewer characters for the FTP server.

no-software

No software is backed up.

Operation when this parameter is omitted:

Backup, including software information, is performed.

Example 1

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

```
> enable  Press the Enter key.
# backup mc MCBackup.dat  Press the Enter key.
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  Press the Enter key.
```

```
# backup ftp 192.168.12.30 MCBackup.dat  Press the Enter key.
Backup information to 192.168.12.30 (MCBackup.dat).
Copy file to 192.168.12.30...
Connecting...

Name: operator
Password:
Backup information success!
```

Example 3

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

```
> enable  Press the Enter key.
# backup mc MCBackup.dat no-software  Press the Enter key.
Backup information to MC (MCBackup.dat).
Copy file to MC...
Backup information success!
```

Display items

None

Impact on communication

None

Response messages

Table 7-10 List of response messages for the backup command

Message	Description
aborted.	File transfer is aborted. DNS request is aborted.
Backup information success!	Backup processing ended successfully.
Backup operation failed.	Backup processing failed.
Can't access to MC by write protection.	Make sure the memory card's protect switch is not set to ▼Lock. If the switch is set to ▼Lock, move it to the opposite side, and then insert the memory card again. Make sure there is no dust in the memory card slot. If there is dust, remove it with a dry cloth and then insert the memory card again.
Can't assign requested address.	The interface of the link-local address is invalid.
Connecting...	Connection to the FTP server is in progress.
Error: Command send failed.	A communication error occurred.
Error: Connect failed.	An attempt to connect to the FTP server failed.
Error: Data accept failed.	A communication error occurred.
Error: Data send failed.	A communication error occurred.
Error: File read failed.	A file could not be read.

Message	Description
Error: Reply receive failed.	A communication error occurred.
MC is not inserted.	A memory card was not inserted.
No address associated with hostname.	The connection to the host could not be established because the address could not be resolved.
Not enough space on device.	The memory card or RAMDISK# capacity is insufficient. # When backing up data to a memory card or FTP server, the RAMDISK is used as a temporary save area. Make sure the RAMDISK is empty. After deleting directories and files on the RAMDISK, execute the command again.
For messages other than those described above, ask the FTP server administrator.	

Notes

- The device information saved by this command can be restored to the Switch by using the `restore` command.
- Do not allow other users to log in while this command is being executed.
- For a backup, the destination memory card must have free capacity of at least 40MB.
- Do not remove or insert the memory card while the `backup mc` command is backing up data to the memory card.
- Before backing up the running configuration, use the `copy` command to copy it to the startup configuration file.
- Specify the file name within the following limits for the number of characters. If the file name is too long, it will not be displayed correctly when the `show mc-file` or `show ramdisk-file` command is executed.

  For the memory card or RAMDISK: Up to 64 characters

  For the FTP server: Up to 1024 characters
- If you execute the `backup` command with the `no-software` parameter specified, also specify the `no-software` parameter when you execute the `restore` command.
- If you want to use login user IDs of 9 or more characters, or passwords of 17 or more characters, see *11. Device Management* in the *Configuration Guide Vol. 1* before executing this command.
- When an FTP server is specified for the backup destination, temporary files *ftpxxxxx* is generated in RAMDISK. If a file with the same name already exists at the destination, it will be deleted.
- To halt execution of this command during the file transfer via FTP, press **Ctrl**+**C**.

restore

Restores the switch information saved to a memory card, RAMDISK, or remote FTP server to the Switch.

Syntax

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

Input mode

Administrator mode

Parameters

{ mc | ramdisk | ftp *<ftp-server>*}

Specifies the location where the image is stored.

mc

Specifies the memory card as the destination.

RAMDISK

Specifies the RAMDISK as the destination.

ftp *<ftp-server>*

Specifies the remote FTP server as the destination. A host name of the server, IPv4 address, IPv6 address, or IPv6 link local unicast address with an interface name (only `fe80::/64`) can be specified in *<ftp-server>*.

<filename>

Specifies the name of a file at the copy source or copy destination.

Specify the file name with 64 or fewer characters for the memory card or RAMDISK. If a file with the same name already exists at the copy destination, it will be overwritten.

For the characters that can be specified, see *Specifiable values for parameters.*

Specify the file name with 1024 or fewer characters for the FTP server.

no-software

No software is restored.

Operation when this parameter is omitted:

Restores all the backup data.

Example 1

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

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

Example 2

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

```
> enable  Press the Enter Key.
# restore ftp 192.168.12.30 MCBackup.dat  Press the Enter Key.
Restore information from 192.168.12.30 (MCBackup.dat).
Copy file from 192.168.12.30...
```

```
Connecting...

Name: operator
Password:
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.

Response messages

Table 7-11 List of response messages for the restore command

Message	Description
aborted.	File transfer is aborted. DNS request is aborted.
Can't assign requested address.	The interface of the link-local address is invalid.
Can't open file.	The specified file could not be opened. Specify the correct file name.
Connecting...	Connection to the FTP server is in progress.
Error: Can't open "ftpxxxxx".	A file could not be opened.
Error: Command send failed.	A communication error occurred.
Error: Connect failed.	An attempt to connect to the FTP server failed.
Error: Data accept failed.	A communication error occurred.
Error: Data receive failed.	A communication error occurred.
Error: File write failed.	Writing to a file failed.
Error: Is a directory "ftpxxxxx".	The `restore ftp` command cannot be executed as the name of directory *ftpxxxxx* exists in the RAMDISK.
Error: Reply receive failed.	A communication error occurred.
Invalid file.	The contents of the specified file are invalid. Specify a valid file.
MC is not inserted.	A memory card was not inserted.
No address associated with hostname.	The connection to the host could not be established because the address could not be resolved.

Message	Description
Not enough space on device.	RAMDISK# capacity is insufficient. # When restoring data from the memory card, the RAMDISK is used as a temporary save area. Make sure the RAMDISK is empty. After deleting directories and files on the RAMDISK, execute the command again.
Restore finished.	The restoration finished.
Restore operation failed.	An attempt to restore the device information failed. After execution of the backup command with `no-software` specified, execution of the `restore` command might cause this message to be displayed. Execute `restore` command with `no-software` specified, also.
Restore software.	The restoration finished. (when `no-software` is not specified)
For messages other than those described above, ask the FTP server administrator.	

Notes

- Do not allow other users to log in while this command is being executed.
- Do not remove or insert the memory card while the `restore mc` command is restoring data from the memory card.
- Specify the file name within the following limits for the number of characters. If the file name is too long, it will not be displayed correctly when the `show mc-file` or `show ramdisk-file` command is executed.

  For the memory card or RAMDISK: Up to 64 characters

  For the FTP server: Up to 1024 characters
- If you want to use login user IDs of 9 or more characters, or passwords of 17 or more characters, see *11. Device Management* in the *Configuration Guide Vol. 1* before executing this command.
- When an FTP server is specified for the image backup destination, temporary files *ftpxxxxx* is generated in RAMDISK. If a file with the same name already exists at the destination, it will be deleted.
- To halt execution of this command during the file transfer via FTP, press **Ctrl**+**C**.

8. Power Saving Functionality

set power-control schedule
show power-control port
show power-control schedule
show power
clear power

set power-control schedule

Sets the startup mode for power saving schedule.

Syntax

```
set power-control schedule {enable | disable}
```

Input mode

User mode and administrator mode

Parameters

{enable | disable}

Sets the startup mode for power saving schedule.

enable

Sets schedule-enabled mode.

disable

Sets schedule-disabled mode.

Operation when this parameter is omitted:

This parameter cannot be omitted.

Example

Set schedule-disabled mode.

```
> set power-control schedule disable
>
```

Display items

None

Impact on communication

None

Response messages

Table 8-1 List of response messages output by the set power-control schedule command

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

Notes

None

show power-control port

Displays the operating status of the port power saving functionality.

Syntax

```
show power-control port
```

Input mode

User mode and administrator mode

Parameters

None

Example

Display the status of port power saving control.

```
> show power-control port

Date 2010/08/04 10:17:58 UTC
Port  status  cool-standby
 0/1  down    applied
 0/2  up      -
 0/3  up      -
 0/4  up      -
 0/5  down    applied
 0/6  up      -
 0/7  up      -
    :     :

>
```

Display items

Table 8-2 Information displayed for the status of port power saving control

Item	Meaning	Displayed detailed information
Port	Port	Interface port number
status	Port state	`up`: Active (normal operating state). `down`: Active (a line failure has occurred). `inact`: The port is blocked.[#1] The following can cause a port to become blocked: ● Operation has been stopped by the `inactivate` command. ● The standby link functionality of link aggregation ● The BPDU guard functionality of a Spanning Tree Protocol ● The storm control functionality ● SML (Split Multi Link) functionality ● Detection of a unidirectional link failure by the UDLD functionality ● The L2 loop detection functionality `dis`: Operation has been stopped by using the `shutdown` or `schedule-power-control shutdown` configuration command.

Item	Meaning	Displayed detailed information
cool-standby	Port power saving functionality operating status	`applied`: The port power saving functionality is operating because of a port in the link-down status or a blocked port.#2 `-`: The port power saving functionality is not operating.#3

#1: `inact` is cleared in the following conditions:

- The port is restored by execution of the `activate` command.

  The BPDU guard functionality of a Spanning Tree Protocol

  The storm control functionality

  SML (Split Multi Link) functionality

  Detection of a unidirectional link failure by the UDLD functionality

  The L2 loop detection functionality. (The automatic restoration functionality can be also used for recovery.)

- The standby link functionality of link aggregation makes the standby port the active port.

#2: Only applies to 10BASE-T, 100BASE-TX, and 1000BASE-T ports.

#3: `-` is displayed in the following conditions:

- The port is in the link-up status.
- For SFP ports and shared SFP/SFP+ ports [10G model]

Impact on communication

None

Response messages

None

Notes

None

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.

Operation 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.

Operation when this parameter is omitted:

The scheduled dates and times for 10 schedules are displayed.

Operation when all parameters are omitted:

Operation proceeds as described for each *Operation when this parameter is omitted* section.

Example

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

```
> show power-control schedule 100801

Date 2010/07/09(Fri) 18:08:07 UTC
Current Schedule Status : Disable
Schedule Power Control Date :
  2010/08/01(Sun) 00:00 UTC  -  2010/08/02(Mon) 06:00 UTC
  2010/08/03(Tue) 00:00 UTC  -  2010/08/03(Tue) 06:00 UTC
  2010/08/04(Wed) 00:00 UTC  -  2010/08/04(Wed) 06:00 UTC
  2010/08/05(Thu) 00:00 UTC  -  2010/08/05(Thu) 06:00 UTC
  2010/08/06(Fri) 00:00 UTC  -  2010/08/06(Fri) 06:00 UTC
  2010/08/06(Fri) 23:00 UTC  -  2010/08/16(Mon) 06:00 UTC
  2010/08/17(Tue) 00:00 UTC  -  2010/08/17(Tue) 06:00 UTC
  2010/08/18(Wed) 00:00 UTC  -  2010/08/18(Wed) 06:00 UTC
```

```
  2010/08/19(Thu) 00:00 UTC  -  2010/08/19(Thu) 06:00 UTC
  2010/08/20(Fri) 00:00 UTC  -  2010/08/20(Fri) 06:00 UTC

>
```

Display items

Table 8-3 Information displayed for the operating status of the scheduling functionality

Item	Meaning	Displayed detailed information
Current Schedule Status :	Power saving schedule status	`Enable`: Power saving is in effect as scheduled. `Enable (force disabled)`: Same as above, except that power saving has been disabled as scheduled. `Disable`: Normal power control is in effect. `Disable (force disabled)`: Same as above, except that power saving is disabled as scheduled.
Schedule Power Control Date :	Scheduled date and time that the power saving schedule is enabled	*<date and time of power saving schedule starts> - <Date and time of power saving schedule ends>* `Infinity` is displayed if the forever (infinity) is set by the schedule settings.

Impact on communication

None

Response messages

None

Notes

- If the end time of power saving schedule is January 18, 2038, 00:00 or later (including when it continues forever), `Infinity` is displayed.
- If this command is executed with no date specified during power saving scheduling, the command execution time will become the start time of the schedule.

show power

Displays power consumption information for a Switch.

Syntax

```
show power
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following shows an example of displaying the operating status.

```
> show power

Date 2010/08/04 09:49:05 UTC
Elapsed time 0days 12:11:44
Current wattage  Accumulated wattage
        73.36 W             0.99 kWh

Power accumulated records
   Wattage     Monitoring date
   72.35 W     2010/08/04 09:37:53 UTC
   73.02 W     2010/08/04 08:37:52 UTC
   73.86 W     2010/08/04 07:37:52 UTC
   73.37 W     2010/08/04 06:37:51 UTC
   72.87 W     2010/08/04 05:37:50 UTC
   71.15 W     2010/08/04 04:37:51 UTC
   71.84 W     2010/08/04 03:37:51 UTC
   73.37 W     2010/08/04 02:37:50 UTC
   73.70 W     2010/08/04 01:37:49 UTC
   72.85 W     2010/08/04 00:37:48 UTC
   73.21 W     2010/08/03 23:37:47 UTC
   70.63 W     2010/08/03 22:37:47 UTC

>
```

Display items

Table 8-4 Item displayed for the power consumption information for a Switch

Item	Displayed information	Displayed detailed information
Elapsed time	Elapsed time	Displays the time elapsed since the Switch started. *ddays hh*:*mm*:*ss* (*d* = days *hh* = hours, *mm* = minutes, *ss* = seconds)
Current wattage	Current power consumption	Unit: [W]
Accumulated wattage	Accumulated power consumption	Unit: [kWh]

Item	Displayed information	Displayed detailed information
Power accumulated records	Past power consumption	Display the power consumption when the switch was started and every following one hour. Maximum of 24 records
Wattage	Monitored power consumption	Unit: [W]
Monitoring date	Monitoring date	*year*/*month*/*day* *hour*:*minute*:*second* *time-zone*

Impact on communication

None

Response messages

None

Notes

The elapsed time is cleared in the following conditions:

- When the switch is turned on/off, or restarted (including sleep mode)
- When the `clear power` command is executed

clear power

Clears the information about the power consumption of the switch.

Syntax

```
clear power
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following shows an example of displaying the operating status.

Clears the information about the power consumption of the switch.

```
> clear power

>
```

Display items

None

Impact on communication

None

Response messages

Table 8-5 List of response messages for the clear power command

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

Notes

None

9. Checking Internal Memory and Memory Cards

format mc
format flash
show mc
show mc-file
show ramdisk
show ramdisk-file

format mc

Initializes formats the memory card for use by the Switch.

Syntax

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

Input mode

User mode and administrator mode

Parameters

-f

Executes the command without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

1. Insert the memory card to be initialized into the slot, and then enter the following command:

   `> format mc` Press the **Enter** key.

2. Display the message asking for confirmation at the start of `format` command execution.

   ```
   Do you wish to initialize memory card? (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 9-1 List of response messages for the format mc command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Can't gain access to MC.	An attempt to access the memory card failed.
MC is not inserted.	A memory card was not inserted.

Message	Description
Can't access to MC by write protection.	Make sure the memory card's protect switch is not set to ▼Lock. If the switch is set to ▼Lock, move it to the opposite side, and then insert the memory card again. Make sure there is no dust in the memory card slot. If there is dust, remove it with a dry cloth and then insert the memory card again.

Notes

Executing this command deletes all the data on the memory card.

format flash

Initializes the internal flash memory file system.

Syntax

```
format flash [-f]
```

Input mode

Administrator mode

Parameters

-f

Executes the command without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

1. Enter the following command:

   `# format flash` Press the **Enter** key.

2. Display the message asking for confirmation at the start of `format` command execution.

   ```
   Do you wish to initialize flash memory?  (y/n): _
   ```

   If `y` is entered, the internal flash memory file system will be initialized.

   If an error occurs, an error message is displayed.

   If `n` is entered, the internal flash memory file system will not be initialized, and you will be returned to administrator mode.

Display items

None

Impact on communication

None

Response messages

Table 9-2 List of response messages for the format flash command

Message	Description
Flash format complete.	Initialization of the internal flash memory file system was completed successfully.
Flash format task not ended. detail=xxxx	Initialization of the internal flash memory file system was not completed. `detail=`*xxxx*: Detailed reason

Message	Description
Flash format system error(1). detail=xxxx	A system error occurred during initialization of the internal flash memory file system. `detail=xxxx`: Detailed reason
Flash format system error(2). detail=xxxx	A system error occurred during initialization of the internal flash memory file system. `detail=xxxx`: Detailed reason
Flash format error. detail=xxxx	Initialization of the internal flash memory file system failed. `detail=xxxx`: Detailed reason

Notes

- When this command is executed, log information is collected even when execution has been successful.
- Executing this command deletes the following information in the internal flash memory file system, and the previous setting is disabled after the switch restarts.

Table 9-3 Switch information saved in internal flash memory

Switch information type	Notes
Startup configuration file	--
Login authentication user ID / Login authentication password	`adduser` operation command `rmuser` operation command `password` operation command
Administrator mode password	`password enable-mode` operation command
Web authentication database	Internal Web authentication DB
Registered HTML files for Web authentication pages (Registered authentication custom file set)	Custom file set of the basic Web authentication page Custom file set of the individual Web authentication page
Web authentication file	--
MAC-based authentication database	Internal MAC-based authentication DB
Presence of lisence	`set license` operation command
Secure Wake on LAN terminal information database	WOL terminal information DB
Secure Wake on LAN user authentication database	WOL user authentication DB

show mc

Displays the memory card format and card usage.

Syntax

```
show mc
```

Input mode

User mode and administrator mode

Parameters

None

Example

```
> show mc

Date 2010/08/06 17:38:24 UTC
    MC : enable
    Manufacture ID : 00000003
       used      7,880,192 byte
       free    118,030,336 byte
       total   125,910,528 byte

>
```

Display items

Table 9-4 Information displayed by the show mc command

Item	Displayed information	Displayed detailed information
MC	Memory card status	`enable`: The memory card can be accessed. `not connect`: The memory card is not installed. `write protect`: Writing to the memory card is not allowed.
Manufacture ID	Type#1	Memory card production ID number
used	Used capacity#1	Capacity in use in the memory card file system
free	Unused capacity#1	Capacity not in use in the memory card file system
total	Total capacity#1	Total of capacity in use and capacity not in use for the memory card file system

#1: Those items are displayed when the memory card status is `enable` or `write protect`.

Impact on communication

None

Response messages

Table 9-5 List of response messages for the show mc command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
MC : not connect	There is no memory card.

Notes

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

show mc-file

Displays the names and sizes of the files on the memory card.

Syntax

```
show mc-file [<Directory name>]
```

Input mode

User mode and administrator mode

Parameters

<Directory name>

Displays the contents of the specified directory.

If a period (`.`) is specified as the directory name, the contents of the current directory are displayed.

Example

- Displaying memory card information

```
> sh mc-file

Date 2010/08/06 17:38:28 UTC
    File Date              Size Name
    2010/08/06 17:21   7,772,160 K.IMG
    2010/08/06 17:35      16,384 Config_File/
    2010/08/06 17:35       6,780 Test_Config.txt
    2010/08/06 17:34       3,163 Config_File/5Floor_Config.txt

>
```

- Specifying a directory name

```
> sh mc-file Config_File

Date 2010/08/06 17:58:28 UTC
    File Date              Size Name
    2010/08/06 17:34       3,163 Config_File/5Floor_Config.txt

>
```

Display items

Table 9-6 Information displayed by the show mc-file command

Item	Displayed information	Displayed detailed information
File Date	Last update date	--
Size	File size	--
Name	File name	No more than 64 characters.

Impact on communication

None

Response messages

Table 9-7 List of response messages for the show mc-file command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command. The directory could not be found. Check the directory.
There is no file. (MC)	There are no files on the memory card.
MC is not inserted.	A memory card was not inserted.
Some files are not listed due to resource limits.	Some files cannot be displayed due to resource limits.

Notes

- Specify the file name with 64 or fewer characters. If the file name is too long, it will not be displayed correctly when the `show mc-file` or `show ramdisk-file` command is executed.
- If you create the configuration file on your PC and save it to the memory card used for operation, specify the file name with 64 or fewer characters.
- If a file name or a directory name (including a path name) exceeds 64 characters, only the fact that the file or directory exists is displayed.
- If the number of the files to be displayed exceeds 512, only 512 files, randomly chosen, are displayed.

show ramdisk

Displays the RAMDISK format and usage.

Syntax

```
show ramdisk
```

Input mode

User mode and administrator mode

Parameters

None

Example

```
> show ramdisk

Date 2010/08/06 17:38:36 UTC
       used       152,576 byte
       free    31,304,704 byte
       total   31,457,280 byte

>
```

Display items

Table 9-8 Information displayed by the show ramdisk command

Item	Displayed information	Displayed detailed information
used	Used capacity	Capacity being used by the RAMDISK file system
free	Unused capacity	Capacity not being used by the RAMDISK file system
total	Total capacity	Total capacity being used and not being used by the RAMDISK file system

Impact on communication

None

Response messages

Table 9-9 List of response messages for the show ramdisk command

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

Notes

None

show ramdisk-file

Displays the names and sizes of the files on the RAMDISK.

Syntax

```
show ramdisk-file [<Directory name>]
```

Input mode

User mode and administrator mode

Parameters

<Directory name>

Displays the contents of the specified directory.

If a period (.) is specified as the directory name, the contents of the current directory are displayed.

Example

- Displaying the RAMDISK information

```
> show ramdisk-file

Date 2010/08/06 17:38:40 UTC
    File Date              Size Name
    2010/08/06 17:37      1,024 Config_File/
    2010/08/06 17:37      6,780 Test_Config.txt
    2010/08/06 17:37      3,163 Config_File/5Floor_Config.txt

>
```

- Specifying a directory name

```
> show ramdisk-file Config_File

Date 2010/08/06 17:58:40 UTC
    File Date              Size Name
    2010/08/06 17:37      3,163 Config_File/5Floor_Config.txt

>
```

Display items

Table 9-10 Information displayed by the show ramdisk-file command

Item	Displayed information	Displayed detailed information
File Date	Last update date	--
Size	File size	--
Name	File name	No more than 64 characters.

Impact on communication

None

Response messages

Table 9-11 List of response messages for the show ramdisk-file command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command. The directory could not be found. Check the directory.
There is no file. (RAMDISK)	There is no file on the RAMDISK.
Some files are not listed due to resource limits.	Some files cannot be displayed due to resource limits.

Notes

- Specify the file name with 64 or fewer characters. If the file name is too long, it will not be displayed correctly when the `show mc-file` or `show ramdisk-file` command is executed.
- If a file name or a directory name (including a path name) exceeds 64 characters, only the fact that the file or directory exists is displayed.
- If the number of the files to be displayed exceeds 512, only 512 files, randomly chosen, are displayed.

10. Log

show logging
clear logging
show logging console
set logging console
show critical-logging
show critical-logging summary
clear critical-logging

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 to be displayed as the command execution result, see *1.2 Checking the log* in *the manual Message and Log Reference*.

Syntax

```
show logging [<kind>] [<command classification>] [search <string>]
```

Input mode

User mode and administrator mode

Parameters

<kind>

reference

Specifies the reference log.

Operation when this parameter is omitted:

Specifies the operation log.

<command classification>

-h

Displays log entries with no header information (`System Information`). `System Information` indicates the device model and software information.

Operation when this parameter is omitted:

Log entries with header information (`System Information`) are displayed.

search *<string>*

Specifies the search string.

If you specify this parameter, the operation or reference log messages that includes the search string are displayed.

Specify the string with 1 to 64 characters. The characters are case sensitive. For details, see *Any character string* in *Specifiable values for parameters*.

Operation when this parameter is omitted:

All the operation or reference log messages are displayed.

Operation when all parameters are omitted:

Operation proceeds as described for each *Operation when this parameter is omitted* section.

Example 1

- Display the operation log entries for the switch when the parameter is omitted.

  `> show logging` Press the **Enter** key.

Figure 10-1 Operation log display (when the parameters are omitted)

```
> show logging

Date 2011/03/29 14:55:50 UTC
System Information
```

```
    AX2530S-48T, OS-L2B, Ver. x.x (Build:yy)#
Logging Information
KEY 03/29 14:55:50 console:show logging
KEY 03/29 14:55:43 console:set terminal pager disable
KEY 03/29 14:55:36 console:enable
EVT 03/29 14:55:31 E3 SESSION 00e02003 Login operator from console.
EVT 03/29 14:55:27 E4 VLAN 00700001 VLAN (1210) Status is Up.
EVT 03/29 14:55:27 E4 VLAN 00700001 VLAN (1209) Status is Up.
EVT 03/29 14:55:27 E4 PORT GigabitEthernet0/43 01e32001 Port up.
EVT 03/29 14:55:27 E4 PORT GigabitEthernet0/2 01e32001 Port up.
EVT 03/29 14:55:27 E4 VLAN 00700001 VLAN (1) Status is Up.
EVT 03/29 14:55:27 E4 PORT GigabitEthernet0/41 01e32001 Port up.
EVT 03/29 14:55:27 E4 PORT GigabitEthernet0/1 01e32001 Port up.
EVT 03/29 14:55:24 E4 SFP GigabitEthernet0/49 02400001 Transceiver not connected.
EVT 03/29 14:55:24 E4 SFP GigabitEthernet0/50 02400001 Transceiver not connected.
EVT 03/29 14:55:24 E4 SFP GigabitEthernet0/51 02400001 Transceiver not connected.
EVT 03/29 14:55:24 E4 SFP GigabitEthernet0/52 02400001 Transceiver not connected.
EVT 03/29 14:55:23 E4 VLAN 0070010a L2LD : L2loop detection frame cannot be sent in
the port where capacity was exceeded.
EVT 03/29 14:55:21 E4 STP 00100039 : Exceeded the number of the maximum spanning tree.

                     :

>
```

- Display the operation log entries for the switch when the parameter is specified.

  `> show logging search up` Press the **Enter** key.

Figure 10-2 Operation log display (when the parameters are specified)

```
> show logging search up

Date 2011/03/29 14:56:33 UTC
System Information
    AX2530S-48T, OS-L2B, Ver. x.x (Build:yy)#
Logging Information
KEY 03/29 14:56:33 console:show logging search up
EVT 03/29 14:55:27 E4 PORT GigabitEthernet0/43 01e32001 Port up.
EVT 03/29 14:55:27 E4 PORT GigabitEthernet0/2 01e32001 Port up.
EVT 03/29 14:55:27 E4 PORT GigabitEthernet0/41 01e32001 Port up.
EVT 03/29 14:55:27 E4 PORT GigabitEthernet0/1 01e32001 Port up.
KEY 03/29 14:52:13 console:show logging search up
EVT 03/29 14:51:51 E4 PORT GigabitEthernet0/43 01e32001 Port up.
EVT 03/29 14:51:51 E4 PORT GigabitEthernet0/41 01e32001 Port up.
EVT 03/29 14:51:51 E4 PORT GigabitEthernet0/2 01e32001 Port up.
EVT 03/29 14:51:51 E4 PORT GigabitEthernet0/1 01e32001 Port up.

 10 events matched.

>
```

- Display the reference log entries for the switch.

  `> show logging reference search E3` Press the **Enter** key.

Figure 10-3 Reference log display

```
> show logging reference search E3

Date 2011/03/29 14:56:46 UTC
System Information
    AX2530S-48T, OS-L2B, Ver. x.x (Build:yy)#
Logging Information
E3 SVP 03900000
  03/29 14:55:01    03/29 14:51:25    2
```

```
E3 SESSION 00e02003
  03/29 14:55:31    03/29 14:51:53    2

 2 events matched.

>
```

#: x.x: Software version, yy: Build version

Display items

None

Impact on communication

None

Response messages

Table 10-1 List of response messages for the show logging command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no logging data.	There is no log data.
There is no log data to match.	Log data matching the specified character string could not be found.

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). 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.
- If you execute this command with the `search` parameter set and if information that matches the specified character string is found, the number of matched events is displayed at the end.

  Example: 3 events matched.

clear logging

Erases the operation log entries recorded by the Switch.

Syntax

```
clear logging [<kind>]
```

Input mode

User mode and administrator mode

Parameters

<kind>

reference

Specifies the reference log.

Operation when this parameter is omitted:

Specifies the operation log.

Example

- Clear the operation log entries.

  `> clear logging` Press the **Enter** key.

- Clear the reference log entries.

  `> clear logging reference` Press the **Enter** key.

Display items

None

Impact on communication

None

Response messages

Table 10-2 List of response messages for the clear logging command

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

Notes

None

show logging console

Shows the contents (event level suppressing the display) set by the `set logging console` command.

Syntax

```
show logging console
```

Input mode

User mode and administrator mode

Parameters

None

Example

- Indicate that all the system messages are set to be displayed.

  `> show logging console` Press the **Enter** key.

  ```
  System message mode : Display all
  ```

- Indicate that system messages whose event level is E6 or less are prevented from being displayed.

  `> show logging console` Press the **Enter** key.

  ```
  System message mode : E6
  ```

Display items

None

Impact on communication

None

Response messages

Table 10-3 List of response messages for the show logging console command

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

Notes

None

set logging console

Controls the display of system messages by event level. Low priority system 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); messages related to events at this specified level and lower levels will not be displayed.

enable

Specifies that all system messages will be displayed.

Example

- Specify that all system messages be displayed.

  ```
  > set logging console enable
  ```
  Press the **Enter** key.

- Specify that system messages whose event level is E5 or less not be displayed.

  ```
  > set logging console disable E5
  ```
  Press the **Enter** key.

Display items

None

Impact on communication

None

Response messages

Table 10-4 List of response messages for the set logging console command

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

Notes

None

show critical-logging

Displays the detailed information regarding device failure log data as log records.

Syntax

```
show critical-logging [<log#>] [ramdisk]
```

Input mode

User mode and administrator mode

Parameters

<log#>

Specifies the number of the log record at which display of the detailed information begins.

The specifiable values are from 1 to 127.

Operation when this parameter is omitted:

Log records starting from log number 1 are displayed.

ramdisk

Directly save the information to the RAMDISK without displaying it on the console screen.

The file `log.txt` is generated for the information saved on the RAMDISK.

Operation when this parameter is omitted:

Information is displayed on the screen, but is not saved to the RAMDISK.

Example

Figure 10-4 Displaying device failure log entries

```
> show critical-logging

Date 2012/08/07 17:07:15 UTC
```

(Displayed data is for analysis by the manufacturer)

Display items

None

Impact on communication

None

Response messages

Table 10-5 List of response messages for the show critical-logging command

Message	Description
Can't execute.	The command could not be executed. After deleting directories and files on the RAMDISK, execute the command again.
No Log data.	There is no log information.

Message	Description
Not enough space on device.	Capacity at the write destination is insufficient.

Notes

Before executing the `show critical-logging ramdisk` command, make sure there are no directories and files on the RAMDISK. If there are any directories or files on the RAMDISK, we recommend that you delete those files before executing this command.

show critical-logging summary

Displays a list of device failure log entries in reference code format.

Syntax

```
show critical-logging summary
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 10-5 Displaying a list of device failure log references

```
> show critical-logging summary

Date 2012/08/07 17:07:08 UTC
```

(Displayed data is for analysis by the manufacturer)

Display items

None

Impact on communication

None

Response messages

Table 10-6 List of response messages for the show critical-logging summary command

Message	Description
No Log data.	There is no log information.

Notes

Log information is obtained at the UTC time immediately after the device is started.

clear critical-logging

Clears the device failure log entries recorded by the Switch.

Syntax

```
clear critical-logging [-f]
```

Input mode

User mode and administrator mode

Parameters

-f

Executes the command without displaying a confirmation message.
Operation when this parameter is omitted:
A confirmation message is displayed.

Example

1. Clear the device failure log entries.

   `> clear critical-logging` Press the **Enter** key.

2. A confirmation message is displayed.

   ```
   Do you wish to clear critical-logging? (y/n): _
   ```

   If `y` is entered, the device failure log entries are cleared

   If `n` is entered, the device failure log entries are not cleared.

Display items

None

Impact on communication

None

Response messages

None

Notes

None

11. Software Management

ppupdate
set license
show license
erase license

ppupdate

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

Syntax

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

Input mode

Administrator mode

Parameters

test

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

no-display

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

-f

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

Operation 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.

ramdisk *<File name>*

Specifies the update file name.

Specify the file name with 64 or fewer characters. The file name is not case sensitive.

For the characters that can be specified, see *Specifiable values for parameters.*

Example

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

```
# ppupdate ramdisk k.img

Software update start

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

old version a.a (Build:xx)    <- Displays the old version.
new version b.b (Build:yy)    <- Displays the new version.


Automatic reboot process will be run after installation process.
Do you wish to continue? (y/n): _
```

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 returns you to administartor mode without starting update processing.

Display items

None

Impact on communication

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

Response messages

Table 11-1 List of response messages for the ppupdate command

Message	Description
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.
Can't support hardware model.	The specified file does not support this switch.
Can't update software. [Hardware rev.x]	The specified update file cannot be used for the update.
Flash memory write failed.	Writing to flash memory failed.
Invalid file (<*File name*>).	The contents of the specified file are invalid. Specify a valid file.
OS Type mismatch. Can't apply this package.	The specified file cannot be used because it is intended for a different device.
There is not OS File.	There is no OS file (when the `ramdisk` <*File name*> parameter is omitted).

Notes

- When updating is performed, the configuration in effect before the update is inherited. However, only the configuration commands that can be recognized by the new software version can be skipped or inherited. The skipped configuration commands are output to the operation log. For details, see *2.1 Configuration* in the manual *Message and Log Reference*.
- Before executing the `ppupdate` command, make sure the memory card is not inserted into the Switch. If the memory card is inserted, remove it, and then execute the `ppupdate` command.
- If you want to use login user IDs of 9 or more characters, or passwords of 17 or more characters, see the *Software Update Guide* before executing this command.

set license

Registers a license key code or license key file on the Switch.

After the Switch is restarted, the function covered by the license can be used.

Syntax

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

Input mode

Administrator mode

Parameters

key-code *<License key>*

Specify the license key code to be registered.

You can specify a maximum of 39 alphanumeric characters and hyphens (-).

The alphabetic characters used in a license key are case sensitive.

key-file ramdisk *<File name>*

Specify the name of the license key file to be registered.

You can specify a maximum of 64 alphanumeric characters.

Alphabetic characters used in a file name are case sensitive.

Example

- Specifying a license key (In this example, `0123-4567-89ab-cdef-0123-4567-89ab-cdef` is specified as a license key)

  Specify the license key code to be registered.

  ```
  # set license key-code 0123-4567-89ab-cdef-0123-4567-89ab-cdef
  ```

  Specify the license key code without hyphens.

  ```
  # set license key-code 0123456789abcdef0123456789abcedf
  ```

- Specifying a license key (In this example, the file `addopt.dat` is specified as a license key file)

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

Display items

None

Impact on communication

None

Response messages

Table 11-2 List of response messages for the set license command

Message	Description
Invalid license key.	The license key is invalid.
There is no corresponding function.	The function corresponding to the license key was not found.
This license is already registered.	The license key is already registered.
A license key cannot be added any more.	The area for registering license keys is full.
Error: String too long.	The specified license key code exceeds the maximum allowed length. The specified license key file name exceeds the maximum allowed length.
It failed in writing the FROM file.	Writing of the file to internal flash memory failed.
File open error.	When an license key file was specified, the specified file could not be opened.
Invalid contents of *<File name>*.	When a license key file was specified, the license key set in the file contained inappropriate information.

Notes

- This command cannot be used concurrently by multiple users.
- If a license key has been set by using this command, the target function can be used after the Switch has been restarted.
- To use a license key file, the file must be transferred to the RAMDISK of the Switch from a memory card (SD card) or via FTP beforehand. Note, however, that restarting the Switch deletes the file because the RAMDISK is only a temporary storage area.

show license

Displays information about the licenses registered on the Switch.

Syntax

```
show license
```

Input mode

User mode and administrator mode

Parameters

None

Example

An example of displaying authorized licenses is described below:

- When information is displayed:

```
> show license

Date 2010/08/05 01:23:29 UTC
  Available: OS-L2A-U
    Serial Number        Licensed software
    0123-4567-89ab-cdef  OS-L2A-U(AX-P2530-22AU)

>
```

- When information is not displayed:

```
> show license

Date 2010/08/05 15:33:23 UTC
  Available: -----
    ----------------

>
```

Display items

Table 11-3 Information displayed by the show license command

Item	Displayed information	Displayed detailed information
Available:	Name of a license that takes effect	`-----` is displayed when no license exists.
Serial Number	Specified license serial number	--

Item	Displayed information	Displayed detailed information
Licensed software	Abbreviated name of purchased software. (The model name is enclosed in parentheses.)	--

Impact on communication

None

Response messages

None

Notes

This command cannot be used concurrently by multiple users.

erase license

Deletes a license registered on the Switch by specifying its serial number.

After the Switch has been restarted, the deleted license is no longer valid.

Syntax

```
erase license <Serial#>
```

Input mode

Administrator mode

Parameters

<Serial#>

Specifies the serial number of the license key code to be deleted.

You can specify a maximum of 19 alphanumeric characters and hyphens (-).

The alphabetic characters used in a serial number are case sensitive.

Example

List license names included in the specified serial number and display a confirmation message.

```
# erase license 0123-4567-89ab-cdef
This serial number enable OS-L2A-U
Erase OK ? (y/n): y
#
```

Display items

None

Impact on communication

None

Response messages

Table 11-4 List of response messages for the erase license command

Message	Description
Invalid serial number.	The serial number is invalid.
There is no corresponding serial number.	There are no entries that correspond to the specified serial number.
It failed in writing the FROM file.	Writing of the information to internal flash memory failed.
Error: String too long.	The specified serial number exceeds the maximum allowed length.

Notes

- This command cannot be used concurrently by multiple users.
- If a license is deleted by using this command, the target function can no longer be used after restarting of the Switch.

12. Resource Information

show cpu
show memory summary

show cpu

Shows CPU usage.

Syntax

```
show cpu [days][hours][minutes][seconds]
```

Input mode

User mode and administrator mode

Parameters

days

Displays statistics collected daily. Statistics for the past 31 days 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.

Operation 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.

Operation when all parameters are omitted:

Displays statistics collected for a 5-second period. Statistics are overwritten every 5 seconds.

Example

Figure 12-1 Example of displaying information when all the parameters are specified

```
> show cpu days hours minutes seconds

Date 2010/08/12 09:31:56 UTC
*** Days ***
                                          0   25   50   75  100[%]
Date  Time              CPU average CPU peak +----+----+----+----+
03/03 11:26:22-23:59:59          12      100  ***                P
03/04 00:00:00-23:59:59          18      100  ****               P
  :
03/10 00:00:00-23:59:59          12      100  ***                P
03/11 00:00:00-23:59:59          12      100  ***                P

*** Hours ***
                                          0   25   50   75  100[%]
Date  Time              CPU average CPU peak +----+----+----+----+
03/11 09:00:00-09:59:59          12      100  ***                P
03/11 10:00:00-10:59:59          12      100  ***                P
  :
03/12 07:00:00-07:59:59          12      100  ***                P
03/12 08:00:00-08:59:59          12      100  ***                P
Date  Time              CPU average CPU peak +----+----+----+----+
```

```
*** Minutes ***
                                          0   25   50   75  100[%]
Date  Time              CPU average CPU peak +----+----+----+----+
03/12 08:31:00-08:31:59          12       94  ***                P
03/12 08:32:00-08:32:59          10       89  **                P
  :
03/12 09:29:00-09:29:59          12       84  ***              P
03/12 09:30:00-09:30:59          11       57  ***        P
Date  Time              CPU average CPU peak +----+----+----+----+

*** Seconds ***
Date  Time              CPU average
03/12 09:30:56-09:31:05   0   0  11   5  26   5  11   5   0  21
03/12 09:31:06-09:31:15  16  10   5   5   0  31   5   5   5   5
03/12 09:31:16-09:31:25  31   5   5   0   0  26   5  68  84   5
03/12 09:31:26-09:31:35  44  31   5   5   5   5  31   5   0   0
03/12 09:31:36-09:31:45  21  78  22  10  15  15  27  15   5   5
03/12 09:31:46-09:31:55   5   5  31   5   5   0   0  31   5  10

>
```

Figure 12-2 Example of displaying information when all the parameters are omitted

```
> show cpu

Date 2010/08/12 09:32:25 UTC
*** Current ***
                                    0   25   50   75  100[%]
Date  Time              CPU average +----+----+----+----+
03/12 09:32:34-09:32:38          33  *******       <- overwritten every 5 seconds.

>
```

To end command execution, press the **Ctrl** + **C** key combination.

Display items

Table 12-1 CPU usage display items

Item	Meaning	Displayed detailed information
CPU average	Average CPU utilization	The average CPU utilization, expressed as a percentage, within the time range indicated under `Time`. # If `seconds` is specified, CPU utilization by the second is displayed.
CPU peak	Peak CPU utilization	Peak CPU utilization, expressed as a percentage, within the time range indicated under `Time`.
Graph display of CPU utilization		
*	Average CPU utilization	The average CPU utilization is displayed in a graph. Utilization is displayed in 5% increments (a value less than 5% is rounded up to 5%).
P	Peak CPU utilization	Peak CPU utilization is displayed in a graph.

Impact on communication

None

Response messages

None

Notes

- Statistics are cleared if the device is restarted, the time zone is changed, or the device enters sleep mode.
- If the time is changed by using the `set clock` command or the NTP client, only the statistics collected by the second and every 5 seconds are cleared.

show memory summary

Displays the installed capacity, used capacity, and free capacity of the device's physical memory.

Syntax

```
show memory summary
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 12-3 Example of displaying memory information

```
> show memory summary

Date 2010/11/16 16:27:04 UTC

    Physical memory = 524288KB(512.00MB)
    Used     memory = 275400KB(268.94MB)
    Free     memory = 248887KB(243.05MB)

>
```

Display items

Table 12-2 Display items of memory information

Item	Displayed information
Physical memory	Displays the installed capacity of physical memory.
Used memory	Displays the used capacity of physical memory.
Free memory	Displays the free capacity of physical memory.

Impact on communication

None

Response messages

None

Notes

None

13. Ethernet

show interfaces
clear counters
show port
activate
inactivate
test interfaces
no test interfaces

show interfaces

Displays information about an Ethernet interface.

Syntax

```
show interfaces {gigabitethernet <IF#> | tengigabitethernet <IF#>} [detail]
```

Input mode

User mode and administrator mode

Parameters

{gigabitethernet <*IF#*> | tengigabitethernet <*IF#*>}

gigabitethernet

Specifies an Ethernet interface with a maximum line speed of 1 Gbit/s.

tengigabitethernet

Specifies an Ethernet interface with a maximum line speed of 10 Gbit/s.

<*IF#*>

Specify an interface port number. For the specifiable range of values, see *Specifiable values for parameters*.

detail

Displays detailed statistics.

Operation when this parameter is omitted:

Detailed statistics are not displayed.

Example 1

The following shows an example of displaying the 10BASE-T/100BASE-TX /1000BASE-T, 100BASE-FX and 1000BASE-X interface information and the detailed port information.

Figure 13-1 Result of executing the command for displaying information about the specified 10BASE-T/100BASE-TX/1000BASE-T interface

```
> show interfaces gigabitethernet 0/2

Date 2010/08/04 15:02:35 UTC

Port 0/2 : active up  1000BASE-T full(auto)  00eb.f103.0102                  <-1
        Time-since-last-status-change: 1day 15:29:39                         ⎫
        Bandwidth: 9999999kbps  Average out: 0Mbps  Average in: 0Mbps        |
        Peak out: 0Mbps at 00:00:00  Peak in: 0Mbps at 00:00:00              |
        Output rate:           0bps           0pps                           |
        Input  rate:           0bps           0pps                          |2
        Flow control send   : off                                           |
        Flow control receive: off                                           |
        TPID: 8100                                                          |
        Frame size: 9234 Octets   Interface name: geth0/2                   |
        Description:                                                        ⎭
       <Out octets/packets counter>       <In octets/packets counter>       ⎫
        Octets      :           966662824  Octets      :           928107200|
        All packets :            14822498  All packets :            14501675|
        Multicast packets     :     27143  Multicast packets     :         0|3
        Broadcast packets     :  14350422  Broadcast packets     :  14501675|
        Pause packets         :         0  Pause packets         :         0⎭
       <Out line error counter>                                              ⎫
        Late collision        :         0  Defer indication      :         0|
```

```
        Single collision      :         0  Excessive deferral    :         0|4
        Multiple collisions   :         0  Excessive collisions  :         0|
        Error frames          :         0                                   |
       <In line error counter>                                              |
        CRC errors            :         0  Symbol errors         :         0|
        Alignment             :         0  Fragments             :         0|5
        Short frames          :         0  Jabber                :         0|
        Long frames           :         0  Error frames          :         0|
       <Line fault counter>                                                 |6
        Link down             :         0                                   |

>
```

Figure 13-2 Execution result when 100BASE-FX/1000BASE-X is specified

```
> show interfaces gigabitethernet 0/1

Date 2010/08/04 13:02:35 UTC
Port 0/1 : active up  1000BASE-LX full(auto)  00eb.f103.0131                  <-1
        SFP connect                                                         |
        Time-since-last-status-change: 00:51:47                             |
        Bandwidth: 9999999kbps  Average out: 0Mbps  Average in: 0Mbps       |
        Peak out: 0Mbps at 00:00:00  Peak in: 0Mbps at 00:00:00             |
        Output rate:           0bps           0pps                          |2
        Input  rate:           0bps           0pps                          |
        Flow control send   : on                                           |
        Flow control receive: on                                           |
        TPID: 8100                                                         |
        Frame size: 9234 Octets   Interface name: geth0/1                  |
        Description:                                                       |
       <Out octets/packets counter>       <In octets/packets counter>      |
        Octets      :          4748794912  Octets      :           531434496|
        All packets :             8282344  All packets :             6066780|3
        Multicast packets     :    453086  Multicast packets     :     63829|
        Broadcast packets     :   6101650  Broadcast packets     :   3073102|
        Pause packets         :    103186  Pause packets         :   2698205|
       <Out line error counter>                                            |
        Late collision        :         0  Defer indication      :         0|
        Single collision      :         0  Excessive deferral    :         0|4
        Multiple collisions   :         0  Excessive collisions  :         0|
        Error frames          :         0                                   |
       <In line error counter>                                             |
        CRC errors            :         0  Symbol errors         :         0|
        Fragments             :         0  Short frames          :         0|5
        Jabber                :         0  Long frames           :         0|
        Error frames          :         0                                   |
       <Line fault counter>                                                |6
        Link down             :         1                                   |

>
```

1. Summary port information
2. Detailed port information
3. Send and receive statistics
4. Send error statistics
5. Receive error statistics
6. Failure statistics

Example 2

The following shows an example of displaying the 10BASE-T/100BASE-TX /1000BASE-T, 100BASE-FX and 1000BASE-X interface information, the detailed port information, and the

detailed statistics.

Figure 13-3 Execution results for the specification of 10BASE-T/100BASE-TX/1000BASE-T detailed statistics

```
> show interfaces gigabitethernet 0/2 detail

Date 2010/08/04 15:22:35 UTC
Port 0/2 : active up  1000BASE-T full(auto)  00eb.f103.0102                  <-1
        Time-since-last-status-change: 1day 15:29:39                          ┐
        Bandwidth: 9999999kbps  Average out: 0Mbps  Average in: 0Mbps         |
        Peak out: 0Mbps at 00:00:00  Peak in: 0Mbps at 00:00:00               |
        Output rate:           0bps           0pps                            |
        Input  rate:           0bps           0pps                           |2
        Flow control send   : off                                             |
        Flow control receive: off                                             |
        TPID: 8100                                                            |
        Frame size: 9234 Octets   Interface name: geth0/2                     |
        Description:                                                          ┘
       <Out octets/packets counter>       <In octets/packets counter>         ┐
        Octets      :           966662824  Octets      :           928107200|
        All packets :            14822498  All packets :            14501675|
        Multicast packets     :    27143  Multicast packets     :         0|
        Broadcast packets     :  14350422  Broadcast packets     :  14501675|
        Pause packets         :         0  Pause packets         :         0|
        64 packets            :         3  64 packets            :        96|3
        65-127 packets        :         4  65-127 packets        :         0|
        128-255 packets       :         0  128-255 packets       :         0|
        256-511 packets       :         0  256-511 packets       :         0|
        512-1023 packets      :         0  512-1023 packets      :         0|
        1024-1518 packets     :         0  1024-1518 packets     :         0┘
       <Out line error counter>                                               ┐
        Late collision        :         0  Defer indication      :         0|
        Single collision      :         0  Excessive deferral    :         0|4
        Multiple collisions   :         0  Excessive collisions  :         0|
        Error frames          :         0                                     ┘
       <In line error counter>                                                ┐
        CRC errors            :         0  Symbol errors         :         0|
        Alignment             :         0  Fragments             :         0|5
        Short frames          :         0  Jabber                :         0|
        Long frames           :         0  Error frames          :         0┘
       <Line fault counter>                                                   ┐6
        Link down             :         0                                     ┘

>
```

Figure 13-4 Execution result when detailed statistics for 100BASE-FX/1000BASE-X are specified

```
> show interfaces gigabitethernet 0/1 detail

Date 2010/08/04 13:12:35 UTC
Port 0/1 : active up  1000BASE-LX full(auto)  00eb.f103.0131                  <-1
        SFP connect                                                           ┐
        Time-since-last-status-change: 00:51:47                               |
        Bandwidth: 9999999kbps  Average out: 0Mbps  Average in: 0Mbps         |
        Peak out: 0Mbps at 00:00:00  Peak in: 0Mbps at 00:00:00               |
        Output rate:           0bps           0pps                           |2
        Input  rate:           0bps           0pps                           |
        Flow control send   : on                                              |
        Flow control receive: on                                              |
        TPID: 8100                                                            |
        Frame size: 9234 Octets   Interface name: geth0/1                     |
        Description:                                                          ┘
       <Out octets/packets counter>       <In octets/packets counter>         ┐
```

```
 Octets      :          4748794912  Octets      :           531434496|
 All packets :             8282344  All packets :             6066780|
 Multicast packets     :    453086  Multicast packets     :     63829|
 Broadcast packets     :   6101650  Broadcast packets     :   3073102|
 Pause packets         :    103186  Pause packets         :   2698205|
 64 packets            :         2  64 packets            :        96|3
 65-127 packets        :         3  65-127 packets        :         0|
 128-255 packets       :         0  128-255 packets       :         0|
 256-511 packets       :         0  256-511 packets       :         0|
 512-1023 packets      :         0  512-1023 packets      :         0|
 1024-1518 packets     :         0  1024-1518 packets     :         0┘
<Out line error counter>                                            ┐
 Late collision        :         0  Defer indication      :         0|
 Single collision      :         0  Excessive deferral    :         0|4
 Multiple collisions   :         0  Excessive collisions  :         0|
 Error frames          :         0                                   ┘
<In line error counter>                                             ┐
 CRC errors            :         0  Symbol errors         :         0|
 Fragments             :         0  Short frames          :         0|5
 Jabber                :         0  Long frames           :         0|
 Error frames          :         0                                   ┘
<Line fault counter>                                                ┐6
 Link down             :         1                                   ┘

>
```

1. Summary port information
2. Detailed port information
3. Send and receive statistics
4. Send error statistics
5. Receive error statistics
6. Failure statistics

Display items in Example 1 and 2

The following shows an example of displaying the 10BASE-T/100BASE-TX/1000BASE-T, 100BASE-FX, and 1000BASE-X interface information, the detailed port information, and detailed statistics.

Table 13-1 Display of summary information for 10BASE-T/100BASE-TX/1000BASE-T, 100BASE-FX, and 1000BASE-X

Item	Displayed information	
	Detailed information	**Meaning**
Port*<IF#>*	Port number	
<port status>	active up	Active (normal operating state)
	active down	Active (A line failure occurred.)
	initialize	Currently initializing
	test	A line test is in progress.
	fault	Failed

Item	Displayed information	
	Detailed information	**Meaning**
	Inactive[#1]	The port is blocked. The following can cause a port to become blocked: ● Operation has been stopped by the `inactivate` command. ● The standby link functionality of link aggregation ● The BPDU guard functionality of the Spanning Tree Protocol ● The storm control functionality ● SML (Split Multi Link) functionality ● Detection of a unidirectional link failure by the UDLD functionality ● The L2 loop detection functionality
	disable	Operation was stopped by using the `shutdown` or `schedule-power-control shutdown` configuration commands.
<line type>	10BASE-T half	10BASE-T half duplex
	10BASE-T half(auto)	10BASE-T half duplex (Line type determined by auto-negotiation.)
	10BASE-T full	10BASE-T full duplex
	10BASE-T full(auto)	10BASE-T full duplex (Line type determined by auto-negotiation.)
	100BASE-TX half	100BASE-TX half duplex
	100BASE-TX half(auto)	100BASE-TX half duplex (Line type determined by auto-negotiation.)
	100BASE-TX full	100BASE-TX full duplex
	100BASE-TX full(auto)	100BASE-TX full duplex (Line type determined by auto-negotiation.)
	1000BASE-T full(auto)	100BASE-T full duplex (Line type determined by auto-negotiation.)
	100BASE-FX full [24S4X][24S4XD]	100BASE-FX full duplex

Item	Displayed information	
	Detailed information	**Meaning**
	1000BASE-LX full	1000BASE-LX full duplex
	1000BASE-SX full	1000BASE-SX full duplex
	1000BASE-SX2 full	1000BASE-SX2 full duplex
	1000BASE-LH full	1000BASE-LH full duplex
	1000BASE-LHB full	1000BASE-LHB full duplex
	1000BASE-LX full(auto)	1000BASE-LX full duplex (Line type determined by auto-negotiation.)
	1000BASE-SX full(auto)	1000BASE-SX full duplex (Line type determined by auto-negotiation.)
	1000BASE-SX2 full(auto)	1000BASE-SX2 full duplex (Line type determined by auto-negotiation.)
	1000BASE-LH full(auto)	1000BASE-LH full duplex (Line type determined by auto-negotiation.)
	1000BASE-LHB full(auto)	1000BASE-LHB full duplex (Line type determined by auto-negotiation.)
	1000BASE-BX10-D full	1000BASE-BX-D (10 km) full duplex
	1000BASE-BX10-U full	1000BASE-BX-U (10 km) full duplex
	1000BASE-BX40-D full	1000BASE-BX-D (40 km) full duplex
	1000BASE-BX40-U full	1000BASE-BX-U (40 km) full duplex
	1000BASE-BX10-D full(auto)	1000BASE-BX-D (10 km) full duplex (Line type determined by auto-negotiation.)
	1000BASE-BX10-U full(auto)	1000BASE-BX-U (10 km) full duplex (Line type determined by auto-negotiation.)
	1000BASE-BX40-D full(auto)	1000BASE-BX-D (40 km) full duplex (Line type determined by auto-negotiation.)
	1000BASE-BX40-U full(auto)	1000BASE-BX-U (40 km) full duplex (Line type determined by auto-negotiation.)

Item	Displayed information	
	Detailed information	**Meaning**
	-	The line type is unknown. A hyphen (-) is displayed in the following cases: ● The port status is not `active up`.
<MAC address>	MAC address of the port	
<type of transceiver> #2	SFP	SFP
<transceiver status> #2	connect	Installed
	not connect	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 the `initialize` status. ● A port is in the `fault` status.

Table 13-2 Display of the detailed information and statistics for a 10BASE-T/100BASE-TX/1000BASE-T, 100BASE-FX, and 1000BASE-X

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) *ddays*`.`*hh*`:`*mm*`:`*ss* (when the elapsed time is more than 24 hours:*d* = 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>*`bps`	Displays the average bandwidth (in bps) 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	

Item	Displayed information	
	Detailed information	**Meaning**
	header and ends with the FCS field.	
`Average in:`*<average bandwidth used on receiving side>*`bps`	Displays the average bandwidth (in bps) used on the receiving side of the line for the one minute interval before the command was executed. `0 Mbps` is displayed if there is no communication (when not even 1 bit of data is transferred). `1 Mbps` is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place. The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.	
Peak out	Displays the maximum bandwidth used on the sending side of the line for the 24-hour interval before the command was executed, and the relevant time. `0 Mbps` is displayed if there is no communication (when not even 1 bit of data is transferred). `1 Mbps` is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place. The relevant time is the last time the bandwidth reached its maximum value. 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 relevant time is the last time the bandwidth reached its maximum value. The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.	
Output rate[#3]	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[#3]	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[#4]	on	A pause packet is sent.
	off	A pause packet is not sent.
Flow control receive[#4]	on	A pause packet is received.

Item		Displayed information	
		Detailed information	**Meaning**
		off	A pause packet is not received.
TPID		Displays a `TagProtocolIDentifier` value that is used on the port to identify the VLAN.	
Frame size[#5]		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/PAD field. For details about frame formats, see the description of frame formats in *14.1.3 Control on the MAC and LLC sublayers* in the *Configuration Guide Vol. 1*.	
Interface name		Displays the name of the interface assigned to the 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.	
Statistics	Category	<Out octets/packets counter>	Send statistics
		<In octets/packets counter>	Receive statistics
		<Out line error counter>	Send error statistics
		<In line error counter>	Receive error statistics
		<Line fault counter>	Failure statistics
		<Uplink redundant>	Uplink redundancy statistics[#9]
	Detailed statistical items for sending and receiving	Octets	The number of octets
		All packets	Number of packets (including error packets)
		Multicast packets	Number of multicast packets
		Broadcast packets	Number of broadcast packets
		Pause packets	Number of pause packets
		64 packets	Number of 64-octet packets[#6]
		65-127 packets	Number of 65-to-127-octet packets[#6]
		128-255 packets	Number of 128-to-255-octet packets[#6]
		256-511 packets	Number of 256-to-511-octet packets[#6]
		512-1023 packets	Number of 512-to-1023-octet packets[#6]

Item		Displayed information	
		Detailed information	**Meaning**
		1024-1518 packets	Number of 1024-to-1518-octet packets[#6]
	Detailed statistical items for send errors	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 for which an error occurred
	Detailed statistical items for receive errors	CRC errors	The number of times the frame length was valid but an error was detected by the FCS check[#8]
		Alignment	The number of times the frame length was invalid and an error was detected by the FCS check[#7#8]
		Fragments	The number of times a short frame (whose length is shorter than 64 octets) is received and an FCS error or an alignment error occurred[#8]
		Jabber	The number of times a long frame (whose length exceeds the max frame length) was received and an FCS error or an alignment error occurred[#8]
		Symbol errors	The number of symbol errors
		Short frames	The number of received packets that are shorter than the frame length[#8]

Item		Displayed information		
		Detailed information		Meaning
		Long frames		The number of received packets that exceed the frame length[#8]
		Error frames		The total number of frames for which an error occurred
	Detailed statistical items for errors	Link down		The number of times a link was not established
	Statistical items for uplink redundancy[#9]	Startup active port selection		Setting of the functionality to fix the active port at Switch startup `primary only`: The functionality to fix the active port at Switch startup is enabled. This item is displayed only when this functionality is enabled.
		Switchport backup pairs	Primary	The number of the primary port or the channel group If an asterisk (`*`) is displayed, the port is an uplink port and the secondary port cannot be used for communication because the functionality to fix the active port at Switch startup is enabled.
			Status	Status of the primary port `Forwarding`: Forwarding `Blocking`: Blocking `Down`: Link down
			Secondary	The number of the secondary port or the channel group
			Status	Status of the secondary port `Forwarding`: Forwarding `Blocking`: Blocking `Down`: Link down
		Preemption	Delay	The time value (in seconds) for automatic or timer switch-back `-` is displayed when this item is not set.
			Limit	The time remaining until a timer switch-back (in seconds) `-` is displayed when this item is not set.

Item		Displayed information		
		Detailed information		Meaning
		Flush	VLAN	VLAN to which flush control frames are sent 1 to 4094: Indicates a VLAN ID. untag: No VLAN is specified. -: Send setting is not set.

#1: inactive is cleared in the following conditions:

- The port is restored by execution of the activate command.

  The BPDU guard functionality of a Spanning Tree Protocol

  The storm control functionality

  SML (Split Multi Link) functionality

  Detection of a unidirectional link failure by the UDLD functionality

  The L2 loop detection functionality.(The automatic restoration functionality can be also used for recovery.)

- The standby link functionality of link aggregation makes the standby port the active port.

#2: This item is displayed only for SFP ports.

#3: If the displayed value is smaller than 10000, the decimal point is not displayed.

If the displayed value is 10000 or larger, the unit is K and one digit is displayed below the decimal point. If the displayed value is 10000 K or larger, the unit is M and one digit is displayed below the decimal point.

#4: This item is always off except when the status of the port is either active up.

#5: This item is always - except when the status of the port is either active up.

#6: This item is displayed only when the command is executed with detail specified.

#7: This item is displayed for interfaces other than 100BASE-FX and 1000BASE-X.

#8: The frame length indicates the length starting from the MAC header and ending with the FCS field.

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

#9. This item is displayed only when uplink redundancy is set in the configuration.

Example 3 [10G model]

The following shows an example of displaying the shared SFP/SFP+ ports interface information and the detailed port information.

Figure 13-5 Execution result when shared SFP/SFP+ ports are specified

```
> show interfaces tengigabitethernet 0/28

Date 2011/02/23 10:49:09 UTC
Port 0/28 : active up  10GBASE-SR full  0012.e2a4.fe2b                    <-1
        SFP+ connect                                                      ]
        Time-since-last-status-change: 00:01:03                           |
        Bandwidth: 10000000kbps  Average out: 1Mbps  Average in: 1Mbps    |
        Peak out: 1Mbps at 10:48:06  Peak in: 272Mbps at 10:31:56         |
        Output rate:         868bps          1pps                         |
        Input  rate:         868bps          1pps                        |2
        Flow control send   : off                                         |
```

```
         Flow control receive: on                                          |
         TPID: 8100                                                        |
         Frame size: 1518 Octets   Interface name: tengeth0/28             |
         Description:                                                      |
        <Out octets/packets counter>                                       |
         Octets                                    :              13884|
         All packets                               :                147|
         Multicast packets                         :                  0|3
         Broadcast packets                         :                 23|
         Pause packets                             :                  0|
        <In octets/packets counter>                                        |
         Octets                                    :              12604|
         All packets                               :                127|4
         Multicast packets                         :                  0|
         Broadcast packets                         :                  2|
         Pause packets                             :                  0|
        <In line error counter>                                            |
         CRC errors                                :                  0|
         Fragments                                 :                  0|
         Jabber                                    :                  0|5
         Symbol errors                             :                  0|
         Short frames                              :                  0|
         Long frames                               :                  0|
         Error frames                              :                  0|
        <Line fault counter>                                               |6
         Link down                                 :                  2|

>
```

Example 4 [10G model]

The following shows an example of displaying the shared SFP/SFP+ ports interface information, the detailed port information, and detailed statistics.

Figure 13-6 Execution result when the detailed statistics for shared SFP/SFP+ ports are specified

```
> show interfaces tengigabitethernet 0/28 detail

Date 2011/02/23 10:49:21 UTC
Port 0/28 : active up  10GBASE-SR full  0012.e2a4.fe2b                    <-1
         SFP+ connect                                                      |
         Time-since-last-status-change: 00:01:15                           |
         Bandwidth: 10000000kbps  Average out: 0Mbps  Average in: 0Mbps    |
         Peak out: 1Mbps at 10:48:06  Peak in: 272Mbps at 10:31:56         |
         Output rate:         868bps           1pps                        |
         Input  rate:         868bps           1pps                        |2
         Flow control send   : off                                         |
         Flow control receive: on                                          |
         TPID: 8100                                                        |
         Frame size: 1518 Octets   Interface name: tengeth0/28             |
         Description:                                                      |
        <Out octets/packets counter>                                       |
         Octets                                    :              13884|
         All packets                               :                147|
         Multicast packets                         :                  0|
         Broadcast packets                         :                 23|
         Pause packets                             :                  0|
         64 packets                                :                 53|3
         65-127 packets                            :                 94|
         128-255 packets                           :                  0|
         256-511 packets                           :                  0|
         512-1023 packets                          :                  0|
         1024-1518 packets                         :                  0|
```

```
<In octets/packets counter>                                    ┐
 Octets                                :              12604|
 All packets                           :                127|
 Multicast packets                     :                  0|
 Broadcast packets                     :                  2|
 Pause packets                         :                  0|
 64 packets                            :                 33|4
 65-127 packets                        :                 94|
 128-255 packets                       :                  0|
 256-511 packets                       :                  0|
 512-1023 packets                      :                  0|
 1024-1518 packets                     :                  0┘
<In line error counter>                                        ┐
 CRC errors                            :                  0|
 Fragments                             :                  0|
 Jabber                                :                  0|5
 Symbol errors                         :                  0|
 Short frames                          :                  0|
 Long frames                           :                  0|
 Error frames                          :                  0┘
<Line fault counter>                                           ┐6
 Link down                             :                  2┘

>
```

1. Summary port information
2. Detailed port information
3. Send statistics
4. Receive statistics
5. Receive error statistics
6. Failure statistics

Display items in Example 3 and 4 [10G model]

The following shows an example of displaying the shared SFP/SFP+ ports interface information, the detailed port information, and detailed statistics.

Table 13-3 Display of summary information for the shared SFP/SFP+ ports

Item	**Displayed information**	
	Detailed information	**Meaning**
Port*<IF#>*	Port number	
<port status>	active up	Active (normal operating state)
	active down	Active (A line failure occurred.)
	initialize	Currently initializing
	test	A line test is in progress.
	fault	Failed

Item	Displayed information	
	Detailed information	**Meaning**
	inactive[#1]	The port is blocked. The following can cause a port to become blocked: ● Operation has been stopped by the `inactivate` command. ● The standby link functionality of link aggregation ● The BPDU guard functionality of the Spanning Tree Protocol ● The storm control functionality ● SML (Split Multi Link) functionality ● Detection of a unidirectional link failure by the UDLD functionality ● The L2 loop detection functionality
	disable	Operation was stopped by using the `shutdown` or `schedule-power-control shutdown` configuration commands.
<line type>	1000BASE-LX full	1000BASE-LX full duplex
	1000BASE-SX full	1000BASE-SX full duplex
	1000BASE-SX2 full	1000BASE-SX2 full duplex
	1000BASE-LH full	1000BASE-LH full duplex
	1000BASE-LHB full	1000BASE-LHB full duplex
	1000BASE-LX full(auto)	1000BASE-LX full duplex (Line type determined by auto-negotiation.)
	1000BASE-SX full(auto)	1000BASE-SX full duplex (Line type determined by auto-negotiation.)
	1000BASE-LH full(auto)	1000BASE-LH full duplex (Line type determined by auto-negotiation.)
	1000BASE-LHB full(auto)	1000BASE-LHB full duplex (Line type determined by auto-negotiation.)
	1000BASE-BX10-D full	1000BASE-BX-D (10 km) full duplex
	1000BASE-BX10-U full	1000BASE-BX-U (10 km) full duplex

Item	Displayed information	
	Detailed information	**Meaning**
	1000BASE-BX40-D full	1000BASE-BX-D (40 km) full duplex
	1000BASE-BX40-U full	1000BASE-BX-U (40 km) full duplex
	1000BASE-BX10-D full(auto)	1000BASE-BX-D (10 km) full duplex (Line type determined by auto-negotiation.)
	1000BASE-BX10-U full(auto)	1000BASE-BX-U (10 km) full duplex (Line type determined by auto-negotiation.)
	1000BASE-BX40-D full(auto)	1000BASE-BX-D (40 km) full duplex (Line type determined by auto-negotiation.)
	1000BASE-BX40-U full(auto)	1000BASE-BX-U (40 km) full duplex (Line type determined by auto-negotiation.)
	10GBASE-SR full	10GBASE-SR full duplex
	10GBASE-LR full	10GBASE-LR full duplex
	10GBASE-ER full	10GBASE-ER full duplex
	10GBASE-CU30CM full	10GBASE-CU (30 cm) full duplex
	10GBASE-CU1M full	10GBASE-CU (1 m) full duplex
	10GBASE-CU3M full	10GBASE-CU (3 m) full duplex
	10GBASE-CU5M full	10GBASE-CU (5 m) full duplex
	-	The line type is unknown. A hyphen (-) is displayed in the following cases: ● The port status is not `active up`. ● SFP (SFP+) is `not connect`
<MAC address>	MAC address of the port	
<type of transceiver> #2	SFP	SFP
	SFP+	SFP+
	-	The transceiver type is unknown.
<transceiver status> #2	connect	Installed
	not connect	Not installed

Item	Displayed information	
	Detailed information	**Meaning**
	not support	An unsupported transceiver is installed.
	-	The transceiver status is unknown. A hyphen (-) is displayed in the following cases: ● A port is in the `initialize` status. ● A port is in the `fault` status.

Table 13-4 Display of detailed information and statistics for the shared SFP/SFP+ ports

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) *ddays*`.`*hh*`:`*mm*`:`*ss* (when the elapsed time is more than 24 hours:*d* = 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*>`bps`	Displays the average bandwidth (in bps) 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*>`bps`	Displays the average bandwidth (in bps) used on the receiving side of the line for the one minute interval before the command was executed. `0 Mbps` is displayed if there is no communication (when not even 1 bit of data is transferred). `1 Mbps` is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place. The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.	
Peak out	Displays the maximum bandwidth used on the sending side of the line for the 24-hour interval before the command was executed, and the relevant time. `0 Mbps` is displayed if there is no communication (when not even 1 bit of data is transferred). `1 Mbps` is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.	

Item		Displayed information	
		Detailed information	**Meaning**
		The relevant time is the last time the bandwidth reached its maximum value. 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 relevant time is the last time the bandwidth reached its maximum value. The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.	
Output rate[#3]		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[#3]		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[#4]		on	A pause packet is sent.
		off	A pause packet is not sent.
Flow control receive[#4]		on	A pause packet is received.
		off	A pause packet is not received.
TPID		Displays a `TagProtocolIDentifier` value that is used on the port to identify the VLAN.	
Frame size[#5]		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/PAD field. For details about frame formats, see the description of frame formats in *14.1.3 Control on the MAC and LLC sublayers* in the *Configuration Guide Vol. 1*.	
Interface name		Displays the name of the interface assigned to the 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.	
Statistics	Category	<Out octets/packets counter>	Send statistics

Item		Displayed information	
		Detailed information	**Meaning**
		<In octets/packets counter>	Receive statistics
		<In line error counter>	Receive error statistics
		<Line fault counter>	Failure statistics
		<Uplink redundant>	Uplink redundancy statistics#8
	Detailed statistical items for sending and receiving	Octets	The number of octets
		All packets	Number of packets (including error packets)
		Multicast packets	Number of multicast packets
		Broadcast packets	Number of broadcast packets
		Pause packets	Number of pause packets
		64 packets	Number of 64-octet packets#6
		65-127 packets	Number of 65-to-127-octet packets#6
		128-255 packets	Number of 128-to-255-octet packets#6
		256-511 packets	Number of 256-to-511-octet packets#6
		512-1023 packets	Number of 512-to-1023-octet packets#6
		1024-1518 packets	Number of 1024-to-1518-octet packets#6
	Detailed statistical items for receive errors	CRC errors	The number of times the frame length was valid but an error was detected by the FCS check#7
		Fragments	The number of times a short frame (whose length is shorter than 64 octets) is received and an FCS error or an alignment error occurred#7
		Jabber	The number of times a long frame (whose length exceeds the max frame length) was received and an FCS error or an alignment error occurred#7
		Symbol errors	The number of symbol errors

Item		Displayed information		
		Detailed information		Meaning
		Short frames		The number of received packets that are shorter than the frame length[#7]
		Long frames		The number of received packets that exceed the frame length[#7]
		Error frames		The total number of frames for which an error occurred
	Detailed statistical items for errors	Link down		The number of times a link was not established
	Statistical items for uplink redundancy[#8]	Startup active port selection		Setting of the functionality to fix the active port at Switch startup `primary only`: The functionality to fix the active port at Switch startup is enabled. This item is displayed only when this functionality is enabled.
		Switchport backup pairs	Primary	The number of the primary port or the channel group If an asterisk (`*`) is displayed, the port is an uplink port and the secondary port cannot be used for communication because the functionality to fix the active port at Switch startup is enabled.
			Status	Status of the primary port `Forwarding`: Forwarding `Blocking`: Blocking `Down`: Link down
			Secondary	The number of the secondary port or the channel group
			Status	Status of the secondary port `Forwarding`: Forwarding `Blocking`: Blocking `Down`: Link down
		Preemption	Delay	The time value (in seconds) for automatic or timer switch-back `-` is displayed when this item is not set.

Item		Displayed information		
		Detailed information		Meaning
			Limit	The time remaining until a timer switch-back (in seconds) `-` is displayed when this item is not set.
		Flush	VLAN	VLAN to which flush control frames are sent `1` to `4094`: Indicates a VLAN ID. `untag`: No VLAN is specified. `-`: Send setting is not set.

#1: `inactive` is cleared in the following conditions:

- The port is restored by execution of the `activate` command.

  The BPDU guard functionality of a Spanning Tree Protocol

  The storm control functionality

  SML (Split Multi Link) functionality

  Detection of a unidirectional link failure by the UDLD functionality

  The L2 loop detection functionality.(The automatic restoration functionality can be also used for recovery.)

- The standby link functionality of link aggregation makes the standby port the active port.

#2 This item is not displayed for 1000BASE-T (SFP).

#3: If the displayed value is smaller than 10000, the decimal point is not displayed.

If the displayed value is 10000 or larger, the unit is K and one digit is displayed below the decimal point. If the displayed value is 10000 K or larger, the unit is M and one digit is displayed below the decimal point.

#4: This item is always `off` except when the status of the port is either `active` `up`.

#5: This item is always `-` except when the status of the port is either `active` `up`.

#6. This item is displayed only when the command is executed with `detail` specified.

#7: The frame length indicates the length starting from the MAC header and ending with the FCS field.

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

#8. This item is displayed only when uplink redundancy is set in the configuration.

Impact on communication

None

Response messages

None

Notes

- All display items are cleared in the following cases:

  When the Switch starts up

When the `clear counters` command is executed

When a device hardware failure occurs

- For notes on uplink redundancy, see the description of the `show switchport-backup` command.

clear counters

Clears the statistics counter of an Ethernet interface to zero.

Syntax

```
clear counters [{gigabitethernet <IF#> | tengigabitethernet <IF#>}]
```

Input mode

User mode and administrator mode

Parameters

{gigabitethernet *<IF#>* | tengigabitethernet *<IF#>*}

gigabitethernet

Specifies an Ethernet interface with a maximum line speed of 1 Gbit/s.

tengigabitethernet

Specifies an Ethernet interface with a maximum line speed of 10 Gbit/s.

<IF#>

Specify an interface port number. For the specifiable range of values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Clears the statistics counter of all Ethernet interfaces to zero.

Example

None

Display items

None

Impact on communication

None

Response messages

None

Notes

- Even if the statistics counter is cleared to zero, the value of the MIB information obtained by using SNMP is not cleared to zero.
- The following information items displayed by the `show interfaces` command are cleared to zero:
  - Send and receive statistics
  - Send error statistics
  - Receive error statistics
  - Failure statistics
- The `clear counters` command also clears, to zero, the port's statistics counter displayed by the `show port statistics` or `show channel -group statistics` command.

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>]
show port vlan [<port list>] [{ access | trunk | protocol | mac | tunnel |
            peer-link }]
```

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*.

Operation 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`.

Operation 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.

Operation 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 command allows you to check the identification information of each transceiver.

vlan

Displays VLAN information for ports.

{ access | trunk | protocol | mac | tunnel | peer-link }

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.

peer-link
Displays VLAN information for SML peer link ports.

Operation when this parameter is omitted:
Displays information for all kinds of ports.

Operation when all parameters are omitted:
Lists information for all implemented Ethernet ports.

Example 1

Figure 13-7 Example of listing link information for ports

```
> show port

Date 2011/09/07 14:01:40 UTC
Port Counts: 52
Port  Name           Status  Speed           Duplex     FCtl FrLen  ChGr/Status
 0/1  geth0/1        up      100BASE-TX      full(auto) on    1518  -/-
 0/2  geth0/2        up      100BASE-TX      full(auto) on    1518  -/-
 0/3  geth0/3        down    -               -          -        -  -/-

             :                                      :

 0/48 geth0/48       down    -               -          -        -  64/down
 0/49 geth0/49       down    -               -          -        -  64/down
 0/50 geth0/50       down    -               -          -        -  -/-
 0/51 geth0/51       down    -               -          -        -  -/-
 0/52 geth0/52       down    -               -          -        -  -/-

>
```

Display items in Example 1

Table 13-5 Explanation of the display of the link information list for ports

Item	Meaning	Displayed detailed information
Port Counts	Number of target ports	--
Port	Port	Interface port number
Name	Port name	The name assigned to a port is displayed.

Item	Meaning	Displayed detailed information
Status	Port state	up: Active (normal operating state). down: Active (a line failure has occurred). init: Initializing test: During line test fault: Failed inact: The port is blocked.#1 The following can cause a port to become blocked: ■ Operation has been stopped by the inactivate command. ■ The standby link functionality of link aggregation ■ The BPDU guard functionality of a Spanning Tree Protocol ■ The storm control functionality ■ SML (Split Multi Link) functionality ■ Detection of a unidirectional link failure by the UDLD functionality ■ The L2 loop detection functionality dis: Operation has been stopped by using the shutdown or schedule-power-control shutdown configuration command.
Speed	Line speed	10BASE-T: 10BASE-T 100BASE-TX: 100BASE-TX 1000BASE-T: 1000BASE-T 100BASE-FX: 100BASE-FX [24S4X][24S4XD] 1000BASE-LX: 1000BASE-LX 1000BASE-SX: 1000BASE-SX 1000BASE-SX2: 1000BASE-SX2 1000BASE-LH: 1000BASE-LH 1000BASE-LHB: 1000BASE-LHB 1000BASE-BX10-D: 1000BASE-BX10-D 1000BASE-BX10-U: 1000BASE-BX10-U 1000BASE-BX40-D: 1000BASE-BX40-D 1000BASE-BX40-U: 1000BASE-BX40-U 10GBASE-SR: 10GBASE-SR [10G model] 10GBASE-LR: 10GBASE-LR [10G model] 10GBASE-ER: 10GBASE-ER [10G model] 10GBASE-CU30CM: 10GBASE-CU (30 cm) [10G model] 10GBASE-CU1M: 10GBASE-CU (1 m) [10G model] 10GBASE-CU3M: 10GBASE-CU (3 m) [10G model] 10GBASE-CU5M: 10GBASE-CU (5 m) [10G model] -: Speed is unknown (appears when Status is not up.)

Item	Meaning	Displayed detailed information
Duplex	Full duplex/half duplex	`full`: Full duplex `full(auto)`: Full duplex (resulting from auto-negotiation) `half`: Half duplex `half(auto)`: Half duplex (resulting from auto-negotiation) `-`: `Duplex` is unknown (appears when `Status` is not `up`.)
FCtl	Flow control	`on`: Flow control is enabled. `off`: Flow control is disabled. `-`: `Status` is not `up`.
FrLen	Maximum frame length	Displays the maximum frame length of a port in octets. `-`: `Status` is not `up`.
ChGr /Status	Channel group and status	The channel group to which the port belongs and the status. Link aggregation channel group number: 1 to 64 `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.

#1: `inact` is cleared in the following conditions:

- The port is restored by execution of the `activate` command.

  The BPDU guard functionality of a Spanning Tree Protocol

  The storm control functionality

  SML (Split Multi Link) functionality

  Detection of a unidirectional link failure by the UDLD functionality

  The L2 loop detection functionality.(The automatic restoration functionality can be also used for recovery.)

- The standby link functionality of link aggregation makes the standby port the active port.

Example 2

Figure 13-8 Example of listing protocol information for ports

```
> show port protocol

Date 2011/09/07 14:01:53 UTC
Port Counts: 52
Port  Name           Type        VLAN  STP    QoS   Filter MACTbl    Ext.
 0/1  geth0/1        Trunk          2    0   0(0)     0(0)      0    - - - - A
 0/2  geth0/2        Trunk          2    0   0(0)     0(0)      0    - - T - A
 0/3  geth0/3        Access         1    0   0(0)     0(0)      0    - - - - -

             :                                    :

 0/48 geth0/48       Access         1    0   0(0)     0(0)      0    - - - - -
 0/49 geth0/49       Access         1    0   0(0)     0(0)      0    - - - - -
 0/50 geth0/50       Access         1    0   0(0)     0(0)      0    - - - - -
```

```
 0/51 geth0/51       Access         1    0   0(0)     0(0)      0    - - - - -
 0/52 geth0/52       Access         1    0   0(0)     0(0)      0    - - - - -
   I: Isolation setting  S: Storm control setting  T: Tag Translation setting
   L: LLDP setting       A: Ring Protocol setting

>
```

Display items in Example 2

Table 13-6 Explanation of the display of the protocol information list for ports

Item	Meaning	Displayed detailed information
Port Counts	Number of target ports	--
Port	Port	Interface port number
Name	Port name	The name assigned to a port is displayed.
Type	Port type	`Protocol`: Protocol port `Trunk`: Trunk port `Access`: Access port `MAC`: MAC port `Tunnel`: Tunneling port `Peer-link`: SML peer link port
VLAN	Number of VLANs that share the port	Number of VLANs that share the port (including the default VLAN and VLANs in `suspend` status.) 0 is fixed if this is set for mirror port. For the SML peer link port, this is fixed at the maximum number (4094) of VLANs set by the switch.
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 used together, the number of VLANs set by `pvst+` + 1) 0 is fixed when `spanning-tree disable` is used
QoS	The 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. The number of QoS flow lists set for the VLAN to which the port belongs is displayed enclosed in parentheses.
Filter	The 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. The number of access lists set for the VLAN to which the port belongs is displayed enclosed in parentheses.
MACTbl	The number of dynamically learned entries in the MAC address table	Displays the number of dynamically learned MAC address table entries.

Item	Meaning	Displayed detailed information
Ext.	Extended functionality information	I: Indicates that relay blocking information is set. S: Indicates that storm control information is set. T: Indicates that tag translation is set. L: Indicates that LLDP is running. A: Indicates that the Ring Protocol is running. - is displayed if the relevant extended functionality is not set or is not running. For the SML peer link port, - is displayed.

Example 3

Figure 13-9 Example of displaying the number of sent, received, and discarded packets for ports

```
> show port statistics

Date 2011/09/07 14:02:07 UTC
Port Counts: 52
Port  Name          Status  T/R  All packets   Multicast   Broadcast    Discard
 0/1  geth0/1       up      Tx        568728        7388      559949          0
                             Rx          8038        7328           1          0
 0/2  geth0/2       up      Tx        568728        7388      559949          0
                             Rx         17264        7328          10          0
 0/3  geth0/3       down    Tx             0           0           0          0
                             Rx             0           0           0          0

             :                                     :

 0/48 geth0/48      down    Tx             0           0           0          0
                             Rx             0           0           0          0
 0/49 geth0/49      down    Tx             0           0           0          0
                             Rx             0           0           0          0
 0/50 geth0/50      down    Tx             0           0           0          0
                             Rx             0           0           0          0
 0/51 geth0/51      down    Tx             0           0           0          0
                             Rx             0           0           0          0
 0/52 geth0/52      down    Tx             0           0           0          0
                             Rx             0           0           0          0

>
```

Display items in Example 3

Table 13-7 Display of the number of sent, received, and discarded packets for ports

Item	Meaning	Displayed detailed information
Port Counts	Number of target ports	--
Port	Port	Interface port number
Name	Port name	The name assigned to a port is displayed.

Item	Meaning	Displayed detailed information
Status	Port state	`up`: Active (normal operating state). `down`: Active (a line failure has occurred). `init`: Initializing `test`: During line test `fault`: Failed `inact`: The port is blocked.# The following can cause a port to become blocked: ■ Operation has been stopped by the `inactivate` command. ■ The standby link functionality of link aggregation ■ The BPDU guard functionality of a Spanning Tree Protocol ■ The storm control functionality ■ SML (Split Multi Link) functionality ■ Detection of a unidirectional link failure by the UDLD functionality ■ The L2 loop detection functionality `dis`: Operation has been 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	

#: `inact` is cleared in the following conditions:

- The port is restored by execution of the `activate` command.

  The BPDU guard functionality of a Spanning Tree Protocol

  The storm control functionality

  SML (Split Multi Link) functionality

  Detection of a unidirectional link failure by the UDLD functionality

  The L2 loop detection functionality.(The automatic restoration functionality can be also used for recovery.)

- The standby link functionality of link aggregation makes the standby port the active port.

Example 4

Figure 13-10 Example of listing transceiver information

```
> show port transceiver

Date 2010/12/27 14:31:48 UTC
Port Counts: 28
Port: 0/1  Status: connect      Type: SFP  Speed: 1000BASE-SX
           Vendor name: FINISAR CORP.         Vendor SN : U9Q3X0S
```

```
                Vendor PN  : FTLF8519P2BNL         Vendor rev: A
                Tx power   : -4.5dBm               Rx power  : -5.3dBm

                   :                                       :

Port: 0/28 Status: connect      Type: SFP+ Speed: 10GBASE-CU3M
                Vendor name: Molex Inc.            Vendor SN : 009130365
                Vendor PN  : 74752-1301            Vendor rev:
                Tx power   : -                     Rx power  : -

>
```

Display items in Example 4

Table 13-8 Display of the transceiver information list

Item	Meaning	Displayed detailed information
Port Counts	Number of target ports	--
Port	Port	Interface port number
Status	Status of the transceiver	`connect`: Installed `not connect`: 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 `SFP+`: SFP+ `-`: The transceiver type is unknown.
Speed	Line speed	10BASE-T/100BASE-TX/1000BASE-T: 10BASE-T/100BASE-TX/1000BASE-T 100BASE-FX: 100BASE-FX [24S4X][24S4XD] 1000BASE-SX: 1000BASE-SX 1000BASE-SX2: 1000BASE-SX2 1000BASE-LX: 1000BASE-LX 1000BASE-LH: 1000BASE-LH 1000BASE-LHB: 1000BASE-LHB 1000BASE-BX10-D: 1000BASE-BX10-D 1000BASE-BX10-U: 1000BASE-BX10-U 1000BASE-BX40-D: 1000BASE-BX40-D 1000BASE-BX40-U: 1000BASE-BX40-U 10GBASE-SR: 10GBASE-SR [10G model] 10GBASE-LR: 10GBASE-LR [10G model] 10GBASE-ER: 10GBASE-ER [10G model] 10GBASE-CU30CM: 10GBASE-CU (30 cm) [10G model] 10GBASE-CU1M: 10GBASE-CU (1 m) [10G model] 10GBASE-CU3M: 10GBASE-CU (3 m) [10G model] 10GBASE-CU5M: 10GBASE-CU (5 m) [10G model] `-`: Unknown line speed (`-` is displayed if the port status is `init` or `fault`, or if the transceiver state is not `connect`).

Item	Meaning	Displayed detailed information
Vendor name	Vendor name	Displays the vendor's name.#1
Vendor SN	Vendor serial number	Displays the serial number added by the vendor.#1
Vendor PN	Vendor part number	Displays the part number added by the vendor.#1
Vendor rev	Vendor revision	Displays a part number revision added by the vendor.#1
Tx Power	Sending optical power	Displays the sending optical power in dBm.#1#2#3
Rx Power	Receiving optical power	Displays the receiving optical power in dBm.#1#2#3

#1: A hypen (-) is displayed if the transceiver status is `not connect`.

#2: If the optical power is outside the range from −40 to 8.2 dBm, a hyphen (-) is displayed.

#3: An error might arise depending on the environmental requirements. For checking the correct value, use an optical power meter.

Example 5

Figure 13-11 Example of listing VLAN information for ports

```
> show port vlan

Date 2011/11/15 14:21:39 UTC
Port Counts: 28
Port  Name           Status Type        VLAN
 0/1  geth0/1        up     Protocol    1,100,1100-1103
 0/2  geth0/2        up     MAC         1,200,1200,1204-1205
 0/3  geth0/3        up     Trunk       1000-1050
 0/4  geth0/4        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
 0/5  geth0/5        up     Access      300 (Global IP Network VLAN)
 0/6  geth0/6        up     Access      300 (Global IP Network VLAN)
 0/7  geth0/7        up     Access      300 (Global IP Network VLAN)
        :                :             :
 0/25 geth0/25       up     Peer-link   1-4094
 0/26 geth0/26       up     Peer-link   1-4094
 0/27 geth0/27       down   Access      1   (VLAN0001)
 0/28 geth0/28       down   Access      1   (VLAN0001)

>
```

Display items in Example 5

Table 13-9 Displayed items (VLAN information for ports)

Item	Meaning	Displayed detailed information
Port Counts	Number of target ports	--
Port	Port	Interface port number
Name	Port name	The name assigned to a port is displayed.

Item	Meaning	Displayed detailed information
Status	Port state	`up`: Active (normal operating state). `down`: Active (a line failure has occurred). `init`: Initializing `test`: During line test `fault`: Failed `inact`: The port is blocked.#1 The following can cause a port to become blocked: ■ Operation has been stopped by the `inactivate` command. ■ The standby link functionality of link aggregation ■ The BPDU guard functionality of a Spanning Tree Protocol ■ The storm control functionality ■ SML (Split Multi Link) functionality ■ Detection of a unidirectional link failure by the UDLD functionality ■ The L2 loop detection functionality `dis`: Operation has been stopped by using the `shutdown` or `schedule-power-control shutdown` configuration command.
Type	Port type	`Protocol`: Protocol port `Trunk`: Trunk port `Access`: Access port `MAC`: MAC port `Tunnel`: Tunneling port `Peer-link`: SML peer link 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. For the SML peer link port, this is fixed to `1-4094`. When automatic VLAN assignment is suppressed, `limited` is displayed.

#1: `inact` is cleared in the following conditions:

- The port is restored by execution of the `activate` command.

  The BPDU guard functionality of a Spanning Tree Protocol

  The storm control functionality

  SML (Split Multi Link) functionality

  Detection of a unidirectional link failure by the UDLD functionality

  The L2 loop detection functionality.(The automatic restoration functionality can be also used for recovery.)

- The standby link functionality of link aggregation makes the standby port the active port.

Impact on communication

None

Response messages

None

Notes

- The displayed number of discarded packets is the total of the values for the items listed in the following table.

Table 13-10 Statistical items used for calculating the number of discarded packets

Port	Statistical item	
	Sending	**Receiving**
Ethernet	Late collision Excessive collisions Excessive deferral	CRC errors Alignment Fragments Jabber Symbol errors Short frames Long frames

- The statistic counter is cleared in the following cases:
  - When the `clear counters` command is executed
  - When a device hardware failure occurs
- If you insert an unsupported transceiver in the Switch, operation is not guaranteed.

activate

Returns the status of the Ethernet interface to `active` from `inactive` when the `inactivate` command has been used to set `inactive`.

Syntax

```
activate {gigabitethernet <IF#> | tengigabitethernet <IF#>}
```

Input mode

User mode and administrator mode

Parameters

{gigabitethernet *<IF#>* | tengigabitethernet *<IF#>*}

gigabitethernet

Specifies an Ethernet interface with a maximum line speed of 1 Gbit/s.

tengigabitethernet

Specifies an Ethernet interface with a maximum line speed of 10 Gbit/s.

<IF#>

Specify an interface port number. For the specifiable range of values, see *Specifiable values for parameters*.

Example

Return the status of interface port 0/1 to `active`.

```
> activate gigabitethernet 0/1
```

Display items

None

Impact on communication

Yes

Response messages

Table 13-11 List of response messages for the activate command

Message	Description
<IF#> is already active.	The specified port is already `active`. The command does not need to be executed if you correctly specified the port. *<IF#>*: Interface port number
<IF#> is already initializing.	The specified port is already being initialized. *<IF#>*: Interface port number
<IF#> is disabled.	The specified port is in `disable` status due to the configuration. Make sure the specified parameter is correct, and then try again. *<IF#>*: Interface port number

Message	Description
<IF#> is failed.	A failure has occurred or a line test is being conducted on the specified port. Make sure the specified parameter is correct. <IF#>: Interface port number
Can't execute.	The command could not be executed. Re-execute the command.

Notes

Using this command does not change the startup configuration file that was stored on the internal flash memory.

inactivate

Changes the status of an Ethernet interface from `active` to `inactive` without changing the startup configuration file stored in internal flash memory.

Syntax

```
inactivate {gigabitethernet <IF#> | tengigabitethernet <IF#>}
```

Input mode

User mode and administrator mode

Parameters

{gigabitethernet *<IF#>* | tengigabitethernet *<IF#>*}

gigabitethernet

Specifies an Ethernet interface with a maximum line speed of 1 Gbit/s.

tengigabitethernet

Specifies an Ethernet interface with a maximum line speed of 10 Gbit/s.

<IF#>

Specify an interface port number. For the specifiable range of values, see *Specifiable values for parameters*.

Example

Changes the status of interface port 0/1 to `inactive`.

```
> inactivate gigabitethernet 0/1
```

Display items

None

Impact on communication

Yes

Response messages

Table 13-12 List of response messages for the inactivate command

Message	Description
<IF#> is already inactive.	The specified port is already `inactive`. The command does not need to be executed if you correctly specified the port. *<IF#>*: Interface port number
<IF#> is disabled.	The specified port is in `disable` status due to the configuration. Make sure the specified parameter is correct, and then try again. *<IF#>*: Interface port number
<IF#> is failed.	The specified port is not in the `active` status. Make sure the specified parameter is correct. *<IF#>*: Interface port number

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Line test executing.	A line test is being conducted. To change the port status, stop the line test.

Notes

- Using this command does not change the startup configuration file that was stored on the internal flash memory.
- 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.

test interfaces

If an error occurs in communication over an Ethernet network, this command can be used to identify the faulty part. After the faulty part (such as a cable) has been replaced, this command can also be used to verify operation (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 line tests, see the *Troubleshooting Guide*.

Syntax

```
test interfaces gigabitethernet <IF#> {internal | connector}
     [auto_negotiation {10base-t | 100base-tx | 1000base-t}]
     [interval <interval time>] [pattern <test pattern no.>]
     [length <data length>]
test interfaces tengigabitethernet <IF#> {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 a maximum line speed of 1 Gbit/s.

tengigabitethernet

Specifies an Ethernet interface with a maximum line speed of 10 Gbit/s.

<IF#>

Specify an interface 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 specification of the segment to which the line test is conducted.

Also note that this parameter can be applied for RJ45 ports only when the line type is 10BASE-T/100BASE-TX/1000BASE-T.

Operation 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.

Operation 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 using test patterns 1 to 4.

`1`: all 0xff

`2`: all 0x00

`3`: "** THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG.0123456789 **" pattern repeated

`4`: Send a data corruption detection pattern.

Operation 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 13-13 Specifiable range of values for each test

No.	Test	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.

Operation when all parameters are omitted:

Operation proceeds as described for each *Operation when this parameter is omitted* section.

Example

The following figure shows an example of the screen displayed at the start of an Ethernet line test. This example starts an internal loopback test that sends a 100-octet frame in the all-`0xff` test pattern at five-second intervals to the port number of `2`.

Figure 13-12 Example of a screen displayed at the start of 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 13-14 List of response messages for the test interfaces command

Message	Description
<IF#> is disabled.	The specified port is in `disable` status due to the configuration. Make sure the specified parameter is correct. *<IF#>*: Interface port number

Message	Description
<IF#> is failed.	The specified port has failed. Make sure the specified parameter is correct. <IF#>: Interface port number
Can't execute.	The command could not be executed. Re-execute the command.
No support auto negotiation parameter.	The specified port does not support auto-negotiation parameters. Make sure the specified parameter is correct.
SML peer-link is configured.	The SML functionality is enabled on the specified port. Disable the SML functionality, then execute the command again.
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 change the configuration of a port under the line test, first execute the `no test interfaces` command to stop the line test.
- 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.
- Please conduct a line test for each port.
- Concerning the line test of this Switch, execute the `inactivate` command, start the line test, stop the line test, and then execute the `activate` command to each of the target ports.

  Take the procedure above even when conducting the line test to the same port again.
- To conduct a loop connector loopback test on a 1000BASE-LH, or 1000BASE-LHB port, an optical attenuator is required. For details about optical attenuation, see the following table.

Table 13-15 Optical attenuation

Line type	Attenuation value (dB)
1000BASE-LH	5 to 22
1000BASE-LHB	17 to 36

- 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 loop connector loopback test on a 10GBASE-CU port. [10G model]:
- 100BASE-FX operates with the fixed setting of `100M-Full`. [24S4X][24S4XD]
- The SFP module keeps emitting transmission waves (optical signals) during the line test, thus do not look into the optical I/O blocks.
- The line test cannot be conducted to the SML peer link port.
- To conduct the line test to a port configured as a mirror port, first cancel its mirror-port setting.
- The following table shows the operating rates by the test type.

Table 13-16 Operating rates by the test type

Test type set by using this command	10BASE-T, 100BASE-TX, or 1000BASE-T port	SFP port or shared SFP/SFP+ port
internal	Line speed of the specification of the segment specified by the `auto_negotiation` parameter	Maximum line speed of the port ● For gigabit Ethernet interface port: 1 Gbit/s ● For 10 gigabit Ethernet interface port: 10 Gbit/s
connector		Maximum line speed of the connected transceiver However, it runs with the 100 Mbit/s, when 10/100/1000BASE-T (SFP) is connected on the AX2530S-24S4X or AX2530S-24S4XD port 0/1 to 0/24.

no test interfaces

Stops an Ethernet line test, and displays the test results.

For details about line tests, see the *Troubleshooting Guide*.

Syntax

```
no test interfaces gigabitethernet <IF#>
no test interfaces tengigabitethernet <IF#>
```

Input mode

User mode and administrator mode

Parameters

gigabitethernet

Specifies an Ethernet interface with a maximum line speed of 1 Gbit/s.

tengigabitethernet

Specifies an Ethernet interface with a maximum line speed of 10 Gbit/s.

<IF#>

Specify an interface port number. For the specifiable range of values, see *Specifiable values for parameters*.

Example 1

- Line test for 10BASE-T/100BASE-TX/1000BASE-T

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`. The following figure shows an example of displaying the line test results for a 10BASE-T/100BASE-TX/1000BASE-T Ethernet port.

Figure 13-13 Example of displaying line test results (for 10BASE-T/100BASE-TX/1000BASE-T)

```
>test interfaces gigabitethernet 0/2 internal interval 5 pattern 1 length 100

> no test interfaces gigabitethernet 0/2

Date 2010/08/06 04:07:39 UTC
Interface type            :100BASE-TX
Test count                :13
Send-OK                   :13            Send-NG                :0
Receive-OK                :13            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 in Example 1

Table 13-17 Items displayed as line test results (for 10BASE-T/100BASE-TX/1000BASE-T)

Item	Meaning	Presumed cause	Measures
Interface type[#1]	Line type (`10BASE-T`, `100BASE-TX`, `1000BASE-T`, or `----`[#2])	--	--
Test count	Number of times a 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 error	For a loop connector loopback test, verify that a loopback connector is correctly connected to the port.
Receive-OK	Number of times data was received normally	--	--
Receive-NG	Number of times data was received abnormally	Sum of the number of times a data compare error occurred and the number of times reception monitoring timed out	See *Data compare error* and subsequent items in this table.
Data compare error	Number of data compare errors (number of received frames that did not match the sent frames)	Line error	Replace the switch.
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 errors that occurred	Line error	Replace the switch.
In CRC error	The number of times the frame length was valid but an error was detected by the FCS check[#3]	Line error	Replace the switch.
In alignment	The number of times the frame length was invalid and an error was detected by the FCS check[#3]	Line error	Replace the switch.

Item	Meaning	Presumed cause	Measures
In monitor time out	Timeout for the reception monitoring timer	Line error	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 errors that occurred	Line error	For a loop connector loopback test, verify that a loopback connector is correctly connected to the port.
H/W error	Whether a hardware error has occurred. `none`: No hardware error occurred. `occurred`: A hardware error occurred.	Line error	Replace the switch.

#1: The following table lists the indication for interface type.

Table 13-18 Interface type indication

Test type set by using test interfaces command	10BASE-T, 100BASE-TX, or 1000BASE-T port	SFP port or shared SFP/SFP+ port
internal	Line speed of the specification of the segment specified by the `auto_negotiation` parameter in the `test interfaces` command.	Line type of the connected transceiver However, `1000BASE-T` is displayed for 10/100/1000BASE-T (SFP).
connector		Line type of the connected transceiver For 10/100/1000BASE-T (SFP) port, see *Table 13-19 Interface type indication for 10/100/1000BASE-T (SFP)*.

Table 13-19 Interface type indication for 10/100/1000BASE-T (SFP)

Model	Port	Interface type indication
AX2530S-24T AX2530S-24TD	0/25 to 0/28	1000BASE-T
AX2530S-24T4X	0/25 to 0/28	
AX2530S-48T AX2530S-48TD	0/49 to 0/52	
AX2530S-48T2X	0/49 to 0/52	

Model	Port	Interface type indication
AX2530S-24S4X AX2530S-24S4XD	0/25 to 0/28	
AX2530S-24S4X AX2530S-24S4XD	0/1 to 0/24	100BASE-TX

#2: The line type is unknown. This is indicated in the following cases:

- 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 *14.1.3 Control on the MAC and LLC sublayers* in the *Configuration Guide Vol. 1*.

#4: If the loop connector is connected correctly, packets for the line test might have accumulated in the device.

Example 2

- Line test for 100BASE-FX/1000BASE-X

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`. The following figure shows an example of displaying the line test results for a 1000BASE-X Ethernet port.

Figure 13-14 Execution result of line test for 100BASE-FX/1000BASE-X

```
> test interfaces gigabitethernet 0/2 internal interval 5 pattern 1 length 100

> no test interfaces gigabitethernet 0/2

Date 2010/12/19 17:27:00 UTC
Interface type             :1000BASE-LH
Test count                 :98
Send-OK                    :98             Send-NG                :0
Receive-OK                 :98             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 in Example 2

Table 13-20 Items displayed as line test results (for 100BASE-FX/1000BASE-X)

Item	Meaning	Presumed cause	Measures
Interface type[#1]	Line type (100BASE-FX, 1000BASE-LX, 1000BASE-SX, 1000BASE-SX2, 1000BASE-LH, 1000BASE-LHB, 1000BASE-BX10-D, 1000BASE-BX10-U, 1000BASE-BX40-D, 1000BASE-BX40-U, or ----[#2])	--	--
Test count	Number of times a 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 error	For a loop connector loopback test, verify that a loopback connector is correctly connected to the port.
Receive-OK	Number of times data was received normally	--	--
Receive-NG	Number of times data was received abnormally	Sum of the number of times a data compare error occurred and the number of times reception monitoring timed out	See *Data compare error* and subsequent items in this table.
Data compare error	Number of data compare errors (number of received frames that did not match the sent frames)	Line error	Replace the switch.
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 errors that occurred	Line error	Replace the switch.
In CRC error	The number of times the frame length was valid but an error was detected by the FCS check[#3]	Line error	Replace the switch.

Item	Meaning	Presumed cause	Measures
In alignment	The number of times the frame length was invalid and an error was detected by the FCS check#3	Line error	Replace the switch.
In monitor time out	Timeout for the reception monitoring timer	Line error	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 errors that occurred	Line error	For a loop connector loopback test, verify that a loopback connector is correctly connected to the port.
H/W error	Whether a hardware error has occurred. `none`: No hardware error occurred. `occurred`: A hardware error occurred.	Line error	Replace the switch.

#1: For interface type indication, see *Table 13-18 Interface type indication*.

#2: The line type is unknown. This is indicated in the following cases:

- 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 *14.1.3 Control on the MAC and LLC sublayers* in the *Configuration Guide Vol. 1*.

#4: If the loop connector is connected correctly, packets for the line test might have accumulated in the device.

Example 3

- Line test for 10GBASE-R

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 `25`. The following figure shows an example of displaying the line test results for a 10GBASE-R Ethernet port.

Figure 13-15 Example of displaying line test results (for 10GBASE-R)

```
> test interfaces tengigabitethernet 0/25 internal interval 5 pattern 1 length 100

> no test interfaces tengigabitethernet 0/25

Date 2010/12/19 17:36:01 UTC
```

```
Interface type            :10GBASE-SR
Test count                :84
Send-OK                   :84            Send-NG                :0
Receive-OK                :84            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 in Example 3

Table 13-21 Items displayed as line test results (for 100GBASE-R)

Item	Meaning	Presumed cause	Measures
Interface type[#1]	Line type (10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-CU30CM, 10GBASE-CU1M, 10GBASE-CU3M, 10GBASE-CU5M, or ----[#2])	--	--
Test count	Number of times a 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 error	For a loop connector loopback test, verify that a loopback connector is correctly connected to the port.
Receive-OK	Number of times data was received normally	--	--
Receive-NG	Number of times data was received abnormally	Sum of the number of times a data compare error occurred and the number of times reception monitoring timed out	See *Data compare error* and subsequent items in this table.
Data compare error	Number of data compare errors (number of received frames that did not match the sent frames)	Line error	Replace the switch.
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.

Item	Meaning	Presumed cause	Measures
Out line error	Number of send line errors that occurred	Line error	Replace the switch.
In CRC error	The number of times the frame length was valid but an error was detected by the FCS check#3	Line error	Replace the switch.
In alignment	The number of times the frame length was invalid and an error was detected by the FCS check#3	Line error	Replace the switch.
In monitor time out	Timeout for the reception monitoring timer	Line error	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 errors that occurred	Line error	For a loop connector loopback test, verify that a loopback connector is correctly connected to the port.
H/W error	Whether a hardware error has occurred. `none`: No hardware error occurred. `occurred`: A hardware error occurred.	Line error	Replace the switch.

#1: For interface type indication, see *Table 13-18 Interface type indication* and *Table 13-19 Interface type indication for 10/100/1000BASE-T (SFP)*.

#2: The line type is unknown. This is indicated in the following cases:

- The transceiver status is not `connect`.
- A line test was stopped immediately after it was 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 *14.1.3 Control on the MAC and LLC sublayers* in the *Configuration Guide Vol. 1*.

#4: If the loop connector is connected correctly, packets for the line test might have accumulated in the device.

Impact on communication

None

Response messages

Table 13-22 List of response messages for the no test interfaces command

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

14. Link Aggregation

show channel-group
show channel-group statistics
clear channel-group statistics lacp

show channel-group

Displays 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*.

Operation when this parameter is omitted:

All link aggregation information is displayed.

detail

Displays detailed link aggregation information.

Operation when this parameter is omitted:

Link aggregation information is displayed.

summary

Displays summary information about link aggregation.

Operation when this parameter is omitted:

All link aggregation information is displayed.

Example 1

Figure 14-1 Example of displaying link aggregation information

```
> show channel-group

Date 2012/12/06 18:20:48 UTC
ChGr: 31  Mode: LACP
  CH Status      : Down    Elapsed Time: -
  Max Active Port: 8
  MAC address    : -               VLAN ID: 4093
  Actor System   : Priority: 128    MAC: 0012.e2a4.fe51  Key: 31
  Partner System : -
  Port Information
    0/23  Down  State: Detached
    0/25  Down  State: Detached
ChGr: 32  Mode: LACP
  CH Status      : Up      Elapsed Time: 00:15:16
  Max Active Port: 8
  Description    : lab network
  MAC address    : 0012.e254.ba14  VLAN ID: 4093
  Periodic Timer : Long
  Actor System   : Priority: 128    MAC: 0012.e2a4.fe51  Key: 32
  Partner System : Priority: 128    MAC: 0012.e2a8.85a2  Key: 32
  Port Information
    0/26  Up    State: Distributing
ChGr: 33  Mode: LACP
```

```
  CH Status      : Down    Elapsed Time: -
  Max Active Port: 8
  MAC address    : -               VLAN ID: 4093
  Actor System   : Priority: 128    MAC: 0012.e2a4.fe51  Key: 33
  Partner System : -
  Port Information
    0/22  Up    State: Detached
ChGr: 64  Mode: Static
  CH Status      : Up      Elapsed Time: 00:15:21
  Max Active Port: 8
  MAC address    : 0012.e254.ba12  VLAN ID: 4093
  Port Information
    0/24  Up    State: Distributing

>
```

Figure 14-2 Example of displaying the link aggregation information for a specific channel group number

```
> show channel-group 32

Date 2012/12/06 18:22:11 UTC
ChGr: 32  Mode: LACP
  CH Status      : Up      Elapsed Time: 00:16:40
  Max Active Port: 8
  Description    : lab network
  MAC address    : 0012.e254.ba14  VLAN ID: 4093
  Periodic Timer : Long
  Actor System   : Priority: 128    MAC: 0012.e2a4.fe51  Key: 32
  Partner System : Priority: 128    MAC: 0012.e2a8.85a2  Key: 32
  Port Information
    0/26  Up    State: Distributing

>
```

Display items in Example 1

Table 14-1 Link aggregation information display items

Item	Meaning	Displayed detailed information
ChGr	Channel group number	Channel group number
Mode	Link aggregation mode	`LACP`: LACP link aggregation mode `Static`: Static link aggregation mode `-`: Link aggregation mode is not set.
CH Status	Channel group status	`Up`: Data packets can be sent and received. `Down`: Data packets cannot be sent or received. `Disabled`: Link aggregation is disabled.
Elapsed Time	Time the channel group has been up	*hh*`:`*mm*`:`*ss* (when the elapsed time is less than 24 hours) *ddd*`.`*hh*`:`*mm*`:`*ss* (when the elapsed time exceeds 24 hours) `Over 1000 days` (when the elapsed time is more than 1000 days) `-` is displayed when the channel group status is not Up.

Item	Meaning	Displayed detailed information
Max Active Port	Maximum number of ports used by link aggregation	1 to 8
	Standby link mode	Standby link link-down mode `(link-down mode)`: Link-down mode `(no-link-down mode)`: Link-not-down mode This item is displayed only when there are standby ports.
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. `-` is displayed when the channel group status is not Up.
VLAN ID	VLAN ID to which the channel group belongs	VLAN ID
Periodic Timer	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. This item is not displayed if it has not been set.
Actor System	Information about the actor system	This item is displayed only when LACP mode is enabled.
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. 0 to 65535
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.
Priority	System priority	Priority of the LACP system ID 0 to 65535 can be specified as the priority value (0 indicates the highest priority).

Item		Meaning	Displayed detailed information
MAC		MAC address	MAC address
Key		Group key	0 to 65535
Port Information		Information about the ports managed by the channel group is displayed.	--
<IF#>		Port number	Number of the port whose information is to be displayed
Up		Link status of the port (up)	--
Down		Link status of the port (down)	--
State		Aggregation status of the port	`Detached`[#1]: The port is reserved, a port speed mismatch occurred, or half-duplex mode is set. `Attached`[#1]: The port is in a transition state or is negotiating. `Collecting`: The port is in a transition state or is negotiating (data can be received). `Distributing`: Data can be sent and received. If the status of the port is `Down`, `Detached` is displayed.
Uplink redundant[#2]		Displays uplink redundancy information.	--
Startup active port selection		Setting of the functionality to fix the active port at Switch startup	`primary only`: The functionality to fix the active port at Switch startup is enabled. This item is displayed only when this functionality is enabled.
Switchport backup pairs	Primary	The number of the primary port or the channel group	If an asterisk (`*`) is displayed, the port is an uplink port and the secondary port cannot be used for communication because the functionality to fix the active port at Switch startup is enabled.
	Status	Status of the primary port	`Forwarding`: Forwarding `Blocking`: Blocking `Down`: Link down
	Secondary	The number of the secondary port or the channel group	--
	Status	Status of the secondary port	`Forwarding`: Forwarding `Blocking`: Blocking `Down`: Link down
Preemption	Delay	The time value (in seconds) for automatic or timer switch-back	`-` is displayed when this item is not set.

Item		Meaning	Displayed detailed information
	Limit	The time remaining until a timer switch-back (in seconds)	- is displayed when this item is not set.
Flush	VLAN	VLAN to which flush control frames are sent	1 to 4094: Indicates a VLAN ID. untag: No VLAN is specified. -: Send setting is not set.

#1: In static link aggregation mode, data can be received while the port is in linkup status.

#2: This item is displayed only when uplink redundancy is set in the configuration.

Example 2

Figure 14-3 Example of displaying detailed information about link aggregation

```
> show channel-group detail

Date 2012/12/06 18:22:36 UTC
ChGr: 31  Mode: LACP
  CH Status      : Down    Elapsed Time: -
  Max Active Port: 8
  MAC address    : -               VLAN ID: 4093
  Actor System   : Priority: 128    MAC: 0012.e2a4.fe51  Key: 31
  Partner System : -
  Port Information
  Port: 0/23  Down
    State: Detached      Speed: -      Duplex: -
    Actor   Port  : Priority: 128
  Port: 0/25  Down
    State: Detached      Speed: -      Duplex: -
    Actor   Port  : Priority: 128
ChGr: 32  Mode: LACP
  CH Status      : Up      Elapsed Time: 00:17:04
  Max Active Port: 8
  Description    : lab network
  MAC address    : 0012.e254.ba14  VLAN ID: 4093
  Periodic Timer : Long
  Actor System   : Priority: 128    MAC: 0012.e2a4.fe51  Key: 32
  Partner System : Priority: 128    MAC: 0012.e2a8.85a2  Key: 32
  Port Information
  Port: 0/26  Up
    State: Distributing  Speed: 1G     Duplex: Full
    Actor   Port  : Priority: 128
    Partner System: Priority: 128    MAC: 0012.e2a8.85a2  Key: 32
    Partner Port  : Priority: 128    Number: 23
ChGr: 33  Mode: LACP
  CH Status      : Down    Elapsed Time: -
  Max Active Port: 8
  MAC address    : -               VLAN ID: 4093
  Actor System   : Priority: 128    MAC: 0012.e2a4.fe51  Key: 33
  Partner System : -
  Port Information
  Port: 0/22  Up
    State: Detached      Speed: 1G     Duplex: Full
    Actor   Port  : Priority: 128
ChGr: 64  Mode: Static
  CH Status      : Up      Elapsed Time: 00:17:11
  Max Active Port: 8
  MAC address    : 0012.e254.ba12  VLAN ID: 4093
  Port Information
  Port: 0/24  Up
```

```
    State: Distributing  Speed: 1G     Duplex: Full

>
```

Figure 14-4 Example of displaying the detailed link aggregation information for a specific channel group number

```
> show channel-group 32 detail

Date 2012/12/06 18:22:46 UTC
ChGr: 32  Mode: LACP
  CH Status      : Up      Elapsed Time: 00:17:14
  Max Active Port: 8
  Description    : lab network
  MAC address    : 0012.e254.ba14  VLAN ID: 4093
  Periodic Timer : Long
  Actor System   : Priority: 128    MAC: 0012.e2a4.fe51  Key: 32
  Partner System : Priority: 128    MAC: 0012.e2a8.85a2  Key: 32
  Port Information
  Port: 0/26  Up
    State: Distributing  Speed: 1G     Duplex: Full
    Actor   Port  : Priority: 128
    Partner System: Priority: 128    MAC: 0012.e2a8.85a2  Key: 32
    Partner Port  : Priority: 128    Number: 23

>
```

Display items in Example 2

Table 14-2 Display items for the detailed link aggregation information

Item	Meaning	Displayed detailed information
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
	Standby link mode	Standby link link-down mode `(link-down mode)`: Link-down mode `(no-link-down mode)`:

Item	Meaning	Displayed detailed information
		Link-not-down mode This item is displayed only when there are standby ports.
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. - is displayed when the channel group status is not Up.
VLAN ID	VLAN ID to which the channel group belongs	VLAN ID
Periodic Timer	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. This item is not displayed if it has not been set.
Actor System	Information about the actor system	This item is displayed only when LACP mode is enabled.
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. 0 to 65535
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.
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

Item	Meaning	Displayed detailed information
Port Information	Information about the ports managed by the channel group is displayed.	--
<IF#>	Port number	Number of the port whose information is to be displayed
Up	Link status of the port (up)	--
Down	Link status of the port (down)	--
State	Aggregation status of the port	`Detached`[#1]: The port went down or is reserved, a port speed mismatch occurred, or half-duplex mode is set. `Attached`[#1]: The port is in a transition state or is negotiating. `Collecting`: The port is in a transition state or is negotiating (data can be received). `Distributing`: Data can be sent and received. If the status of the port is `Down`, `Detached` is displayed.
Speed	Line speed	`10M`: 10 Mbit/s
		`100M`: 100 Mbit/s
		`1G`: 1 Gbit/s
		`10G`: 10 Gbit/s
		`-` is displayed if the port status is `Down`.
Duplex	Duplex mode	`Full`: Full duplex
		`Half`: Half duplex
		`-` is displayed if the port status is `Down`.
Actor Port	Actor system port information	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).
Partner System	Information about the partner system	This item is displayed only when LACP mode is used for connection.
Priority	System priority of the partner system	Priority of the LACP system ID 1 to 65535 can be specified as the priority value (1 indicates the highest priority).

Item		Meaning	Displayed detailed information
MAC		MAC address of the partner system	--
Key		Partner system key	0 to 65535
Partner Port		Information about the partner system port	This item is displayed only when LACP mode is used for connection.
Priority		System priority of the partner system	0 to 65535 can be specified as the priority value (0 indicates the highest priority).
Number		Port number of the partner system	--
Uplink redundant#2		Displays uplink redundancy information.	--
Startup active port selection		Setting of the functionality to fix the active port at Switch startup	`primary only`: The functionality to fix the active port at Switch startup is enabled. This item is displayed only when this functionality is enabled.
Switchport backup pairs	Primary	The number of the primary port or the channel group	If an asterisk (`*`) is displayed, the port is an uplink port and the secondary port cannot be used for communication because the functionality to fix the active port at Switch startup is enabled.
	Status	Status of the primary port	`Forwarding`: Forwarding `Blocking`: Blocking `Down`: Link down
	Secondary	The number of the secondary port or the channel group	--
	Status	Status of the secondary port	`Forwarding`: Forwarding `Blocking`: Blocking `Down`: Link down
Preemption	Delay	The time value (in seconds) for automatic or timer switch-back	`-` is displayed when this item is not set.
	Limit	The time remaining until a timer switch-back (in seconds)	`-` is displayed when this item is not set.
Flush	VLAN	VLAN to which MAC address table flush control frames are sent	`1` to `4094`: Indicates a VLAN ID. `untag`: No VLAN is specified. `-`: Send setting is not set.

#1: In static link aggregation mode, data can be received while the port is in linkup status.

#2: This item is displayed only when uplink redundancy is set in the configuration.

Example 3

Figure 14-5 Displaying summary information about link aggregation

```
> show channel-group summary

Date 2012/12/06 18:23:05 UTC
ChGr CH Status  Port
 31  Down       0/23,0/25
 32  Up         0/26
 33  Down       0/22
 64  Up         0/24

>
```

Display items in Example 3

Table 14-3 Display items for the summary information about link aggregation

Item	Meaning	Displayed detailed information
ChGr	Channel group number	Channel group number
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.
Port	Port list of the channel group	`-` is displayed if the port has not been set.

Impact on communication

None

Response messages

Table 14-4 List of response messages for the show channel-group command

Message	Description
There is no information. (channel-group)	There is no `channel-group` information.

Notes

For notes on uplink redundancy, see the description of the `show switchport-backup` command.

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*.

Operation when this parameter is omitted:

Statistics for all link aggregations are displayed.

Operation when all parameters are omitted:

Statistics for sent and received data packets (for each port) in all link aggregations are displayed.

Example 1

Figure 14-6 Example of displaying statistics on sent and received data packets for link aggregation (by port)

```
> show channel-group statistics

Date 2010/09/13 10:54:32 UTC
channel-group counts: 2
ChGr: 1(Up)
 Total:      Octets    Tx:              37208  Rx:            2038024
             Frames    Tx:                575  Rx:              28306
             Discards  Tx:                  0  Rx:                  0
 Port: 0/20  Octets    Tx:              11928  Rx:              22032
             Frames    Tx:                180  Rx:                306
             Discards  Tx:                  0  Rx:                  0
 Port: 0/21  Octets    Tx:               8512  Rx:            1924192
             Frames    Tx:                133  Rx:              26725
             Discards  Tx:                  0  Rx:                  0
 Port: 0/22  Octets    Tx:               8256  Rx:              91800
             Frames    Tx:                129  Rx:               1275
             Discards  Tx:                  0  Rx:                  0
 Port: 0/23  Octets    Tx:               8512  Rx:                  0
             Frames    Tx:                133  Rx:                  0
             Discards  Tx:                  0  Rx:                  0
ChGr: 8(Up)
 Total:      Octets    Tx:              28864  Rx:              59008
             Frames    Tx:                285  Rx:                744
             Discards  Tx:                  0  Rx:                  0
 Port: 0/1   Octets    Tx:               5568  Rx:               6144
             Frames    Tx:                 44  Rx:                 53
```

```
             Discards  Tx:                 0  Rx:                 0
 Port: 0/2   Octets    Tx:              4992  Rx:              4992
             Frames    Tx:                39  Rx:                39
             Discards  Tx:                 0  Rx:                 0
 Port: 0/3   Octets    Tx:              5376  Rx:             40960
             Frames    Tx:                42  Rx:               597
             Discards  Tx:                 0  Rx:                 0
 Port: 0/4   Octets    Tx:              5376  Rx:              5632
             Frames    Tx:                42  Rx:                45
             Discards  Tx:                 0  Rx:                 0
 Port: 0/5   Octets    Tx:                 0  Rx:                 0
             Frames    Tx:                 0  Rx:                 0
             Discards  Tx:                 0  Rx:                 0
 Port: 0/6   Octets    Tx:              7552  Rx:              1280
             Frames    Tx:               118  Rx:                10
             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

>
```

Figure 14-7 Example of displaying statistics on sent and received data packets for a specific channel group number (by port)

```
> show channel-group statistics 8

Date 2010/09/13 11:20:17 UTC
channel-group counts: 1
ChGr: 8(Up)
 Total:      Octets    Tx:         102307556  Rx:            135296
             Frames    Tx:           1598165  Rx:              1715
             Discards  Tx:                 0  Rx:                 0
 Port: 0/1   Octets    Tx:         102262144  Rx:             13312
             Frames    Tx:           1597747  Rx:               109
             Discards  Tx:                 0  Rx:                 0
 Port: 0/2   Octets    Tx:             12160  Rx:             12032
             Frames    Tx:                95  Rx:                94
             Discards  Tx:                 0  Rx:                 0
 Port: 0/3   Octets    Tx:             12544  Rx:             95808
             Frames    Tx:                98  Rx:              1399
             Discards  Tx:                 0  Rx:                 0
 Port: 0/4   Octets    Tx:             13156  Rx:             12864
             Frames    Tx:               107  Rx:               103
             Discards  Tx:                 0  Rx:                 0
 Port: 0/5   Octets    Tx:                 0  Rx:                 0
             Frames    Tx:                 0  Rx:                 0
             Discards  Tx:                 0  Rx:                 0
 Port: 0/6   Octets    Tx:              7552  Rx:              1280
             Frames    Tx:               118  Rx:                10
             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

>
```

Display items in Example 1

Table 14-5 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
ChGr	Channel group number. The status of the channel group is displayed enclosed in parentheses.	Channel group number `Up`: Data packets can be sent and received. `Down`: Data packets cannot be sent or received. `Disabled`: Link aggregation is disabled.
Total	Total statistics	Statistics are displayed for each channel group.
Port	Interface port number	Statistics are displayed for each port.
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

Example 2

Figure 14-8 Displaying statistics for sent and received LACPDUs in link aggregation

```
> show channel-group statistics lacp

Date 2010/09/13 11:21:16 UTC
channel-group counts: 1
ChGr: 8  Port Counts: 8
  Port: 0/1
    TxLACPDUs           :        101   RxLACPDUs   :         99
    TxMarkerResponsePDUs:          0   RxMarkerPDUs:          0
    RxIllegals          :          2   RxUnknowns  :          0
  Port: 0/2
    TxLACPDUs           :         97   RxLACPDUs   :         95
    TxMarkerResponsePDUs:          0   RxMarkerPDUs:          0
    RxIllegals          :          1   RxUnknowns  :          0
  Port: 0/3
    TxLACPDUs           :        100   RxLACPDUs   :         98
    TxMarkerResponsePDUs:          0   RxMarkerPDUs:          0
    RxIllegals          :          2   RxUnknowns  :          0
  Port: 0/4
    TxLACPDUs           :        100   RxLACPDUs   :         99
    TxMarkerResponsePDUs:          0   RxMarkerPDUs:          0
    RxIllegals          :          1   RxUnknowns  :          0
  Port: 0/5
    TxLACPDUs           :          0   RxLACPDUs   :          0
    TxMarkerResponsePDUs:          0   RxMarkerPDUs:          0
```

```
    RxIllegals          :          0   RxUnknowns  :          0
  Port: 0/6
    TxLACPDUs           :          0   RxLACPDUs   :          0
    TxMarkerResponsePDUs:          0   RxMarkerPDUs:          0
    RxIllegals          :          9   RxUnknowns  :          0
  Port: 0/7
    TxLACPDUs           :          0   RxLACPDUs   :          0
    TxMarkerResponsePDUs:          0   RxMarkerPDUs:          0
    RxIllegals          :          0   RxUnknowns  :          0
  Port: 0/8
    TxLACPDUs           :          0   RxLACPDUs   :          0
    TxMarkerResponsePDUs:          0   RxMarkerPDUs:          0
    RxIllegals          :          0   RxUnknowns  :          0

>
```

Figure 14-9 Displaying statistics for sent and received LACPDUs for the specified channel group

```
> show channel-group statistics 8 lacp

Date 2010/09/13 11:21:42 UTC
channel-group counts: 1
ChGr: 8  Port Counts: 8
  Port: 0/1
    TxLACPDUs           :        102   RxLACPDUs   :        100
    TxMarkerResponsePDUs:          0   RxMarkerPDUs:          0
    RxIllegals          :          2   RxUnknowns  :          0
  Port: 0/2
    TxLACPDUs           :         98   RxLACPDUs   :         96
    TxMarkerResponsePDUs:          0   RxMarkerPDUs:          0
    RxIllegals          :          1   RxUnknowns  :          0
  Port: 0/3
    TxLACPDUs           :        101   RxLACPDUs   :         99
    TxMarkerResponsePDUs:          0   RxMarkerPDUs:          0
    RxIllegals          :          2   RxUnknowns  :          0
  Port: 0/4
    TxLACPDUs           :        101   RxLACPDUs   :        100
    TxMarkerResponsePDUs:          0   RxMarkerPDUs:          0
    RxIllegals          :          1   RxUnknowns  :          0
  Port: 0/5
    TxLACPDUs           :          0   RxLACPDUs   :          0
    TxMarkerResponsePDUs:          0   RxMarkerPDUs:          0
    RxIllegals          :          0   RxUnknowns  :          0
  Port: 0/6
    TxLACPDUs           :          0   RxLACPDUs   :          0
    TxMarkerResponsePDUs:          0   RxMarkerPDUs:          0
    RxIllegals          :          9   RxUnknowns  :          0
  Port: 0/7
    TxLACPDUs           :          0   RxLACPDUs   :          0
    TxMarkerResponsePDUs:          0   RxMarkerPDUs:          0
    RxIllegals          :          0   RxUnknowns  :          0
  Port: 0/8
    TxLACPDUs           :          0   RxLACPDUs   :          0
    TxMarkerResponsePDUs:          0   RxMarkerPDUs:          0
    RxIllegals          :          0   RxUnknowns  :          0

>
```

Display items in Example 2

Table 14-6 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	Interface port number	--
TxLACPDUs	Number of sent LACPDUs	--
RxLACPDUs	Number of received LACPDUs	--
Tx MarkerResponsePDUs	Number of sent marker response PDUs	--
RxMarkerPDUs	Number of received marker PDUs	--
RxIllegals	Number of discarded received PDUs	Invalid PDUs
RxUnknowns	Number of discarded received PDUs	Unknown PDUs

Impact on communication

None

Response messages

Table 14-7 List of response messages for the show channel-group statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no information. (channel-group statistics)	There is no `channel-group statistics` information.

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, to zero, the statistics for sent and received LACPDUs in link aggregation.

Syntax

```
clear channel-group statistics lacp
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 14-10 Clearing statistics on sent and received LACPDUs for link aggregation

```
> clear channel-group statistics lacp

>
```

Display items

None

Impact on communication

None

Response messages

Table 14-8 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.
There is no information. (channel-group statistics)	There is no `channel-group statistics` information.

Notes

- This command clears only LACPDU statistics. It cannot clear the statistics for the data packets for each channel group. Also 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 the configuration is deleted or added, the relevant LACPDU statistics are cleared to zero.

15. MAC Address Table

show mac-address-table
clear mac-address-table

show mac-address-table

Displays information about the MAC address table.

Syntax

```
show mac-address-table [mac <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>]
```

Input mode

User mode and administrator mode

Parameters

mac *<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*.

Operation when this parameter is omitted:

Displays the information in the MAC address table for all VLANs.

[port *<Port# list>*] [channel-group-number *<Channel group# list>*]

Displays the information in the MAC address table for the specified ports or the specified link aggregation groups. Ports and link aggregation groups cannot be specified at the same time.

port *<Port# list>*

Displays the information in the MAC address table for the ports specified in list format. The MAC address 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.

Operation when this parameter is omitted:

The information in the MAC address table for all ports and link aggregation 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 functionality.

dot1x

Displays the information in the MAC address table registered by using the IEEE 802.1X functionality.

wa

Displays the information in the MAC address table registered by using the Web authentication functionality.

macauth

Displays the information in the MAC address table registered by using the MAC-based authentication functionality.

learning-counter

Displays the number of learned addresses in the MAC address table for each port.

Note on setting parameters

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 each parameter condition will be displayed.

Operation when all parameters are omitted:

Displays all information about the MAC address table.

Example 1

Figure 15-1 Displaying all information in a MAC address table

```
> show mac-address-table

Date 2010/08/09 21:30:08 UTC
Aging time : 300
MAC address        VLAN    Type     Port-list
0012.e2cf.fd5d        1    Dot1x    0/6
0012.e203.0110        1    Dynamic  0/15
0012.e203.0132        1    Dynamic  0/49
0012.e200.00fb        1    Snoop    0/3,0/6-15,0/18-22,0/24-32,0/34-44,0/48-49
0012.e27f.fffa        1    Snoop    0/6
0012.e2a5.429c        2    Dynamic  0/24,0/48
0012.e2a5.e756        2    MacAuth  0/50
0012.e2a5.e895     4094    Static   0/24,0/48
0012.e2a5.ee4e     4094    WebAuth  0/5

>
```

Display items in Example 1

Table 15-1 Display items for the information in the MAC address table

Item	Meaning	Displayed detailed information
Aging time	Aging time in the MAC address table	`Infinity` is displayed if aging is not performed.

Item	Meaning	Displayed detailed information
MAC address	MAC address	--
VLAN	VLAN ID	--
Type	Type of MAC address table entry	`Dynamic`: Entry registered dynamically `Snoop`: Entry registered by using the IGMP snooping or MLD snooping functionality `Static`: Entry registered statically `Dot1x`: Entry registered after authentication by the IEEE 802.1X functionality (port-based authentication) `WebAuth`: Entry registered after authentication by Web authentication `MacAuth`: Entry registered after authentication by MAC-based authentication
Port-list	Port (Interface port number or peer link)	Interface port number: The port number to which the MAC address belongs `Drop`: The port to which a MAC address belongs does not exist. (The channel group to which the port belongs is not in the `Up` state.)# `peer-link`: The entry that was learned on either of the following: ● A single port of the neighboring device ● An SML channel group that is active only on the neighboring device (displayed during SML operation only)

#: When the frames that match MAC address and VLAN are received, the frames are discarded.

Example 2

Figure 15-2 Displaying the status of learning in the MAC address table

```
> show mac-address-table learning-counter

Date 2010/08/09 21:47:47 UTC
 Port          Count
 0/1               0
 0/2           13961
 0/3              12
 0/4               2
 0/5               0
  :
  :
 ChGr:8            0
 ChGr:62          13
 ChGr:63           1
 ChGr:64          34

>
```

Display items in Example 2

Table 15-2 Display items for the status of learning in the MAC address table

Item	Meaning	Displayed detailed information
Port	Port (Interface port number or peer link)	Interface port number: The port number to which the MAC address belongs Drop: The port to which a MAC address belongs does not exist. (The channel group to which the port belongs is not in the Up state.)# peer-link: The entry that was learned on either of the following: ● A single port of the neighboring device ● An SML channel group that is active only on the neighboring device (displayed during SML operation only)
Count	Number of learnt entries in the current MAC address table	--

#: When the frames that match MAC address and VLAN are received, the frames are discarded.

Impact on communication

None

Response messages

Table 15-3 List of response messages for the show mac-address-table command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no information. (mac-address-table)	There is no information in the MAC address table.

Notes

This command does not display information for undefined channel group numbers.

clear mac-address-table

Clears the information in the MAC address table registered dynamically through MAC address learning.

Syntax

```
clear mac-address-table [-f]
```

Input mode

User mode and administrator mode

Parameters

-f

Clears information in the MAC address table without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

Figure 15-3 Clearing information in the MAC address table

```
> clear mac-address-table
Do you wish to clear mac-address-table? (y/n): y

>
```

If `y` is entered, the information in the MAC address table is cleared.

If `n` is entered, the information in the MAC address table is not cleared.

Display items

None

Impact on communication

Frames are flooded until learning is completed again. Execute this command at a time when flooding will have a minimal impact.

Response messages

Table 15-4 List of response messages for the clear mac-address-table command

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

Notes

This command clears all information in the MAC address table with the exception of static entries. During clear processing, learning is not performed for the MAC address table. Processing by this command might take as much as 10 seconds or more.

16. VLAN

show vlan
show vlan mac-vlan

show vlan

Displays various VLAN statuses and the status of accommodated lines.

Syntax

```
show vlan [{<vlan id list> | port <port list> | channel-group-number
          <channel group list>}][{summary | detail | list}]
```

Input mode

User mode and administrator mode

Parameters

{ *<vlan id list>* | port *<port list>* | channel-group-number *<channel group list>*}

<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*.

port *<port list>*

Displays the VLAN information for the port numbers specified in list format. All the VLAN information that includes one or more ports specified in the list 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>*

Displays VLAN 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*.

Operation when this parameter is omitted:

All VLAN information is displayed according to the `summary`, `detail`, or `list` option specified.

{summary | detail | list}

summary

Displays the VLAN summary information.

detail

Displays detailed information about VLANs.

list

Displays VLAN information with the information for one VLAN being displayed on one line.

Operation when this parameter is omitted:

Displays VLAN information.

Operation when all parameters are omitted:

Displays all VLAN information.

Example 1

The following shows an example of displaying the statuses of all configured VLANs and the status of accommodated ports.

Figure 16-1 Example of displaying VLAN information

```
> show vlan
```

```
Date 2012/02/27 08:57:56 UTC
VLAN counts: 6
VLAN ID: 1     Type: Port based      Status: Up
  Learning: On            Tag-Translation:
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN0001
  IP Address:
  Source MAC address: 0012.e262.1fdf(System)
  Description: VLAN0001
  Spanning Tree: None(-)
  AXRP RING ID:       AXRP VLAN group:
  IGMP snooping:      MLD snooping:
  Untagged(43)  : 0/1-9,0/13,0/16-17,0/20-21,0/23,0/25-52
  Tagged(0)     :
VLAN ID: 10    Type: Port based      Status: Down
  Learning: On            Tag-Translation:
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN0010
  IP Address:
  Source MAC address: 0012.e262.1fdf(System)
  Description: VLAN0010
  Spanning Tree: None(-)
  AXRP RING ID: 200   AXRP VLAN group: Control-VLAN
  IGMP snooping:      MLD snooping:
  Untagged(0)   :
  Tagged(4)     : 0/18-19,0/22,0/24
VLAN ID: 20    Type: Port based      Status: Up
  Learning: On            Tag-Translation:
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN0020
  IP Address:
  Source MAC address: 0012.e262.1fdf(System)
  Description: Ring-VL
  Spanning Tree: PVST+(802.1D)
  AXRP RING ID: 200   AXRP VLAN group: 1
  AXRP Virtual-Link-VLAN
  IGMP snooping:      MLD snooping:
  Untagged(0)   :
  Tagged(4)     : 0/18-19,0/22,0/24
VLAN ID: 30    Type: Protocol based  Status: Up
  Protocol VLAN Information  Name:
  EtherType:  LLC:  Snap-EtherType:
  Learning: On            Tag-Translation:
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN0030
  IP Address:
  Source MAC address: 0012.e262.1fdf(System)
  Description: VLAN0030
  Spanning Tree: None(-)
  AXRP RING ID: 200   AXRP VLAN group: 2
  IGMP snooping:      MLD snooping:
  Untagged(2)   : 0/3,0/13
  Tagged(4)     : 0/18-19,0/22,0/24
VLAN ID: 51    Type: MAC based       Status: Up
  Learning: On            Tag-Translation:
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN0051
  IP Address: 10.215.196.1/23
              3ffe:501:811:ff08::5/64
              fe80::212:e2ff:fe62:1fdf/64
  Source MAC address: 0012.e262.1fdf(System)
  Description: IPv4/IPv6
  Spanning Tree: None(-)
```

```
  AXRP RING ID:       AXRP VLAN group:
  IGMP snooping:      MLD snooping:
  Untagged(3)   : 0/6,0/16,0/20
  Tagged(0)     :
VLAN ID: 4094  Type: Port based      Status: Up
  Learning: On            Tag-Translation: On
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN4094
  IP Address:
  Source MAC address: 0012.e262.1fdf(System)
  Description: VLAN4094
  Spanning Tree: None(-)
  AXRP RING ID:       AXRP VLAN group:
  IGMP snooping:      MLD snooping:
  Untagged(0)   :
  Tagged(5)     : 0/10-12,0/14-15
  Tag-Trans(5)  : 0/10-12,0/14-15

>
```

Figure 16-2 Example of displaying VLAN information for a specific port

```
> show vlan port 0/6

Date 2012/02/27 08:59:36 UTC
VLAN counts: 2
VLAN ID: 1     Type: Port based      Status: Up
  Learning: On            Tag-Translation:
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN0001
  IP Address:
  Source MAC address: 0012.e262.1fdf(System)
  Description: VLAN0001
  Spanning Tree: None(-)
  AXRP RING ID:       AXRP VLAN group:
  IGMP snooping:      MLD snooping:
  Untagged(43)  : 0/1-9,0/13,0/16-17,0/20-21,0/23,0/25-52
  Tagged(0)     :
VLAN ID: 51    Type: MAC based       Status: Up
  Learning: On            Tag-Translation:
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN0051
  IP Address: 10.215.196.1/23
              3ffe:501:811:ff08::5/64
              fe80::212:e2ff:fe62:1fdf/64
  Source MAC address: 0012.e262.1fdf(System)
  Description: IPv4/IPv6
  Spanning Tree: None(-)
  AXRP RING ID:       AXRP VLAN group:
  IGMP snooping:      MLD snooping:
  Untagged(3)   : 0/6,0/16,0/20
  Tagged(0)     :

>
```

Display items in Example 1

Table 16-1 Basic display items for VLANs

Item	Meaning	Displayed detailed information
VLAN counts	Number of target VLANs	--

Item	Meaning	Displayed detailed information
VLAN tunneling enabled	VLAN tunneling information	VLAN tunneling is enabled. (This item is displayed only when VLAN tunneling 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 Up status. `Down`: Indicates Down status. `Disabled`: Indicates Disabled status
Protocol VLAN Information	Protocol VLAN information	This item is displayed only for a protocol VLAN.
Name	Protocol 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 information	Blank: No setting `On`: Tag translation is being used.
BPDU Forwarding	BPDU forwarding	Blank: No setting `On`: BPDU forwarding functionality is being used.
EAPOL Forwarding	EAPOL forwarding	Blank: No setting `On`: EAPOL forwarding functionality is being used.
Router Interface Name	Interface name	Displays the name of the interface assigned to the VLAN.
IP Address	IP address (/mask)	Blank: No setting
Source MAC address	Source MAC address used during Layer 3 communication	`System`: The MAC address for the device is used.
Description	Description	The character string set for the VLAN name is displayed. `VLAN`*xxxx* is displayed if this item is not set. (*xxxx*: VLAN ID)

Item	Meaning	Displayed detailed information
Spanning Tree	Spanning Tree Protocol being used	`Single (802.1D)`: IEEE 802.1D is used for the entire Switch. `Single (802.1w)`: IEEE 802.1w is used for the entire Switch. `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. `None (-)`: Displayed when this item is not set.
AXRP RING ID	Ring Protocol ring ID	Blank: No setting
AXRP VLAN group	ID of the VLAN group using the Ring Protocol functionality or the control VLAN	Blank: No setting `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 functionality.	This item is displayed when the VLAN is assigned to the virtual link VLAN for the Ring Protocol functionality.
IGMP snooping	Setting status of IGMP snooping	Blank: No setting `On`: IGMP snooping is being used.
MLD snooping	Setting status of MLD snooping	Blank: No setting `On`: MLD snooping is being used.
Untagged(n)	Untagged port	*n*: Number of applicable ports Port list This item includes ports that automatically participate in the VLAN through automatic VLAN assignment.
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

Example 2

The following shows an example of displaying summary information about all configured VLANs.

Figure 16-3 Example of displaying VLAN summary information

```
> show vlan summary

Date 2012/02/27 08:59:46 UTC
Total(6)           : 1,10,20,30,51,4094
Port based(4)      : 1,10,20,4094
Protocol based(1)  : 30
MAC based(1)       : 51

>
```

Display items in Example 2

Table 16-2 Display items of VLAN summary

Item	Meaning	Displayed detailed information
Total(n)	Applicable VLAN information	*n*: Number of applicable VLANs n=0: Blank VLAN ID list
Port based(n)	Port VLAN information	*n*: Number of applicable VLANs n=0: Blank VLAN ID list
Protocol based(n)	Protocol VLAN information	*n*: Number of applicable VLANs n=0: Blank VLAN ID list
MAC based(n)	MAC VLAN information	*n*: Number of applicable VLANs n=0: Blank VLAN ID list

Example 3

The following shows an example of displaying VLAN detailed information when a VLAN ID is specified.

Figure 16-4 Example of displaying VLAN detailed information for a specific VLAN ID

```
> show vlan 10,4094 detail

Date 2012/02/27 09:00:00 UTC
VLAN counts: 2
VLAN ID: 10    Type: Port based      Status: Down
  Learning: On            Tag-Translation:
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN0010
  IP Address:
  Source MAC address: 0012.e262.1fdf(System)
  Description: VLAN0010
  Spanning Tree: None(-)
  AXRP RING ID: 200   AXRP VLAN group: Control-VLAN
  IGMP snooping:      MLD snooping:
  Port Information
   0/18(ChGr:9)  Down -               Tagged
   0/19(ChGr:9)  Down -               Tagged
   0/22(ChGr:9)  Down -               Tagged
   0/24          Up   Blocking(AXRP)  Tagged
VLAN ID: 4094  Type: Port based      Status: Up
  Learning: On            Tag-Translation: On
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN4094
  IP Address:
  Source MAC address: 0012.e262.1fdf(System)
  Description: VLAN4094
  Spanning Tree: None(-)
  AXRP RING ID:       AXRP VLAN group:
  IGMP snooping:      MLD snooping:
  Port Information
   0/10(ChGr:64) Up   Forwarding      Tagged   Tag-Translation:4093
   0/11(ChGr:64) Up   Forwarding      Tagged   Tag-Translation:4093
```

```
0/12(ChGr:64) Down -              Tagged   Tag-Translation:4093
0/14(ChGr:64) Up   Forwarding     Tagged   Tag-Translation:4093
0/15(ChGr:64) Down -              Tagged   Tag-Translation:4093

>
```

Display items in Example 3

Table 16-3 Display items of detailed VLAN information

Item	Meaning	Displayed detailed information
VLAN counts	Number of applicable VLANs	--
VLAN tunneling enabled	VLAN tunneling information	VLAN tunneling is enabled. (This item is displayed only when VLAN tunneling 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 Up status. `Down`: Indicates Down status. `Disabled`: Indicates Disabled status
Protocol VLAN Information	Protocol VLAN information	This item is displayed only for a protocol VLAN.
Name	Protocol 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 information	Blank: No setting `On`: Tag translation is being used.
BPDU Forwarding	BPDU forwarding	Blank: No setting `On`: BPDU forwarding functionality is being used.
EAPOL Forwarding	EAPOL forwarding	Blank: No setting `On`: EAPOL forwarding functionality is being used.
Router Interface Name	Interface name	Displays the name of the interface assigned to the VLAN.

Item	Meaning	Displayed detailed information
IP Address	IP address (/mask)	Blank: No setting
Source MAC address	Source MAC address used during Layer 3 communication	`System`: The MAC address for the device is used.
Description	Description	The character string set for the VLAN name is displayed. `VLAN`*xxxx* is displayed if this item is not set. (*xxxx*: VLAN ID)
Spanning Tree	Spanning Tree Protocol being used	`Single (802.1D)`: IEEE 802.1D is used for the entire Switch. `Single (802.1w)`: IEEE 802.1w is used for the entire Switch. `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. `None (-)`: Displayed when this item is not set.
AXRP RING ID	Ring Protocol ring ID	Blank: No setting
AXRP VLAN group	ID of the VLAN group using the Ring Protocol functionality or the control VLAN	Blank: No setting `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 functionality.	This item is displayed when the VLAN is assigned to the virtual link VLAN for the Ring Protocol functionality.
IGMP snooping	Setting status of IGMP snooping	Blank: No setting `On`: IGMP snooping is being used.
MLD snooping	Setting status of MLD snooping	Blank: No setting `On`: MLD snooping is being used.
Port Information	Port information (Interface port number)	`No Port` is displayed if there is no port information for the VLAN. This item includes ports that automatically participate in the VLAN through automatic VLAN assignment.
ChGr	Channel group number	This item is not displayed for the ports that do not belong to the channel group.
<line-status>	Port state	`Up`: Indicates that the port status is Up. `Down`: Indicates that the port status is Down.

Item	Meaning	Displayed detailed information
<data-forwarding-status>	Data forwarding status	`Forwarding`: Data is being forwarded. `Blocking`: Data forwarding is blocked. `(VLAN)`: The VLAN is disabled. `(CH)`: Data forwarding has been stopped by link aggregation. `(STP)`: Data forwarding has been stopped by STP. `(dot1x)`: Data forwarding has been stopped by the IEEE 802.1x functionality. `(ULR)`: Data forwarding has been stopped by ULR. `(AXRP)`: Data forwarding has been stopped by the Ring Protocol. `-`: The port status is Down.
Tag	Tag setting status	`Untagged`: Untagged port `Tagged`: Tagged port
Tag-Translation	ID subject to tag translation	1 to 4094

Example 4

The following shows an example of displaying VLAN information in list format.

Figure 16-5 Example of displaying VLAN information in list format

```
> show vlan list

Date 2012/02/27 09:00:09 UTC
VLAN counts: 6
ID   Status   Fwd/Up /Cfg Name            Type  Protocol        Ext.  IP
   1 Up         3/  3/ 43 VLAN0001        Port  -               - -   -
  10 Down       0/  1/  4 VLAN0010        Port  AXRP (C)        - -   -
  20 Up         1/  1/  4 Ring-VL         Port  -               - -   -
  30 Up         1/  1/  6 VLAN0030        Proto AXRP (-)        - -   -
  51 Up         1/  1/  3 IPv4/IPv6       MAC   -               - -   4/6
4094 Up         3/  3/  5 VLAN4094        Port  -               - T   -
     AXRP (C:Control-VLAN)
     S:IGMP/MLD snooping  T:Tag Translation
     4:IPv4 address configured  6:IPv6 address configured

>
```

Figure 16-6 Example of displaying VLAN information in list format (when the Ring Protocol is used)

```
> show vlan list

Date 2012/02/27 09:17:57 UTC
VLAN counts: 4
ID   Status   Fwd/Up /Cfg Name            Type  Protocol        Ext.  IP
   1 Up         2/  2/  2 VLAN0001        Port  AXRP (-)        - -   -
   5 Up         2/  2/  2 VLAN0005        Port  AXRP (C)        - -   -
  10 Up         2/  2/  2 VLAN0010        Port  AXRP (-)        - -   -
  20 Up         4/  4/  4 VLAN0020        Port  AXRP (-)        - -   -
     AXRP (C:Control-VLAN)
     S:IGMP/MLD snooping  T:Tag Translation
     4:IPv4 address configured  6:IPv6 address configured
```

```
>
```

Figure 16-7 Example of displaying VLAN information in list format (when both the Ring Protocol and STP are used)

```
> show vlan list

Date 2012/02/28 12:05:42 UTC
VLAN counts: 4
ID   Status   Fwd/Up /Cfg Name            Type  Protocol         Ext.  IP
   1 Up         3/  3/  3 VLAN0001        Port  STP Single:1D    - -   -
   5 Up         2/  2/  2 VLAN0005        Port  AXRP (C)         - -   -
  10 Up         3/  3/  3 VLAN0010        Port  STP PVST+:1D     - -   -
  20 Up         3/  3/  3 VLAN0020        Port  STP Single:1D    - -   -
     AXRP (C:Control-VLAN)
     S:IGMP/MLD snooping  T:Tag Translation
     4:IPv4 address configured  6:IPv6 address configured

>
```

Display items in Example 4

Table 16-4 Display items for VLAN information in list format

Item	Meaning	Displayed detailed information
VLAN counts	Number of applicable VLANs	--
VLAN tunneling enabled	VLAN tunneling information	VLAN tunneling is enabled. (This item is displayed only when VLAN tunneling is used.)
ID	VLAN ID	VLAN ID
Status	VLAN status	`Up`: Indicates Up status. `Down`: Indicates Down status. `Disabled`: Indicates Disabled status
Fwd	Number of ports in `Forward` status	The number of ports belonging to the VLAN that are in `Forward` status This item includes ports that automatically participate in the VLAN through automatic VLAN assignment.
Up	Number of ports in `Up` status	The number of ports belonging to the VLAN that are in `Up` status This item includes ports that automatically participate in the VLAN through automatic VLAN assignment.
Cfg	Number of VLAN ports	The number of ports belonging to the VLAN This item includes ports that automatically participate in the VLAN through automatic VLAN assignment.
Name	VLAN name	The first 14 characters of the character string set for the VLAN name are displayed. `VLAN`*xxxx* is displayed if this item is not set. (*xxxx*: VLAN ID)

Item	Meaning	Displayed detailed information
Type	VLAN type	`Port`: Port VLAN `Proto`: Protocol VLAN `Mac`: MAC VLAN
Protocol	STP information, Ring Protocol information	For STP: `STP` *<type>*`:` *<protocol>* *<type>*: `Single`, `PVST+`, or `MSTP` *<protocol>*:`802.1D`, `802.1W`, or `802.1S` For the Ring Protocol: AXRP `(C)`: Indicates that the control VLAN is assigned. (`(-)` is displayed if the control VLAN is not assigned. Note, however, that `(-)` is not displayed for a VLAN that co-exists with other protocols.) If nothing is specified: a hyphen (`-`) is displayed.
Ext.	Extended functionality information	`S`: Indicates that IGMP snooping or MLD snooping is set. `T`: Indicates that tag translation is set. `-`: Indicates that the relevant functionality is not set.
IP	IP address setting information	`4`: Indicates that an IPv4 address is set. `6`: Indicates that an IPv6 address is set. `4/6`: Indicates that both an IPv4 address and an IPv6 address are set. `-`: Indicates that an IP address is not set for the VLAN.

Impact on communication

None

Response messages

Table 16-5 List of response messages for the show vlan command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no information. (vlan)	No information was found.

Notes

In the following situation, the `show vlan` command displays and counts the MAC VLANs assigned by automatic VLAN assignment: if the `switchport mac` configuration command with the `vlan` parameter specified has not been executed for MAC ports that were placed in IEEE 802.1X port-based authentication (dynamic), or placed in dynamic VLAN mode for Web authentication, or placed in dynamic VLAN mode for MAC-based authentication.

show vlan mac-vlan

Displays 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 the 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*.

Operation when this parameter is omitted:

Displays the MAC VLAN information for all VLANs.

{ 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 Layer 2 authentication.

Operation when this parameter is omitted:

Displays the MAC address information registered for `static` and `dynamic`.

<mac>

Displays VLANs for which the specified MAC address is registered.

The MAC address information in the configuration disabled by hardware conditions is also displayed.

Operation when all parameters are omitted:

Displays all MAC VLAN information.

Example

The following shows an example of displaying information related to MAC VLANs from the information for all configured VLANs.

Figure 16-8 Example of displaying MAC VLAN information

```
> show vlan mac-vlan

Date 2010/09/17 06:12:04 UTC
VLAN counts: 1    Total MAC Counts: 3
VLAN ID: 100         MAC Counts: 3
   0000.e22b.ffdd(mac-auth)   000b.972f.e22b(mac-auth)
   0050.daba.4fc8(mac-auth)

>
```

Display items

Table 16-6 Display items for MAC VLAN information

Item	Meaning	Displayed detailed information
VLAN counts	Number of displayed MAC VLANs	--
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 functionality registered the address. `static`: Indicates that the address was registered by configuration. `dot1x`: Indicates that the address was registered by IEEE 802.1X authentication. `web-auth`: Indicates that the address was registered by Web authentication. `mac-auth`: Indicates that the address was registered by MAC-based authentication. *: Indicates that the entry has not been registered on hardware due to capacity limits.

Impact on communication

None

Response messages

Table 16-7 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.
There is no information. (vlan mac-vlan)	No MAC VLAN information was found.

Notes

None

17. Spanning Tree Protocols

show spanning-tree
show spanning-tree statistics
clear spanning-tree statistics
clear spanning-tree detected-protocol
show spanning-tree port-count

show spanning-tree

Displays 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*.

Operation when this parameter is omitted:

Statistics for all VLANs for which PVST+ is running are displayed.

single

Displays information about Single Spanning Tree.

mst

Displays information about Multiple Spanning Tree.

instance *<mst instance id list>*

Displays information about Multiple Spanning Tree for the MST instance IDs specified in list format. Specifiable values for 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.

Operation 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. 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.

Note on setting parameters

This command can display only the information relevant to the condition applied by a

parameter that has been set. If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information that meets the conditions will be displayed.

detail

Displays detailed information about Spanning Tree Protocols.

Operation when this parameter is omitted:

Displays Spanning Tree information.

active

Displays port information for only those ports in the Up status.

Operation when this parameter is omitted:

Displays information for all ports.

Operation when all parameters are omitted:

Displays Spanning Tree information for Single Spanning Tree, PVST+, and Multiple Spanning Tree.

Example 1

Figure 17-1 Example of displaying PVST+ Spanning Tree information

```
> show spanning-tree vlan 1-4094

Date 2010/09/14 11:22:22 UTC
VLAN 1  PVST+ Spanning Tree:Enabled   Mode:PVST+
  Bridge ID       Priority: 32769     MAC Address: 00ed.f010.0001
    Bridge Status: Designated
  Root Bridge ID  Priority: 32769     MAC Address: 0012.e2c4.2772
    Root Cost: 19
    Root Port: 0/24
  Port Information
    0/14      Down Status:Disabled    Role:-            PortFast
    0/16      Down Status:Disabled    Role:-            PortFast
    0/23      Down Status:Disabled    Role:-            -
    0/24      Up   Status:Forwarding  Role:Root         -
    0/25      Down Status:Disabled    Role:-            LoopGuard
    0/26      Down Status:Disabled    Role:-            LoopGuard
VLAN 2  PVST+ Spanning Tree:Enabled   Mode:PVST+
  Bridge ID       Priority: 32770     MAC Address: 00ed.f010.0001
    Bridge Status: Designated
  Root Bridge ID  Priority: 32770     MAC Address: 0012.e2c4.2772
    Root Cost: 19
    Root Port: 0/12
  Port Information
    0/1       Up   Status:Blocking    Role:Designated   RootGuard
    0/2       Down Status:Disabled    Role:-            RootGuard
    0/3       Down Status:Disabled    Role:-            -
    0/4       Down Status:Disabled    Role:-            -
    0/5       Down Status:Disabled    Role:-            -
    0/6       Down Status:Disabled    Role:-            -
    0/7       Down Status:Disabled    Role:-            RootGuard
    0/8       Down Status:Disabled    Role:-            RootGuard
    0/11      Down Status:Disabled    Role:-            LoopGuard
    0/12      Up   Status:Forwarding  Role:Root         LoopGuard
    ChGr:1    Up   Status:Blocking    Role:Designated   RootGuard
VLAN 4094  PVST+ Spanning Tree:Enabled   Mode:PVST+
  Bridge ID       Priority: 36862     MAC Address: 00ed.f010.0001
    Bridge Status: Designated
  Root Bridge ID  Priority: 36862     MAC Address: 0012.e2c4.2772
    Root Cost: 19
    Root Port: 0/20
```

```
            Port Information
              0/17      Down Status:Disabled    Role:-            LoopGuard
              0/18      Down Status:Disabled    Role:-            LoopGuard
              0/19      Down Status:Disabled    Role:-            LoopGuard
              0/20      Up   Status:Forwarding  Role:Root         PortFast
              0/21      Down Status:Disabled    Role:-            -
              0/22      Up   Status:Blocking    Role:Alternate    -
              ChGr:8    Down Status:Disabled    Role:-            RootGuard

           >
```

Display items in Example 1

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:	Operating status of the PVST+ Spanning Tree Protocol	`Enabled`: The Spanning Tree Protocol is running. `Disabled`: The Spanning Tree Protocols 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 on 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 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

Item	Meaning	Displayed detailed information
		bridge.
Port Information	Displays information about the ports managed by the PVST+ Spanning Tree Protocol.	
<IF#>	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 the `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 the `Down` status.
Status	Port state	If `Mode` is `PVST+`: `Blocking`: Blocking `Listening`: Listening `Learning`: Learning `Forwarding`: Indicates Forwarding status. `Disabled`: Disabled If `Mode` is `Rapid PVST+`: `Discarding`: Discarding `Learning`: Learning `Forwarding`: Indicates Forwarding status. `Disabled`: Disabled This parameter becomes `Disabled` if the port is in the `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 the `Down` status, a hyphen (`-`) is displayed, because ports in this status are not included in the topology calculations. These parameters are commonly used when `Mode` is `PVST+` or `Rapid PVST+`.
PortFast	PortFast	Indicates that the port is a PortFast port.
PortFast(BPDU Guard)	PortFast (BPDU guard functionality is applied)	Indicates that the port is a PortFast port, and that the BPDU guard functionality is applied.

Item	Meaning	Displayed detailed information
BPDU Filter	BPDU filter	Indicates that the BPDU filter functionality is applied.
LoopGuard	Loop guard	Indicates that the port applies the loop guard functionality.
RootGuard	Root guard	Indicates that the port applies the root guard functionality.
Compatible	Compatible mode	Indicates that the port is operating in compatible mode when `Mode` for the Spanning Tree Protocol is `Rapid PVST+`. Ports operating in compatible mode do not perform rapid status transitions.

Example 2

Figure 17-2 Example of displaying information about Single Spanning Tree

```
> show spanning-tree single

Date 2010/09/14 11:38:40 UTC
Single Spanning Tree:Enabled   Mode:STP
  Bridge ID       Priority: 32768     MAC Address: 00ed.f010.0001
    Bridge Status: Root
  Root Bridge ID  Priority: 32768     MAC Address: 00ed.f010.0001
    Root Cost: 0
    Root Port: -
  Port Information
    0/1       Up   Status:Learning    Role:Designated   RootGuard
    0/2       Down Status:Disabled    Role:-            RootGuard
    0/3       Down Status:Disabled    Role:-            -
    0/4       Down Status:Disabled    Role:-            -
    0/5       Down Status:Disabled    Role:-            -
    0/6       Down Status:Disabled    Role:-            -
    0/7       Down Status:Disabled    Role:-            RootGuard
    0/8       Down Status:Disabled    Role:-            RootGuard
    0/11      Down Status:Disabled    Role:-            LoopGuard
    0/12      Up   Status:Blocking    Role:Alternate    LoopGuard
    0/14      Down Status:Disabled    Role:-            PortFast
    0/16      Down Status:Disabled    Role:-            PortFast
    0/17      Down Status:Disabled    Role:-            LoopGuard
    0/18      Down Status:Disabled    Role:-            LoopGuard
    0/19      Down Status:Disabled    Role:-            LoopGuard
    0/20      Up   Status:Forwarding  Role:Designated   PortFast
    0/21      Down Status:Disabled    Role:-            -
    0/22      Up   Status:Learning    Role:Designated   -
    0/23      Down Status:Disabled    Role:-            -
    0/24      Up   Status:Learning    Role:Designated   -
    0/25      Down Status:Disabled    Role:-            LoopGuard
    0/26      Down Status:Disabled    Role:-            LoopGuard
    ChGr:1    Up   Status:Learning    Role:Designated   RootGuard
    ChGr:8    Down Status:Disabled    Role:-            RootGuard

>
```

Display items in Example 2

Item	Meaning	Displayed detailed information
Single Spanning Tree:	Operating status of the 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 on 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 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.	
<IF#>	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 the `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 the `Down` status.
Status	Port state	If `Mode` is `STP`: `Blocking`: Blocking `Listening`: Listening `Learning`: Learning `Forwarding`: Indicates Forwarding status. `Disabled`: Disabled If `Mode` is `Rapid STP`: `Discarding`: Discarding `Learning`: Learning `Forwarding`: Indicates Forwarding status. `Disabled`: Disabled This parameter becomes `Disabled` if the port is in the `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 the `Down` status, a hyphen (`-`) is displayed, because ports in this status are not included in the topology calculations. These parameters are commonly used when `Mode` is `STP` or `Rapid STP`.
PortFast	PortFast	Indicates that the port is a PortFast port.
PortFast(BPDU Guard)	PortFast (BPDU guard functionality is applied)	Indicates that the port is a PortFast port, and that the BPDU guard functionality is applied.
BPDU Filter	BPDU filter	Indicates that the BPDU filter functionality is applied.
LoopGuard	Loop guard	Indicates that the port applies the loop guard functionality.
RootGuard	Root guard	Indicates that the port applies the root guard functionality.
Compatible	Compatible mode	Indicates that the port is operating in compatible mode when `Mode` for the Spanning Tree Protocol is `Rapid STP`. Ports operating in compatible mode do not perform rapid status transitions.

Example 3

Figure 17-3 Example of displaying information about Multiple Spanning Tree

```
> show spanning-tree mst instance 1-4095
```

```
Date 2010/09/14 13:04:05 UTC
Multiple Spanning Tree: Enabled
Revision Level: 0      Configuration Name:
MST Instance 1
  VLAN Mapped: 2
  Unmatch VLAN Mapped: -
  Regional Root  Priority: 32769       MAC      : 00ed.f010.0001
  Internal Root Cost     : 0           Root Port: -
  Bridge ID      Priority: 32769       MAC      : 00ed.f010.0001
  Regional Bridge Status : Root
  Port Information
    0/1       Up   Status:Forwarding  Role:Designated   RootGuard
    0/2       Down Status:Disabled    Role:-            RootGuard
    0/3       Down Status:Disabled    Role:-            -
    0/4       Down Status:Disabled    Role:-            -
    0/5       Down Status:Disabled    Role:-            -
    0/6       Down Status:Disabled    Role:-            -
    0/7       Down Status:Disabled    Role:-            RootGuard
    0/8       Down Status:Disabled    Role:-            RootGuard
    0/11      Down Status:Disabled    Role:-            -
    0/12      Up   Status:Forwarding  Role:Designated   -
    ChGr:1    Up   Status:Forwarding  Role:Designated   RootGuard
MST Instance 4095
  VLAN Mapped: 4094
  Unmatch VLAN Mapped: -
  Regional Root  Priority: 36863       MAC      : 00ed.f010.0001
  Internal Root Cost     : 0           Root Port: -
  Bridge ID      Priority: 36863       MAC      : 00ed.f010.0001
  Regional Bridge Status : Root
  Port Information
    0/17      Down Status:Disabled    Role:-            -
    0/18      Down Status:Disabled    Role:-            -
    0/19      Down Status:Disabled    Role:-            -
    0/20      Up   Status:Forwarding  Role:Designated   PortFast
    0/21      Down Status:Disabled    Role:-            -
    0/22      Up   Status:Forwarding  Role:Designated   -
    ChGr:8    Down Status:Disabled    Role:-            RootGuard

>
```

Display items in Example 3

Item	Meaning	Displayed detailed information
Multiple Spanning Tree	Operating 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 assigned to MST instance 0 (IST). A hyphen (-) is displayed if no VLANs are assigned. 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.

Item	Meaning	Displayed detailed information
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	MAC address of the Switch
Regional Bridge Status	Status of the bridge for MST instance 0 (IST) of the Switch	`Root`: Root bridge `Designated`: Designated bridge
MST Instance	MST instance ID	Displays the MST instance ID and information about the instance.
VLAN Mapped	Instance mapping VLAN	Lists the VLANs assigned to the MST instance. A hyphen (`-`) is displayed if no VLANs are assigned.
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	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.
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	MAC address of the Switch

Item	Meaning	Displayed detailed information
Regional Bridge Status	Status of the bridge for 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 assigned to the MST instance, a response message is displayed because there are no ports.
<IF#>	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 the `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 the `Down` status.
Status	Port state	`Discarding`: Discarding `Learning`: Learning `Forwarding`: Indicates Forwarding status. `Disabled`: Disabled This parameter becomes `Disabled` if the port is in the `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 the `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 partner device port is 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 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 functionality for PortFast	Indicates that the port is a PortFast port, and that the BPDU guard functionality is applied. `(Received)`: Indicates that the port is down because BPDUs are received while

Item	Meaning	Displayed detailed information
		PortFast is being applied.
BPDUFilter	BPDU filter	Indicates that the BPDU filter functionality is applied.
RootGuard	Root guard	Indicates that the port applies the root guard functionality.
Compatible	Compatible mode	Indicates that the port is operating in compatible mode for an MSTP Spanning Tree Protocol. Ports operating in compatible mode do not perform rapid status transitions.

Example 4

Figure 17-4 Example of displaying detailed PVST+ Spanning Tree information

```
> show spanning-tree vlan 2,4094 port 0/10-11,0/16-17,0/20 detail

Date 2010/09/14 11:26:46 UTC
VLAN 2  PVST+ Spanning Tree:Enabled   Mode:PVST+
  Bridge ID
    Priority:32770                MAC Address:00ed.f010.0001
    Bridge Status:Designated      Path Cost Method:Short
    Max Age:20                    Hello Time:2
    Forward Delay:15
  Root Bridge ID
    Priority:32770                MAC Address:0012.e2c4.2772
    Root Cost:19
    Root Port:0/12
    Max Age:20                    Hello Time:2
    Forward Delay:15
  Port Information
  Port:0/11 Down
    Status:Disabled               Role:-
    Priority:128                  Cost:-
    Link Type:-                   Compatible Mode:-
    Loop Guard:ON(Blocking)       PortFast:OFF
    BPDUFilter:OFF                RootGuard:OFF
  Port:ChGr:1 Up
    Status:Blocking               Role:Designated
    Priority:128                  Cost:19
    Link Type:-                   Compatible Mode:-
    Loop Guard:OFF                PortFast:OFF
    BPDUFilter:OFF                RootGuard:ON(Blocking)
    BPDU Parameters(2010/09/14 11:26:45):
      Designated Root
        Priority:32770            MAC address:0012.e2c4.2772
      Designated Bridge
        Priority:32770            MAC address:0012.e2c4.2772
        Root Cost:0
      Port ID
        Priority:128              Number:66
      Message Age Timer:1(0)/20
VLAN 4094  PVST+ Spanning Tree:Enabled   Mode:PVST+
```

```
    Bridge ID
      Priority:36862                MAC Address:00ed.f010.0001
      Bridge Status:Designated      Path Cost Method:Short
      Max Age:20                    Hello Time:2
      Forward Delay:15
    Root Bridge ID
      Priority:36862                MAC Address:0012.e2c4.2772
      Root Cost:19
      Root Port:0/20
      Max Age:20                    Hello Time:2
      Forward Delay:15
    Port Information
    Port:0/17 Down
      Status:Disabled               Role:-
      Priority:128                  Cost:-
      Link Type:-                   Compatible Mode:-
      Loop Guard:ON(Blocking)       PortFast:OFF
      BPDUFilter:OFF                RootGuard:OFF
    Port:0/20 Up
      Status:Forwarding             Role:Root
      Priority:128                  Cost:19
      Link Type:-                   Compatible Mode:-
      Loop Guard:OFF                PortFast:ON(BPDU received)
      BPDUFilter:OFF                RootGuard:OFF
      BPDU Parameters(2010/09/14 11:26:47):
        Designated Root
          Priority:36862            MAC address:0012.e2c4.2772
        Designated Bridge
          Priority:36862            MAC address:0012.e2c4.2772
          Root Cost:0
        Port ID
          Priority:128              Number:20
        Message Age Timer:2(0)/20

>
```

Display items in Example 4

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:	Operating 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 on the Switch	--
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 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	Interval for sending BPDUs	Interval for sending BPDUs that are regularly sent from the Switch
Forward Delay	Time required for a state transition of the port	Time required for a state transition when the state 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 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 BPDUs sent from the root bridge	Maximum valid time of BPDUs sent from the root bridge
Hello Time	Interval for sending BPDUs sent from the root bridge	Interval for sending BPDUs that are regularly sent from the root bridge
Forward Delay	Time required for a state transition of the root bridge port	Time required for a state transition when the state 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

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 the `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 the `Down` status.
Status	Port state	If `Mode` is `PVST+`: `Blocking`: Blocking `Listening`: Listening `Learning`: Learning `Forwarding`: Indicates Forwarding status. `Disabled`: Disabled. This status is displayed when the port is in the `Down` status. `Disabled(unmatched)`: Disabled. A configuration mismatch was detected because a BPDU with an IEEE 802.1Q tag was received when the port was disabled. If `Mode` is `Rapid PVST+`: `Discarding`: Discarding `Learning`: Learning `Forwarding`: Indicates Forwarding status. `Disabled`: Disabled. This status is displayed when the port is in the `Down` status. `Disabled(unmatched)`: Disabled. A configuration mismatch was detected because a BPDU with an IEEE 802.1Q tag was received when the port was disabled.
Role	The role of the port	`Root`: Root port `Designated`: Designated port `Alternate`: Alternate port `Backup`: Backup port If the port is in the `Down` status, a hyphen (`-`) is displayed, because ports in this status are not included in the topology calculations. These parameters are commonly used by `STP` and `Rapid STP`.
Priority	Port priority	Value set for the priority of the port on the Switch If the port is in the `Down` status, a hyphen (`-`) is displayed.
Cost	Port cost	Value set for the port cost of the Switch. If the port is in the `Down` status, a hyphen (`-`) is displayed.

Item	Meaning	Displayed detailed information
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 the `Down` status.
Compatible Mode	Compatible mode	`ON`: Operation is in progress in compatible mode. A hyphen (`-`) is displayed when operation is in progress in normal mode (non-compatible mode) or when the port is in the `Down` status. Ports operating in compatible mode do not perform rapid status transitions.
Loop Guard	Loop guard functionality	`ON`: The loop guard functionality is being applied. `ON(Blocking)`: The loop guard functionality is running and the port is blocked. `OFF`: The loop guard functionality is not being used.
PortFast	The PortFast status. The receive status of BPDUs is displayed enclosed in parentheses.	`OFF`: PortFast is not operating. `ON`: PortFast is operating. `BPDU Guard`: The BPDU guard functionality is being applied to 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 functionality is being applied. `OFF`: The BPDU filter functionality is not being used.
Root Guard	Root guard functionality	`ON`: The root guard functionality is being applied. `ON(Blocking)`: The root guard functionality is running and the port is blocked. `OFF`: The root guard functionality is not being used.
BPDU Parameters	Information about received BPDUs on the 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 functionality, this item displays information about the BPDUs that caused the port to be blocked.
Designated Root	Root bridge information stored in the BPDU	--

Item	Meaning	Displayed detailed information
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address for root bridge
Designated Bridge	Information about the bridge that sent the BPDU	--
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address for root bridge
Root Cost	Root path cost	Root path cost of the bridge that sent the BPDU
Port ID	Information about the port that sent the BPDU	--
Priority	Port priority	0 to 255 The lower the value, the higher the priority.
Number	Port number	0 to 897
Message Age Timer	Valid time of the 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 17-5 Example of displaying detailed information about Single Spanning Tree

```
> show spanning-tree single detail

Date 2010/09/14 11:42:35 UTC
Single Spanning Tree:Enabled   Mode:STP
  Bridge ID
    Priority:32768                MAC Address:00ed.f010.0001
    Bridge Status:Root            Path Cost Method:Short
    Max Age:20                    Hello Time:2
    Forward Delay:15
  Root Bridge ID
    Priority:32768                MAC Address:00ed.f010.0001
    Root Cost:0
    Root Port:-
    Max Age:20                    Hello Time:2
```

```
  Forward Delay:15
Port Information
Port:0/1 Up
  Status:Forwarding              Role:Designated
  Priority:128                   Cost:19
  Link Type:-                    Compatible Mode:-
  Loop Guard:OFF                 PortFast:OFF
  BPDUFilter:OFF                 RootGuard:ON
Port:0/2 Down
  Status:Disabled                Role:-
  Priority:128                   Cost:-
  Link Type:-                    Compatible Mode:-
  Loop Guard:OFF                 PortFast:OFF
  BPDUFilter:OFF                 RootGuard:ON

            :

Port:ChGr:1 Up
  Status:Forwarding              Role:Designated
  Priority:128                   Cost:19
  Link Type:-                    Compatible Mode:-
  Loop Guard:OFF                 PortFast:OFF
  BPDUFilter:OFF                 RootGuard:ON
Port:ChGr:8 Down
  Status:Disabled                Role:-
  Priority:128                   Cost:-
  Link Type:-                    Compatible Mode:-
  Loop Guard:OFF                 PortFast:OFF
  BPDUFilter:OFF                 RootGuard:ON

>
```

Display items in Example 5

Item	Meaning	Displayed detailed information
Single Spanning Tree:	Operating status of the 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 on 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

Item	Meaning	Displayed detailed information
		value.
Max Age	Maximum valid time of BPDUs	Maximum valid time of BPDUs sent from the Switch
Hello Time	Interval for sending BPDUs	Interval for sending BPDUs that are regularly sent from the Switch
Forward Delay	Time required for a state transition of the port	Time required for a state transition when the state 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 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 BPDUs sent from the root bridge	Maximum valid time of BPDUs sent from the root bridge
Hello Time	Interval for sending BPDUs sent from the root bridge	Interval for sending BPDUs that are regularly sent from the root bridge
Forward Delay	Time required for a state transition of the root bridge port	Time required for a state transition when the state 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 the `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 the `Down` status.
Status	Port state	If `Mode` is `STP`: `Blocking`: Blocking `Listening`: Listening `Learning`: Learning `Forwarding`: Indicates Forwarding status. `Disabled`: Disabled. This status is displayed when the port is in the `Down` status. `Disabled(unavailable)`: Disabled. Single Spanning Tree cannot be used because PVST+ is enabled for the port. If `Mode` is `Rapid STP`: `Discarding`: Discarding `Learning`: Learning `Forwarding`: Indicates Forwarding status. `Disabled`: Disabled. This status is displayed when the port is in the `Down` status. `Disabled(unavailable)`: Disabled. 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 the `Down` status, a hyphen (`-`) is displayed, because ports in this status are not included in the topology calculations. These parameters are used by both `STP` and `Rapid STP`.
Priority	Port priority	Value set for the priority of the port on the Switch If the port is in the `Down` status, a hyphen (`-`) is displayed.
Cost	Port cost	Value set for the port cost of the Switch. If the port is in the `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 the `Down` status.

Item	Meaning	Displayed detailed information
Compatible Mode	Compatible mode	`ON`: Operation is in progress in compatible mode. A hyphen (`-`) is displayed when operation is in progress in normal mode (non-compatible mode) or when the port is in the `Down` status. Ports operating in compatible mode do not perform rapid status transitions.
Loop Guard	Loop guard functionality	`ON`: The loop guard functionality is being applied. `ON(Blocking)`: The loop guard functionality is running and the port is blocked. `OFF`: The loop guard functionality is not being used.
PortFast	The PortFast status. The receive status of BPDUs is displayed enclosed in parentheses.	`OFF`: PortFast is not operating. `ON`: PortFast is operating. `BPDU Guard`: The BPDU guard functionality is being applied to 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 functionality is being applied. `OFF`: The BPDU filter functionality is not being used.
Root Guard	Root guard functionality	`ON`: The root guard functionality is being applied. `ON(Blocking)`: The root guard functionality is running and the port is blocked. `OFF`: The root guard functionality is not being used.
BPDU Parameters	Information about received BPDUs on the 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 functionality, 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 root bridge

Item	Meaning	Displayed detailed information
Designated Bridge	Information about the bridge that sent the BPDU	--
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address for root bridge
Root Cost	Root path cost	Root path cost of the bridge that sent the BPDU
Port ID	Information about the port that sent the BPDU	--
Priority	Port priority	0 to 255 The lower the value, the higher the priority.
Number	Port number	0 to 897
Message Age Timer	Valid time of the received BPDUs	Indicates how long received BPDUs are valid. A hyphen (-) is displayed if this period has expired. *<current-time>*(*<time-BPDU-received>*)/*<maximum-time>* *<current-time>*: The time at which the BPDU is received plus the time that has elapsed *<time-BPDU-received>*: The time that has elapsed when the BPDU is received (Message Age of the received BPDU) *<maximum-time>*: Valid time (Max Age of the received BPDU)

Example 6

Figure 17-6 Example of displaying detailed information about Multiple Spanning Tree

```
> show spanning-tree mst detail

Date 2010/09/14 13:07:18 UTC
Multiple Spanning Tree: Enabled
Revision Level: 0      Configuration Name:
CIST Information           Time Since Topology Change: 1:15:35
  VLAN Mapped: 1,3-4093,4095
  Unmatch VLAN Mapped: -
  CIST Root      Priority: 32768       MAC           : 00ed.f010.0001
  External Root Cost     : 0           Root Port     : -
  Max Age                : 20
  Forward Delay          : 15
  Regional Root  Priority: 32768       MAC           : 00ed.f010.0001
  Internal Root Cost     : 0
  Remaining Hops         : 20
  Bridge ID      Priority: 32768       MAC           : 00ed.f010.0001
  Regional Bridge Status : Root        Path Cost Method: Long
  Max Age                : 20          Hello Time    : 2
  Forward Delay          : 15          Max Hops      : 20
```

```
  Port Information
  Port:0/1  Up
    Status    : Forwarding       Role      : Designated
    Priority  : 128              Cost      : 1
    Link Type : point-to-point   PortFast  : OFF
    BPDUFilter: OFF              Hello Time: 2
    RootGuard : ON
  Port:0/2  Down
    Status    : Disabled         Role      : -
    Priority  : 128              Cost      : -
    Link Type : -                PortFast  : OFF
    BPDUFilter: OFF              Hello Time: 2
    RootGuard : ON

              :

  Port:ChGr:8  Down
    Status    : Disabled         Role      : -
    Priority  : 128              Cost      : -
    Link Type : -                PortFast  : OFF
    BPDUFilter: OFF              Hello Time: 2
    RootGuard : ON
MST Instance 1             Time Since Topology Change: 0:3:45
  VLAN Mapped: 2
  Unmatch VLAN Mapped: -
  Regional Root  Priority: 32769       MAC           : 00ed.f010.0001
  Internal Root Cost     : 0           Root Port     : -
  Remaining Hops         : 20
  Bridge ID      Priority: 32769       MAC           : 00ed.f010.0001
  Regional Bridge Status : Root
  Max Age                : 20          Hello Time    : 2
  Forward Delay          : 15          Max Hops      : 20
  Port Information
  Port:0/1  Up
    Status    : Forwarding       Role      : Designated
    Priority  : 128              Cost      : 1
    Link Type : point-to-point   PortFast  : OFF
    BPDUFilter: OFF              Hello Time: 2
    RootGuard : ON
  Port:0/2  Down
    Status    : Disabled         Role      : -
    Priority  : 128              Cost      : -
    Link Type : -                PortFast  : OFF
    BPDUFilter: OFF              Hello Time: 2
    RootGuard : ON

              :

  Port:ChGr:1  Up
    Status    : Forwarding       Role      : Designated
    Priority  : 128              Cost      : 1
    Link Type : point-to-point   PortFast  : OFF
    BPDUFilter: OFF              Hello Time: 2
    RootGuard : ON
MST Instance 4095          Time Since Topology Change: 0:3:34
  VLAN Mapped: 4094
  Unmatch VLAN Mapped: -
  Regional Root  Priority: 36863       MAC           : 00ed.f010.0001
  Internal Root Cost     : 0           Root Port     : -
  Remaining Hops         : 20
  Bridge ID      Priority: 36863       MAC           : 00ed.f010.0001
  Regional Bridge Status : Root
  Max Age                : 20          Hello Time    : 2
```

```
Forward Delay          : 15          Max Hops      : 20
Port Information
Port:0/17  Down
  Status    : Disabled          Role      : -
  Priority  : 128               Cost      : -
  Link Type : -                 PortFast  : OFF
  BPDUFilter: OFF               Hello Time: 2
  RootGuard : OFF
Port:0/18  Down
  Status    : Disabled          Role      : -
  Priority  : 128               Cost      : -
  Link Type : -                 PortFast  : OFF
  BPDUFilter: OFF               Hello Time: 2
  RootGuard : OFF
Port:0/19  Down
  Status    : Disabled          Role      : -
  Priority  : 128               Cost      : -
  Link Type : -                 PortFast  : OFF
  BPDUFilter: OFF               Hello Time: 2
  RootGuard : OFF
Port:0/20  Up
  Status    : Forwarding        Role      : Designated
  Priority  : 128               Cost      : 4095
  Link Type : point-to-point    PortFast  : ON(BPDU not received)
  BPDUFilter: OFF               Hello Time: 2
  RootGuard : OFF

            :

>
```

Display items in Example 6

Item	Meaning	Displayed detailed information
Multiple Spanning Tree	Operating 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
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)

Item	Meaning	Displayed detailed information
VLAN Mapped	Instance mapping VLAN	Lists the VLANs assigned to MST instance 0 (IST). A hyphen (`-`) is displayed if no VLANs are assigned. 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 state transition of the CIST root bridge port	Displays the time required for a state transition when the state transition in the CIST root bridge is triggered by the timer
Regional Root	Bridge ID for the regional root bridge of MST instance 0 (IST)	Displays information about the regional root bridge of MST instance 0 (IST).
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)

Item	Meaning	Displayed detailed information
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	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	Interval for sending the BPDUs of MST instance 0 (IST) of the Switch	Displays the interval for sending BPDUs that are regularly sent from the MST instance 0 (IST) bridge of the Switch.
Forward Delay	Time required for a state transition of the MSI instance 0 (IST) port on the Switch	Displays the time required for a state transition when the state transition in the bridge of MSI 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 Displays the maximum number of hops for BPDUs sent from the MST instance 0 (IST) bridge of the Switch.
MST Instance	MST instance ID	Displays the MST instance ID and information about the instance.
Time Since Topology Change	Time since a topology change was detected	*hh*`:`*mm*`:`*ss* (when the elapsed time is less than 24 hours) *ddd*`.`*hh*`:`*mm*`:`*ss* (when the elapsed time exceeds 24 hours) `Over 1000 days` (when the elapsed time is more than 1000 days)
VLAN Mapped	Instance mapping VLAN	Lists the VLANs assigned to the MST instance. A hyphen (`-`) is displayed if no VLANs are assigned.

Item	Meaning	Displayed detailed information
Unmatch VLAN Mapped	Instance mapping VLAN in `Blocking` status	If Ring Protocol is also used, this item displays instance mapping VLANs whose Spanning Tree Protocols are blocked because of mismatches with the VLAN mapping of Ring Protocol. A hyphen (`-`) is displayed if there is no mismatch.
Regional Root	Bridge ID for the regional root bridge of the MST instance	Displays information about the regional root bridge of the MST instance.
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address for the regional root bridge of the MST instance
Internal Root Cost	Internal root path cost for the MST instance	Path cost value from the Switch to the regional root bridge of MST instance. `0` is displayed if the Switch is the regional root bridge of the MST instance.
Root Port	Root port of the MST instance	Displays the port number of the root port of the MST instance. If the root port of the MST instance is a link aggregation port, the link aggregation port list and the channel group number are displayed. 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	MAC address of the Switch
Regional Bridge Status	Status of the bridge for the MST instance of the Switch	`Root`: Root bridge `Designated`: Designated bridge
Max Age	Maximum valid time of BPDUs sent from the MST instance of the Switch	Displays the maximum valid time of BPDUs sent from the MST instance bridge of the Switch.
Hello Time	Interval for sending BPDUs sent from the MST instance of the Switch	Displays the interval for sending BPDUs that are regularly sent from the MST instance bridge of the Switch.

Item	Meaning	Displayed detailed information
Forward Delay	Time required for a state transition of the MST instance port on the Switch	Displays the time required for a state transition when the state 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 assigned to the MST instance, a response message is displayed because there are no ports.
<IF#>	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 the `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 the `Down` status.
Boundary	Boundary port	Indicates that the port is the boundary port for the region. If the role of the partner device port is 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 operating in compatible mode for an MSTP Spanning Tree Protocol. Ports operating in compatible mode do not perform rapid status transitions.
Status	Port state	`Discarding`: Discarding `Learning`: Learning `Forwarding`: Indicates Forwarding status. `Disabled`: Disabled This parameter becomes `Disabled` if the port is in the `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 the `Down` status, a hyphen (`-`) is displayed, because ports in this status are

Item	Meaning	Displayed detailed information
		not included in the topology calculations.
Priority	Port priority	Displays the value of the port priority setting for the MST instance of the Switch. If the port is in the `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 the `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 the `Down` status.
PortFast	The PortFast status. The status of receive BPDUs is displayed enclosed in parentheses.	`OFF`: PortFast is not operating. `ON`: PortFast is operating. `BPDU Guard`: The BPDU guard functionality is being applied to 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 functionality is being applied. `OFF`: The BPDU filter functionality 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 functionality	`ON`: The root guard functionality is being applied. `ON(Blocking)`: The root guard functionality is running and the port is blocked. (All MSTIs for the port are blocked.) `OFF`: The root guard functionality is not being used.

Item	Meaning	Displayed detailed information
BPDU Parameters	Information about received BPDUs on the 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(IEEE802.1D)`: Indicates that BPDUs in which the protocol version is set to STP (IEEE 802.1D) were received from neighboring devices. `Rapid STP(IEEE802.1w)`: Indicates that BPDUs in which the protocol version is set to RSTP (IEEE 802.1W) were received from neighboring devices. `MSTP(IEEE802.1s)`: 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 of the root bridge that sent BPDUs
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 of the regional root bridge that sent BPDUs

Item	Meaning	Displayed detailed information
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	Information about the neighboring bridge that sent the BPDU	--
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address of the bridge that sent BPDUs
Port ID	Information about the port that sent 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 the received BPDUs	Indicates how long received BPDUs are valid. A hyphen (`-`) is displayed if this period has expired. *<current-time>*(*<time-BPDU-received>*)/*<maximum-time>* *<current-time>*: The time at which the BPDU is received plus the time that has elapsed *<time-BPDU-received>*: The time that has already elapsed when the BPDU is received (Message Age of the received BPDU) *<maximum-time>*: Valid time (Max Age of the received BPDU)
Remaining Hops	Number of remaining hops	0 to 40 Displays the number of remaining hops for BPDUs that the MST bridge sends. A hyphen (`-`) is displayed if `Mode Version` is `STP` or `Rapid STP`.

Impact on communication

None

Response messages

Table 17-1 List of response messages for the show spanning-tree command

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

Displays statistics about Spanning Tree Protocols.

Syntax

```
show spanning-tree statistics [ {vlan [ <vlan id list> ] | single | mst [ instance <mst instance 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*.

Operation 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 Multiple Spanning Tree for the MST instance IDs specified in list format. Specifiable values for 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.

Operation 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. 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.

Operation when all parameters are omitted:

Displays statistics about Single Spanning Tree, PVST+, and Multiple Spanning Tree.

Example 1

Figure 17-7 Example of displaying PVST+ Spanning Tree statistics

```
> show spanning-tree statistics vlan 1,4094

Date 2010/09/14 11:28:22 UTC
VLAN 1
Time Since Topology Change:0 day 0 hour 15 minute 59 second
Topology Change Times: 1
 Port:0/14  Down
   TxBPDUs              :         0  RxBPDUs        :         0
   Forward Transit Times:         0  RxDiscard BPDUs:         0
   Discard BPDUs by reason
         Timeout        :         0  Invalid        :         0
         Not Support    :         0  Other          :         0
 Port:0/16  Down
   TxBPDUs              :         0  RxBPDUs        :         0
   Forward Transit Times:         0  RxDiscard BPDUs:         0
   Discard BPDUs by reason
         Timeout        :         0  Invalid        :         0
         Not Support    :         0  Other          :         0
 Port:0/23  Down
   TxBPDUs              :         0  RxBPDUs        :         0
   Forward Transit Times:         0  RxDiscard BPDUs:         0
   Discard BPDUs by reason
         Timeout        :         0  Invalid        :         0
         Not Support    :         0  Other          :         0
 Port:0/24  Up
   TxBPDUs              :         2  RxBPDUs        :       498
   Forward Transit Times:         1  RxDiscard BPDUs:         0
   Discard BPDUs by reason
         Timeout        :         0  Invalid        :         0
         Not Support    :         0  Other          :         0
 Port:0/25  Down
   TxBPDUs              :         0  RxBPDUs        :         0
   Forward Transit Times:         0  RxDiscard BPDUs:         0
   Discard BPDUs by reason
         Timeout        :         0  Invalid        :         0
         Not Support    :         0  Other          :         0
 Port:0/26  Down
   TxBPDUs              :         0  RxBPDUs        :         0
   Forward Transit Times:         0  RxDiscard BPDUs:         0
   Discard BPDUs by reason
         Timeout        :         0  Invalid        :         0
         Not Support    :         0  Other          :         0
VLAN 4094
Time Since Topology Change:0 day 0 hour 10 minute 46 second
Topology Change Times: 2
 Port:0/17  Down
   TxBPDUs              :         0  RxBPDUs        :         0
   Forward Transit Times:         0  RxDiscard BPDUs:         0
   Discard BPDUs by reason
         Timeout        :         0  Invalid        :         0
         Not Support    :         0  Other          :         0
 Port:0/18  Down
   TxBPDUs              :         0  RxBPDUs        :         0
   Forward Transit Times:         0  RxDiscard BPDUs:         0
   Discard BPDUs by reason
         Timeout        :         0  Invalid        :         0
         Not Support    :         0  Other          :         0
 Port:0/19  Down
   TxBPDUs              :         0  RxBPDUs        :         0
   Forward Transit Times:         0  RxDiscard BPDUs:         0
```

```
  Discard BPDUs by reason
        Timeout        :         0  Invalid        :         0
        Not Support    :         0  Other          :         0
 Port:0/20  Up
  TxBPDUs              :         2  RxBPDUs        :       506
  Forward Transit Times:         2  RxDiscard BPDUs:         0
  Discard BPDUs by reason
        Timeout        :         0  Invalid        :         0
        Not Support    :         0  Other          :         0
 Port:0/21  Down
  TxBPDUs              :         0  RxBPDUs        :         0
  Forward Transit Times:         0  RxDiscard BPDUs:         0
  Discard BPDUs by reason
        Timeout        :         0  Invalid        :         0
        Not Support    :         0  Other          :         0
 Port:0/22  Up
  TxBPDUs              :         1  RxBPDUs        :       504
  Forward Transit Times:         0  RxDiscard BPDUs:         0
  Discard BPDUs by reason
        Timeout        :         0  Invalid        :         0
        Not Support    :         0  Other          :         0
 ChGr:8  Down
  TxBPDUs              :         0  RxBPDUs        :         0
  Forward Transit Times:         0  RxDiscard BPDUs:         0
  Discard BPDUs by reason
        Timeout        :         0  Invalid        :         0
        Not Support    :         0  Other          :         0

>
```

Figure 17-8 Example of displaying Single Spanning Tree statistics

```
> show spanning-tree statistics single

Date 2010/09/14 11:44:38 UTC
Time Since Topology Change:0 day 0 hour 5 minute 43 second
Topology Change Times: 4
 Port:0/1  Up
  TxBPDUs              :       187  RxBPDUs        :         0
  Forward Transit Times:         1  RxDiscard BPDUs:         0
  Discard BPDUs by reason
        Timeout        :         0  Invalid        :         0
        Not Support    :         0  Other          :         0
 Port:0/2  Down
  TxBPDUs              :         0  RxBPDUs        :         0
  Forward Transit Times:         0  RxDiscard BPDUs:         0
  Discard BPDUs by reason
        Timeout        :         0  Invalid        :         0
        Not Support    :         0  Other          :         0

           :

ChGr:1  Up
  TxBPDUs              :       187  RxBPDUs        :         0
  Forward Transit Times:         1  RxDiscard BPDUs:         0
  Discard BPDUs by reason
        Timeout        :         0  Invalid        :         0
        Not Support    :         0  Other          :         0
 ChGr:8  Down
  TxBPDUs              :         0  RxBPDUs        :         0
  Forward Transit Times:         0  RxDiscard BPDUs:         0
  Discard BPDUs by reason
        Timeout        :         0  Invalid        :         0
        Not Support    :         0  Other          :         0
```

>

Display items in Example 1

Item	Meaning	Displayed detailed information
VLAN	VLAN ID subject to PVST+	Displayed only when `vlan` is specified.
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 Spanning Tree Protocol operation started.
Topology ChangeTimes	Number of detecting topology changes	--
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. If link aggregation is used, this means that the channel group is in the `Up` status. If a virtual link is used, this means that at least one virtual link port is in the `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 the `Down` status. If a virtual link is used, this means that all virtual link ports are in the `Down` status.
Forward Transit Times	Number of transitions to the forwarding state	--
TxBPDUs	Number of sent BPDUs	--
RxBPDUs	Number of received BPDUs	--
RxDiscardsBPDUs	Number of discarded received BPDUs	--
Timeout	Number of BPDUs whose valid time expired	Number of received BPDUs whose 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 included unsupported parameters

Item	Meaning	Displayed detailed information
Other	Number of BPDUs discarded for another reason	Displays the number of discarded received BPDUs when BPDU discard has been configured. ● When a BPDU filter has been set ● When the root guard functionality is operating

Example 2

Figure 17-9 Example of displaying Multiple Spanning Tree statistics

```
> show spanning-tree statistics mst instance 1,4095

Date 2010/09/14 13:09:55 UTC
MST Instance ID: 1  Topology Change Times: 7
 Port:0/1  Up
   TxBPDUs              :       203  RxBPDUs        :         0
   Forward Transit Times:         1  Discard Message:         0
   Exceeded Hop         :         0
 Port:0/2  Down
   TxBPDUs              :         0  RxBPDUs        :         0
   Forward Transit Times:         0  Discard Message:         0
   Exceeded Hop         :         0

           :

ChGr:1  Up
   TxBPDUs              :       203  RxBPDUs        :         0
   Forward Transit Times:         1  Discard Message:         0
   Exceeded Hop         :         0
MST Instance ID: 4095  Topology Change Times: 1
 Port:0/17  Down
   TxBPDUs              :         0  RxBPDUs        :         0
   Forward Transit Times:         0  Discard Message:         0
   Exceeded Hop         :         0
 Port:0/18  Down
   TxBPDUs              :         0  RxBPDUs        :         0
   Forward Transit Times:         0  Discard Message:         0
   Exceeded Hop         :         0
 Port:0/19  Down
   TxBPDUs              :         0  RxBPDUs        :         0
   Forward Transit Times:         0  Discard Message:         0
   Exceeded Hop         :         0
 Port:0/20  Up
   TxBPDUs              :         1  RxBPDUs        :         0
   Forward Transit Times:         1  Discard Message:         0
   Exceeded Hop         :         0

           :

>
```

Display items in Example 2

Item	Meaning	Displayed detailed information
MST Instance ID	Instance ID subject to MST	--
Topology ChangeTimes	Number of detecting topology changes	--
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 the Up status. If a virtual link is used, this means that at least one virtual link port is in the 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 the Down status. If a virtual link is used, this means that all virtual link ports are in the Down status.
TxBPDUs	Number of sent BPDUs	--
RxBPDUs	Number of received BPDUs	--
Forward Transit Times	Number of transitions to the forwarding state	--
RxDiscard BPDUs	Number of discarded received BPDUs	-- (Displayed only for MST instance: 0.)
Discard BPDUs by reason	Number of discarded received BPDUs	-- (Displayed only for MST instance: 0.)
Timeout	Number of BPDUs whose valid time expired	Displays the number of received BPDUs whose 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

Item	Meaning	Displayed detailed information
Not Support	Number of unsupported BPDUs	Displays the number of received BPDUs that include 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 discarded received BPDUs when PVST+ BPDUs are received or when BPDU discard has been configured. ● When a BPDU filter has been configured ● When the root guard functionality is operating (Displayed only for MST Instance ID: 0)
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 functionality: ● When the root guard functionality is set (Displayed only for MST instances 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 17-2 List of response messages for the show spanning-tree statistics command

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

clear spanning-tree statistics

Clears statistics about Spanning Tree Protocols.

Syntax

```
clear spanning-tree statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 17-10 Example of clearing the statistics for all Spanning Tree Protocols

```
> clear spanning-tree statistics

>
```

Display items

None

Impact on communication

None

Response messages

Table 17-3 List of response messages for the clear spanning-tree statistics command

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

Notes

- Even if statistics are cleared to zero, the value for the MIB information obtained by using SNMP is not cleared to zero.
- 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 <port 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*.

Operation 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. For details about how to specify *<channel group list>*, see *Specifiable values for parameters*.

Operation when all parameters are omitted:

STP compatible mode is forcibly recovered for the ports of all Spanning Tree Protocols.

Example

The following shows an example of forcing recovery of STP compatible mode for Spanning Tree Protocols.

Figure 17-11 Example of forcibly recovering STP compatible mode for Spanning Tree Protocols

```
> clear spanning-tree detected-protocol

>
```

Display items

None

Impact on communication

None

Response messages

Table 17-4 List of response messages for the clear spanning-tree detected-protocol command

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

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 numbers handled by PVST+.

single

Displays the numbers handled by Single Spanning Tree.

mst

Displays the numbers handled by Multiple Spanning Tree.

Operation when this parameter is omitted:

The numbers handled by the Spanning Tree Protocol that is set in the configuration are displayed.

Example 1

The following shows an example of displaying the numbers handled by PVST+.

Figure 17-12 Example of displaying the numbers handled by PVST+

```
> show spanning-tree port-count vlan

Date 2010/09/14 11:29:39 UTC
PVST+    VLAN Counts:    3          VLAN Port Counts:      26

>
```

Display items in Example 1

Item	Meaning	Displayed detailed information
PVST+ VLAN Counts	Number of VLANs	Number of VLANs subject to PVST+
VLAN Port Counts	Number of VLAN ports	Total number of ports configured for all VLANs subject to PVST+

Example 2

The following shows an example of displaying the numbers handled by Single Spanning Tree.

Figure 17-13 Example of displaying the numbers handled by Single Spanning Tree

```
> show spanning-tree port-count single

Date 2010/09/14 11:48:21 UTC
```

```
Single   VLAN Counts:    1          VLAN Port Counts:       6

>
```

Display items in Example 2

Item	Meaning	Displayed detailed information
Single VLAN Counts	Number of VLANs	Number of VLANs subject to Single Spanning Tree
VLAN Port Counts	Number of VLAN ports	Total number of ports configured for all VLANs subject to Single Spanning Tree

Example 3

The following shows an example of displaying the numbers handled by Multiple Spanning Tree.

Figure 17-14 Example of displaying the numbers handled by Multiple Spanning Tree

```
> show spanning-tree port-count mst

Date 2010/09/14 13:12:48 UTC
CIST     VLAN Counts: 4093          VLAN Port Counts:       6
MST    1 VLAN Counts:    1          VLAN Port Counts:      12
MST 4095 VLAN Counts:    1          VLAN Port Counts:       8

>
```

Display items in Example 3

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 17-5 List of response messages for the show spanning-tree port-count command

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

Message	Description
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 PVST+ and Single Spanning Tree VLANs does not include the number of VLANs in the `suspend` status.
- The number of VLAN ports for PVST+, Single Spanning Tree, and Multiple Spanning Tree does not include the ports of VLANs in the `suspend` status.

18. Ring Protocol

show axrp
clear axrp
clear axrp preempt-delay

show axrp

Displays 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.

Operation when all parameters are omitted:

All summary information about the Ring Protocol is displayed.

Example 1

The following shows an example of displaying summary information about the Ring Protocol.

Figure 18-1 Example of displaying summary information about the Ring Protocol

```
> show axrp

Date 2012/03/02 17:08:17 UTC
Total Ring Counts:3

Ring ID:5
 Name:
 Oper State:enable           Mode:Transit    Attribute:rift-ring-edge(2)
 Shared Edge Port:64(ChGr)

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              0/40       -/down                64(ChGr)   -/-
 2              -          -/-                   -          -/-

Ring ID:10
 Name:
 Oper State:enable           Mode:Master     Attribute:-

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              0/1        secondary/forwarding  64(ChGr)   primary/down
 2              -          -/-                   -          -/-

Ring ID:11
 Name:
 Oper State:enable           Mode:Transit    Attribute:rift-ring-edge(2)
 Shared Edge Port:64(ChGr)

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
```

```
 1              0/30       -/forwarding          64(ChGr)   -/-
 2              -          -/-                   -          -/-

>
```

Display items in Example 1

Table 18-1 Display contents of summary information about Ring Protocol

Item	Meaning	Displayed detailed information
Total Ring Counts	Number of rings	1 to 51
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 functionality for a ring ID is not operating for a reason such as an improper configuration (a hyphen (`-`) is displayed if the necessary configuration for operating the Ring Protocol functionality has not been set).
Mode	Operating 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
Shared Edge Port	Port number on the shared-link side of the terminal node in a shared-link non-monitoring ring	Physical port number (interface 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 (interface 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

Item	Meaning	Displayed detailed information
Ring Port	Ring port number	Physical port number (interface port number) or channel group number (ChGr) A hyphen (-) is displayed when this item is not set.
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 Ring Protocol functionality is enabled.
State	Ring port state	Forwarding: Forwarding Blocking: Blocking down: The port or channel group is down. (If the Ring Protocol functionality of the applicable ring ID 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 shows an example of displaying detailed Ring Protocol information.

Figure 18-2 Example of displaying detailed Ring Protocol information

```
> show axrp detail

Date 2012/03/02 17:08:24 UTC
Total Ring Counts:3

Ring ID:5
 Name:
 Oper State:enable           Mode:Transit    Attribute:rift-ring-edge(2)
 Shared Edge Port:64(ChGr)
 Control VLAN ID:5
 Health Check Interval  (msec):500
 Forwarding Shift Time (sec):10
 Last Forwarding:flush request receive

 VLAN Group ID:1
  VLAN ID:50-99
  Ring Port:0/40        Role:-            State:down
  Ring Port:64(ChGr)    Role:-            State:-

 VLAN Group ID:2
  VLAN ID:-
  Ring Port:-           Role:-            State:-
  Ring Port:-           Role:-            State:-

Ring ID:10
 Name:
 Oper State:enable           Mode:Master     Attribute:-
 Control VLAN ID:10          Ring State:fault
 Health Check Interval  (msec):200
 Health Check Hold Time (msec):500
 Flush Request Counts:3

 VLAN Group ID:1
  VLAN ID:50-99
  Ring Port:0/1         Role:secondary    State:forwarding
```

```
 Ring Port:64(ChGr)    Role:primary      State:down

VLAN Group ID:2
 VLAN ID:-
 Ring Port:-           Role:-            State:-
 Ring Port:-           Role:-            State:-

Last Transition Time:2012/03/02 17:07:45
Fault Counts    Recovery Counts    Total Flush Request Counts
32              31                 327

Multi Fault Detection State:fault
 Mode:monitoring    Backup Ring ID:11
 Control VLAN ID:999
 Multi Fault Detection Interval  (msec):2000
 Multi Fault Detection Hold Time (msec):6000

Ring ID:11
 Name:
 Oper State:enable           Mode:Transit    Attribute:rift-ring-edge(2)
 Shared Edge Port:64(ChGr)
 Control VLAN ID:11
 Health Check Interval  (msec):500
 Forwarding Shift Time (sec):10
 Last Forwarding:flush request receive

 VLAN Group ID:1
  VLAN ID:50-99
  Ring Port:0/30       Role:-            State:forwarding
  Ring Port:64(ChGr)   Role:-            State:-

 VLAN Group ID:2
  VLAN ID:-
  Ring Port:-          Role:-            State:-
  Ring Port:-          Role:-            State:-

>
```

Display items in Example 2

Table 18-2 Description of displayed items (detailed Ring Protocol information)

Item	Meaning	Displayed detailed information
Total Ring Counts	Number of rings	1 to 51
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 functionality for a ring ID is not operating for a reason such as an improper configuration (a hyphen (`-`) is displayed if the necessary configuration for operating the Ring Protocol functionality has not been set).
Mode	Operating mode	`Master`: Master node `Transit`: Transit node

Item	Meaning	Displayed detailed information
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
Shared Edge Port	Port number on the shared-link side of the terminal node in a shared-link non-monitoring ring	Physical port number (interface 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 (interface 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.)
Ring State	Status of the ring	`normal`: Normal `fault`: A fault has occurred. `preempt delay`: Path switch-backs are suppressed. `monitoring recovery`: Recovery is being monitored. Note: This item is displayed only for the master node. However, if Ring Protocol functionality is not enabled, a hyphen (`-`) is displayed.
Health Check Interval	Value of the health-check frame sending interval timer	200 to 60000 (milliseconds) 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) (This item is displayed only for the master node.)

Item	Meaning	Displayed detailed information
Preempt Delay Time	Time required to complete a switch-back operation that has been suppressed	1 to 3600 (seconds), or `infinity`. If a switch-back operation has not been suppressed, 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 switches in the neighboring ring	1 to 4094 (This item is displayed only for transit nodes.)
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`. (This item is displayed only for transit nodes.)
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. A hyphen (`-`) is displayed for another reason. (This item is displayed only for transit nodes.)
VLAN Group ID	Data transfer VLAN group ID	1 to 2
VLAN ID	Data transfer VLAN ID	1 to 4094
Ring Port	Ring port number	Physical port number (interface port number) or channel group number (ChGr) A hyphen (`-`) is displayed when this item is not set.
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 Ring Protocol functionality is enabled.
State	Ring port state	`Forwarding`: Forwarding `Blocking`: Blocking `down`: The port or channel group is down. (If the Ring Protocol functionality of the applicable ring ID is not enabled, or if the port is a shared port in a shared-link non-monitoring ring, a hyphen (`-`) is displayed.)

Item	Meaning	Displayed detailed information
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 fault 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: A fault has occurred. (This item is displayed if the multi-fault monitoring functionality 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 functionality is enabled. - is displayed when this item 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.) A hyphen (-) is displayed if this item has not been set (multi-fault-detection mode command only).
Multi Fault Detection Interval	Value of the multi-fault monitoring frame sending interval timer	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 a multi-failure 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 18-3 List of response messages for the show axrp command

Message	Description
Can't execute.	The command could not be executed. 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.	The specified ring ID has not been configured.

Notes

The counter values for statistics do not increment when the upper limit is reached.

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.

Operation when all parameters are omitted:

All Ring Protocol statistics are cleared.

Example

Figure 18-3 Example of clearing all Ring Protocol statistics

```
> clear axrp
>
```

Figure 18-4 Example of clearing all Ring Protocol statistics for a specific ring ID

```
> clear axrp 1
>
```

Display items

None

Impact on communication

None

Response messages

Table 18-4 List of response messages for the clear axrp command

Message	Description
Can't execute.	The command could not be executed. 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.	The specified ring ID has not been configured.

Notes

- Even if statistics are cleared to zero, the value for the MIB information obtained by

using SNMP is not cleared to zero.

- If the configuration is deleted or added, the target statistics are cleared to zero.

clear axrp preempt-delay

Clears the path switch-back 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 switch-back suppression status you want to clear.

The specifiable values are from 1 to 65535.

-f

Clears the path switch-back suppression status without outputting any messages.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

Figure 18-5 Example of executing the clear axrp preempt-delay command

```
> clear axrp preempt-delay 1
Fault recovery process restore OK? (y/n) :y

>
```

Figure 18-6 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 for a ring ID for which path switch-back suppression is enabled, the suppression is disabled and a path switch-back operation 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 18-5 List of response messages for the clear axrp preempt-delay command

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

Message	Description
Ring Protocol is not configured.	The Ring Protocol has not been configured. Check the configuration.
Specified Ring ID is not configured.	The specified ring ID has not been configured.
Specified Ring ID is not preempt delay state.	Path switch-back suppression is not enabled for the specified ring ID.

Notes

None

19. IGMP/MLD Snooping

show igmp-snooping
clear igmp-snooping
show mld-snooping
clear mld-snooping

show igmp-snooping

Displays IGMP snooping information. The following information is displayed for each VLAN:

- Whether the querier functionality 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>

Specify 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*.

Operation when this parameter is omitted:

Displays information about IGMP snooping for all VLANs.

{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>

Specify the multicast group IP address for which you want to display IGMP snooping information.

port *<port list>*

Displays the subscription multicast group addresses for the specified ports. For details about how to specify *<port list>* and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number *<channel group list>*

Displays the subscription multicast group addresses for the specified channel groups. For details about how to specify *<Channel group list>* and the specifiable range of values, see *Specifiable values for parameters*.

statistics

Displays statistics.

Example 1

Figure 19-1 Example of displaying IGMP snooping information

```
> show igmp-snooping

Date 2011/02/23 14:21:03 UTC
VLAN counts: 3
```

```
VLAN: 3253
  IP Address: 192.168.53.100      Querier: enable
  IGMP querying system: 192.168.53.100
  Querier version: V3
  Fast-leave: Off
  Port(4): 0/13-16
  Mrouter-port: 0/13-16
  Group counts: 3
VLAN: 3254
  IP Address: 192.168.54.100      Querier: disable
  IGMP querying system:
  Querier version: V2
  Fast-leave: Off
  Port(4): 0/17-20
  Mrouter-port: 0/17-20
  Group counts: 3
VLAN: 3255
  IP Address: 192.168.55.100      Querier: disable
  IGMP querying system:
  Querier version: V3
  Fast-leave: Off
  Port(4): 0/21-24
  Mrouter-port: 0/21-24
  Group counts: 3

>


> show igmp-snooping 3253

Date 2011/02/23 14:21:25 UTC
VLAN counts: 1
VLAN: 3253
  IP Address: 192.168.53.100      Querier: enable
  IGMP querying system: 192.168.53.100
  Querier version: V3
  Fast-leave: Off
  Port(4): 0/13-16
  Mrouter-port: 0/13-16
  Group counts: 3

>
```

Display items in Example 1

Item	Meaning	Displayed detailed information
VLAN counts	Number of VLANs on which IGMP snooping is enabled	--
VLAN	VLAN information	--
IP Address	IP addresses	Blank: No setting
Querier	Whether the querier functionality has been set	`enable`: The functionality has been set. `disable`: The functionality has not been set.
IGMP querying system	IGMP querier in the VLAN	Blank: There is no IGMP querier.

Item	Meaning	Displayed detailed information
Querier version	IGMP version of the querier	V2: Version 2 V3: Version 3
Fast-leave	Whether the IGMP Snooping instant leave functionality has been set for the VLAN	On: Not set. Off: The functionality has been set.
Port(n)	Port numbers of the ports subscribing to the VLAN	*n*: Number of applicable ports
Mrouter-port	Multicast router ports	--
Group counts	Number of multicast groups in the VLAN	--

Example 2

Figure 19-2 Example of displaying IGMP group information for each VLAN

```
> show igmp-snooping group

Date 2011/02/23 14:21:41 UTC
Total Groups: 9
VLAN counts: 3
VLAN 3253  Group counts: 3
  Group Address     MAC Address         Version      Mode
  230.0.0.11        0100.5e00.000b      V3           INCLUDE
    Port-list:0/13
  230.0.0.10        0100.5e00.000a      V2,V3        EXCLUDE
    Port-list:0/13
  230.0.0.12        0100.5e00.000c      V1,V2,V3     EXCLUDE
    Port-list:0/13
VLAN 3254  Group counts: 3
  Group Address     MAC Address         Version      Mode
  230.0.0.34        0100.5e00.0022      V1           -
    Port-list:0/17
  230.0.0.33        0100.5e00.0021      V2           -
    Port-list:0/17
  230.0.0.32        0100.5e00.0020      V3           EXCLUDE
    Port-list:0/17
VLAN 3255  Group counts: 3
  Group Address     MAC Address         Version      Mode
  230.0.0.24        0100.5e00.0018      V1,V2        -
    Port-list:0/21
  230.0.0.23        0100.5e00.0017      V1,V3        EXCLUDE
    Port-list:0/21
  230.0.0.22        0100.5e00.0016      V2,V3        EXCLUDE
    Port-list:0/21

>


> show igmp-snooping group 3253

Date 2011/02/23 14:22:27 UTC
Total Groups: 3
VLAN counts: 1
VLAN 3253  Group counts: 3
```

```
  Group Address     MAC Address         Version      Mode
  230.0.0.11        0100.5e00.000b      V3           INCLUDE
    Port-list:0/13
  230.0.0.10        0100.5e00.000a      V2,V3        EXCLUDE
    Port-list:0/13
  230.0.0.12        0100.5e00.000c      V1,V2,V3     EXCLUDE
    Port-list:0/13

>
```

Display items in Example 2

Item	Meaning	Displayed detailed information
Total Groups	Number of participating groups on the device	--
VLAN counts	Number of VLANs on which IGMP snooping is enabled	--
VLAN	VLAN information	--
Group counts	Number of subscription multicast groups in the VLAN	--
Group Address	Subscription group addresses	--
MAC Address	Learned MAC addresses	--
Version	IGMP version information	V1: IGMP version 1 V2: IGMP version 2 V3: IGMP version 3 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 A hyphen (-) is displayed if V3 is not included in the IGMP version information. 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	Forwarding port number (interface port number)	--

Example 3

Figure 19-3 Example of displaying IGMP group information for each port

```
> show igmp-snooping port 0/13
```

```
Date 2011/02/23 14:23:02 UTC
Port 0/13  VLAN counts: 1
  VLAN: 3253  Group counts: 3
    Group Address     Last Reporter      Uptime     Expires
    230.0.0.11        192.168.53.17      02:15      03:37
    230.0.0.10        192.168.53.16      02:15      03:37
    230.0.0.12        192.168.53.18      02:15      03:37

>
```

Display items in Example 3

Item	Meaning	Displayed detailed information
Port	Target port	--
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. "1day", "2days", ... are displayed if the time is 24 hours or more.
Expires	Group information aging (remaining time)	*xx*:*yy* *xx* (minutes), *yy* (seconds) "1hour", "2hours", ... are displayed if the time is 60 minutes or more. "1day", "2days", ... are displayed if the time is 24 hours or more.

Example 4

Figure 19-4 Example of displaying IGMP snooping statistics

```
> show igmp-snooping statistics

Date 2011/02/23 19:31:18 UTC
VLAN: 3253
  Port 0/13  Rx:  Query(V2)              0     Tx:  Query(V2)      3
                  Query(V3)              1          Query(V3)      4
                  Report(V1)            28
                  Report(V2)            56
                  Report(V3)            84
                  Leave                  0
```

```
                  Error                 0
Port 0/14  Rx:    Query(V2)             0     Tx:   Query(V2)      0
                  Query(V3)             0           Query(V3)      0
                  Report(V1)            0
                  Report(V2)            0
                  Report(V3)            0
                  Leave                 0
                  Error                 0
Port 0/15  Rx:    Query(V2)             0     Tx:   Query(V2)      0
                  Query(V3)             0           Query(V3)      0
                  Report(V1)            0
                  Report(V2)            0
                  Report(V3)            0
                  Leave                 0
                  Error                 0
Port 0/16  Rx:    Query(V2)             0     Tx:   Query(V2)      0
                  Query(V3)             0           Query(V3)      0
                  Report(V1)            0
                  Report(V2)            0
                  Report(V3)            0
                  Leave                 0
                  Error                 0

>
```

Display items in Example 4

Item	Meaning	Displayed detailed information
VLAN	VLAN information	--
Port	Applicable port in the VLAN	--
Rx	Number of received IGMP packets	--
Tx	Number of sent IGMP packets.	--
Query(V2)	IGMP Version 2 Query messages	--
Query(V3)	IGMP Version 3 Query messages	--
Report(V1)	IGMP Version 1 Report messages	--
Report(V2)	IGMP Version 2 Report messages	--
Report(V3)	IGMP Version 3 Report messages	--
Leave	Leave messages	--
Error	Error packets	--

Impact on communication

None

Response messages

Table 19-1 List of response messages for the show igmp-snooping command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no information. (IGMP snooping)	There is no IGMP-snooping information.

Notes

None

clear igmp-snooping

Clears all IGMP snooping information.

Syntax

```
clear igmp-snooping [-f]
```

Input mode

User mode and administrator mode

Parameters

-f

Clears statistics without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

Figure 19-5 Clearing all IGMP snooping information

```
> clear igmp-snooping
Do you wish to clear IGMP or MLD snooping data? (y/n): y

>
```

If `y` is entered, IGMP snooping information are cleared.

If `n` is entered, IGMP snooping information are not cleared.

Display items

None

Impact on communication

Note that when the `clear igmp-snooping` command is executed, multicast communication temporarily stops.

Response messages

Table 19-2 List of response messages for the clear igmp-snooping command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no information. (IGMP snooping)	There is no IGMP-snooping information.

Notes

None

show mld-snooping

Displays MLD snooping information. The following information is displayed for each VLAN:

- Whether the querier functionality is set, the MLD querier address, and the 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>

Displays information about MLD snooping for the VLAN IDs specified in list format.

For details about how to specify *<vlan id list>*, see *Specifiable values for parameters.*

Operation when this parameter is omitted:

Displays information about MLD snooping for all VLANs.

{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>

Displays information about MLD snooping for the specified multicast group address.

port *<port list>*

Displays the subscription multicast group addresses for the specified ports. For details about how to specify *<port list>* and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number *<channel group list>*

Displays the subscription multicast group addresses for the specified channel groups. For details about how to specify *<channel group list>* and the specifiable range of values, see *Specifiable values for parameters*.

statistics

Displays statistics.

Example 1

Figure 19-6 Example of displaying MLD snooping information

```
> show mld-snooping

Date 2012/12/06 02:01:53 UTC
VLAN counts: 3
VLAN: 100
```

```
  IP Address: fe80::1  Querier: enable
  MLD querying system: fe80::1
  Querier version: V1
  Port(1): 0/20
  Mrouter-port:
  Group counts: 2
VLAN: 200
  IP Address: fe80::2  Querier: enable
  MLD querying system: fe80::2
  Querier version: V1
  Port(1): 0/21
  Mrouter-port:
  Group counts: 3
VLAN: 300
  IP Address: fe80::3  Querier: disable
  MLD querying system: fe80::10
  Querier version: V2
  Port(2): 0/11,0/22
  Mrouter-port: 0/11
  Group counts: 3

>


> show mld-snooping 300

Date 2012/12/06 02:02:08 UTC
VLAN counts: 1
VLAN: 300
  IP Address: fe80::3  Querier: disable
  MLD querying system: fe80::10
  Querier version: V2
  Port(2): 0/11,0/22
  Mrouter-port: 0/11
  Group counts: 3

>
```

Display items in Example 1

Item	Meaning	Displayed detailed information
VLAN counts	Number of VLANs on which MLD snooping is enabled	--
VLAN	VLAN information	--
IP Address	IP addresses	Blank: No setting
Querier	Whether the querier functionality has been set	`enable`: The functionality has been set. `disable`: The functionality 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

Item	Meaning	Displayed detailed information
Port(n)	Port numbers of the ports subscribing to the VLAN	*n*: Number of applicable ports
Mrouter-port	Multicast router ports	--
Group counts	Number of subscription multicast groups in the VLAN	--

Example 2

Figure 19-7 Example of displaying MLD group information for each VLAN

```
> show mld-snooping group

Date 2012/12/06 02:02:29 UTC
Total Groups: 8
VLAN counts: 3
VLAN 100  Group counts: 2
  Group Address                          MAC Address      Version   Mode
  ff03::10                               3333.0000.0010   V1        -
    Port-list: 0/20
  ff03::11                               3333.0000.0011   V1        -
    Port-list: 0/20
VLAN 200  Group counts: 3
  Group Address                          MAC Address      Version   Mode
  ff03::22                               3333.0000.0022   V1        -
    Port-list: 0/21
  ff03::21                               3333.0000.0021   V1        -
    Port-list: 0/21
  ff03::20                               3333.0000.0020   V1        -
    Port-list: 0/21
VLAN 300  Group counts: 3
  Group Address                          MAC Address      Version   Mode
  ff03::3                                3333.0000.0003   V2        INCLUDE
    Port-list: 0/22
  ff03::2                                3333.0000.0002   V2        INCLUDE
    Port-list: 0/22
  ff03::1                                3333.0000.0001   V2        INCLUDE
    Port-list: 0/22

>


> show mld-snooping group 300

Date 2012/12/06 02:02:41 UTC
Total Groups: 3
VLAN counts: 1
VLAN 300  Group counts: 3
  Group Address                          MAC Address      Version   Mode
  ff03::3                                3333.0000.0003   V2        INCLUDE
    Port-list: 0/22
  ff03::2                                3333.0000.0002   V2        INCLUDE
    Port-list: 0/22
  ff03::1                                3333.0000.0001   V2        INCLUDE
    Port-list: 0/22

>
```

Display items in Example 2

Item	Meaning	Displayed detailed information
Total Groups	Number of participating groups on the device	--
VLAN counts	Number of VLANs on which MLD snooping is enabled	--
VLAN	VLAN information	--
Group counts	Number of subscription multicast groups in the VLAN	--
Group Address	Subscription group addresses	--
MAC Address	Learned MAC addresses	--
Version	MLD version information	`V1`: MLD version 1 `V2`: MLD version 2 `V1, V2`: MLD version 1 and version 2 mixed
Mode	Group mode	`INCLUDE`: INCLUDE mode `EXCLUDE`: EXCLUDE mode (A hyphen (`-`) is displayed if the MLD version information is `V1`.)
Port-list	Forwarding port number (interface port number)	--

Example 3

Figure 19-8 Example of displaying MLD group information for each port

```
> show mld-snooping port 0/22

Date 2012/12/06 02:06:58 UTC
Port 0/22  VLAN counts: 1
  VLAN 300  Group counts: 3
    Group Address              Last Reporter              Uptime    Expires
    ff03::3                    fe80::10                   08:24     04:20
    ff03::2                    fe80::10                   08:24     04:20
    ff03::1                    fe80::10                   08:24     04:20

>
```

Display items in Example 3

Item	Meaning	Displayed detailed information
Port	Target port	--
VLAN counts	Number of VLANs to which the specified port belongs	--

Item	Meaning	Displayed detailed information
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. "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 19-9 Example of displaying MLD snooping statistics

```
> show mld-snooping statistics

Date 2012/12/06 02:07:22 UTC
VLAN 100
  Port 0/20  Rx:  Query(V1)           0    Tx:  Query(V1)          4
                  Query(V2)           0         Query(V2)          0
                  Report(V1)       1057
                  Report(V2)          0
                  Done                0
                  Error               0
VLAN 200
  Port 0/21  Rx:  Query(V1)           0    Tx:  Query(V1)          4
                  Query(V2)           0         Query(V2)          0
                  Report(V1)       1584
                  Report(V2)          0
                  Done                0
                  Error               0
VLAN 300
  Port 0/11  Rx:  Query(V1)           0    Tx:  Query(V1)          0
                  Query(V2)         124         Query(V2)          0
                  Report(V1)          0
                  Report(V2)          0
                  Done                0
                  Error               0
  Port 0/22  Rx:  Query(V1)           0    Tx:  Query(V1)          0
                  Query(V2)           0         Query(V2)          0
                  Report(V1)          0
                  Report(V2)       1584
                  Done                0
                  Error               0

>
```

Display items in Example 4

Item	Meaning	Displayed detailed information
VLAN	VLAN information	--
Port	Applicable port in the VLAN	--
Rx	Number of received MLD packets	--
Tx	Number of sent MLD packets.	--
Query(V1)	MLD Version 1 Query messages	--
Query(V2)	MLD Version 2 Query messages	--
Report(V1)	MLD Version 1 Report messages	--
Report(V2)	MLD Version 2 Report messages	--
Done	Done messages	--
Error	Error packets	--

Impact on communication

None

Response messages

Table 19-3 List of response messages for the show mld-snooping command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no information. (MLD snooping)	There is no MLD snooping information.

Notes

None

clear mld-snooping

Clears all MLD snooping information.

Syntax

```
clear mld-snooping [-f]
```

Input mode

User mode and administrator mode

Parameters

-f

Clears statistics without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

Figure 19-10 Clearing all MLD snooping information

```
> clear mld-snooping
Do you wish to clear IGMP or MLD snooping data? (y/n): y

>
```

If `y` is entered, MLD snooping information are cleared.

If `n` is entered, MLD snooping information are not cleared.

Display items

None

Impact on communication

Note that when the `clear mld-snooping` command is executed, multicast communication temporarily stops.

Response messages

Table 19-4 List of response messages for the clear mld-snooping command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no information. (MLD snooping)	There is no MLD snooping information.

Notes

None

20. IPv4, ARP, and ICMP

show ip-dual interface
show ip interface
show ip arp
clear arp-cache
show ip route
ping
traceroute

show ip-dual interface

Displays the status of IPv4 and IPv6 interfaces.

Syntax

```
show ip-dual interface
show ip-dual interface summary
show ip-dual interface up
show ip-dual interface down
show ip-dual interface vlan <vlan id>
```

Input mode

User mode and administrator mode

Parameters

summary

Displays a summary of the status of all interfaces.

up

Displays detailed information about interfaces in the `Up` status.

down

Displays detailed information about interfaces in the `Down` status.

vlan <*vlan id*>

Displays detailed information about the applicable interface.

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

Operation when all parameters are omitted:

Displays the detailed status of all interfaces.

Example 1

This example shows how to display a summary of the status of all interfaces.

```
>show ip-dual interface summary
```
Press the **Enter** key.

Figure 20-1 Example of displaying a summary of all interfaces

```
> show ip-dual interface summary

Date 2012/03/03 14:49:28 UTC
VLAN0004: Up  2001:254::249/64
              fe80::2eb:f0ff:fe02:1%VLAN0004/64
VLAN0010: Up  192.168.253.44/24
              2001::1:10/64
              fe80::2eb:f0ff:fe02:1%VLAN0010/64

>
```

Display items in Example 1

Table 20-1 Information displayed for a summary of all interfaces

Item	Meaning	Displayed detailed information
VLANxxxx	Interface name	--

Item	Meaning	Displayed detailed information
Up/Down	Status of the interface	--
Dot notation	IPv4 address/subnet mask length	If the secondary IP address is set, it is displayed followed by the primary IP address.
Colon notation	IPv6 address/prefix length	`duplicated`: The address is duplicated. `tentative`: The address is being checked for duplication. `autonomous`: Automatically generated triggered by reception of RA.

Example 2

- Display detailed information about interfaces in the `Up` status.

  `>show ip-dual interface up` Press the **Enter** key.

- Display the detailed status of an interface.

  `> show ip-dual interface vlan 10` Press the **Enter** key.

The following shows an example of executing the command with an interface specified.

Figure 20-2 Example of executing the command with an interface specified

```
> show ip-dual interface vlan 10

Date 2012/03/03 14:50:20 UTC
VLAN0010: Up
  mtu 1500
  inet 192.168.253.44/24 broadcast 192.168.253.255
  inet6 2001::1:10/64
  inet6 fe80::2eb:f0ff:fe02:1%VLAN0010/64
  Port 0/1 : Up media 1000BASE-T full(auto) 00eb.f002.0001
  Port 0/2 : Up media 1000BASE-T full(auto) 00eb.f002.0001 ChGr:5 (Up)
  Port 0/4 : Down media - 00eb.f002.0001 ChGr:5 (Up)
  Time-since-last-status-change: 00:17:11
  Last down at: 2012/03/03 14:32:52
  VLAN: 10

>
```

Display items in Example 2

Table 20-2 Contents of the displayed detailed information

Item	Meaning	Displayed detailed information
VLANxxxx	Interface name	--
Up/Down	Status of the interface	--
mtu	MTU for the interface	--
inet	IPv4 address/subnet mask length	If the secondary IP address is set, it is displayed followed by the primary IP address.

Item	Meaning	Displayed detailed information
broadcast	Broadcast address	--
inet6	IPv6 address/prefix length	`duplicated`: The address is duplicated. `tentative`: The address is being checked for duplication. `autonomous`: Automatically generated triggered by reception of RA.
Port	Port number that belongs to the applicable VLAN	--
Up/Down	Port status	`Up`: In operation (Normal operating state) `Down`: In operation (line has failed), or not in operation
media	Line type	For details about the line type, see the display item *<line type>* in `show interfaces` command.
xxxx.xxxx.xxxx	MAC address	The MAC address used by packets sent from the interface.
ChGr	Channel group number and channel status	Displayed for a link aggregation line. `Up`: Indicates that the channel status is Up. `Down`: Indicates that the channel status is Down.
Time-since-last-status-change	Time elapsed since the status changed to `Up` or `Down`.	Time elapsed since the status of the VLAN interface last changed. The display format is *hour*`:`*minute*`:`*second* or *number-of-days*, *hour*`:`*minute*`:`*second*. `Over 100 days` is displayed if the number of days exceeds 100. `-----` is displayed if there has never been an `Up`/`Down` status change. This is not cleared by adding, deleting, or changing IP addresses.
Last down at	Status of the interface	Time the VLAN interface last went down. The display format is *year/month/day hour*`:`*minute*`:`*second*. `-----` is displayed if the interface has never gone down. This is not cleared by adding, deleting, or changing IP addresses.
VLAN	VLAN ID	1 to 4094

Impact on communication

None

Response messages

Table 20-3 List of response messages for the show ip-dual interface command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no information. (ip-dual interface)	There is no ip-dual interface information.

Notes

None

show ip interface

Displays the status of IPv4 interfaces.

Syntax

```
show ip interface
show ip interface summary
show ip interface up
show ip interface down
show ip interface vlan <vlan id>
```

Input mode

User mode and administrator mode

Parameters

summary
: Displays a summary of the status of all interfaces.

up
: Displays detailed information about interfaces in the `Up` status.

down
: Displays detailed information about interfaces in the `Down` status.

vlan *<vlan id>*
: Displays detailed information about the applicable interface.

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

Operation when all parameters are omitted:
: Displays the detailed status of all interfaces.

Example 1

This example shows how to display a summary of the status of all interfaces.

`> show ip interface summary` Press the **Enter** key.

Figure 20-3 Example of displaying a summary of all interfaces

```
> show ip interface summary

Date 2012/03/03 13:49:51 UTC
VLAN0001: Up  192.168.0.100/24
              192.168.1.100/24
              192.168.2.100/24
VLAN0010: Down  192.168.10.100/24
VLAN3005: Up  192.168.5.10/24
              192.168.6.10/24
VLAN3253: Down  192.168.53.100/24
VLAN3254: Up  192.168.54.100/24
VLAN3255: Up  192.168.55.100/24
VLAN3256: Down  192.168.56.100/24
VLAN4094: Up  192.168.4.10/24

>
```

Display items in Example 1

Table 20-4 Information displayed for a summary of all interfaces

Item	Meaning	Displayed detailed information
VLANxxxx	Interface name	--
Up/Down	Status of the interface	--
Dot notation	IPv4 address/subnet mask length	If the secondary IP address is set, it is displayed followed by the primary IP address.

Example 2

- Display detailed information about interfaces in the `Up` status.

  `> show ip interface up` Press the **Enter** key.

- Display the detailed status of an interface.

  `> show ip interface vlan 3005` Press the **Enter** key.

The following shows an example of executing the command with an interface specified.

Figure 20-4 Example of executing the command with an interface specified

```
> show ip interface vlan 3005

Date 2012/03/03 13:51:09 UTC
VLAN3005: Up
  mtu 1500
  inet 192.168.5.10/24 broadcast 192.168.5.255
  inet 192.168.6.10/24 broadcast 192.168.6.255
  Port 0/4 : Down media - 00eb.f002.0001
  Port 0/5 : Up media 1000BASE-T full(auto) 00eb.f002.0001 ChGr:7 (Up)
  Port 0/7 : Down media - 00eb.f002.0001 ChGr:7 (Up)
  Time-since-last-status-change: 00:05:34
  Last down at: 2012/03/03 13:45:29
  VLAN: 3005

>
```

Display items in Example 2

Table 20-5 Contents of the displayed detailed information

Item	Meaning	Displayed detailed information
VLANxxxx	Interface name	--
Up/Down	Status of the interface	--
mtu	MTU for the interface	--
inet	IPv4 address/subnet mask length	If the secondary IP address is set, it is displayed followed by the primary IP address.
broadcast	Broadcast address	--

Item	Meaning	Displayed detailed information
Port	Port number that belongs to the applicable VLAN	--
Up/Down	Port status	`Up`: In operation (Normal operating state) `Down`: In operation (line has failed), or not in operation
media	Line type	For details about the line type, see the display item *<line type>* in `show interfaces` command.
xxxx.xxxx.xxxx	MAC address	The MAC address used by packets sent from the interface.
ChGr	Channel group number and channel status	Displayed for a link aggregation line. `Up`: Indicates that the channel status is Up. `Down`: Indicates that the channel status is Down.
Time-since-last-status-change	Time elapsed since the status changed to `Up` or `Down`.	Time elapsed since the status of the VLAN interface last changed. The display format is *hour*`:`*minute*`:`*second* or *number-of-days*, *hour*`:`*minute*`:`*second*. `Over 100 days` is displayed if the number of days exceeds 100. `-----` is displayed if there has never been an `Up`/`Down` status change. This is not cleared by adding, deleting, or changing IP addresses.
Last down at	Status of the interface	Time the VLAN interface last went down. The display format is *year/month/day hour*`:`*minute*`:`*second*. `-----` is displayed if the interface has never gone down. This is not cleared by adding, deleting, or changing IP addresses.
VLAN	VLAN ID	1 to 4094

Example 3

The following shows an example of the detailed information displayed for the IP address status.

Figure 20-5 Detailed information displayed for IP addresses

```
> show ip interface

Date 2012/03/03 13:52:05 UTC
VLAN0001: Up
  mtu 1500
  inet 192.168.0.100/24 broadcast 192.168.0.255
  inet 192.168.1.100/24 broadcast 192.168.1.255
  inet 192.168.2.100/24 broadcast 192.168.2.255
  Port 0/1 : Up media 1000BASE-T full(auto) 00eb.f002.0001
  Port 0/3 : Down media - 00eb.f002.0001
  Port 0/6 : Down media - 00eb.f002.0001
  Port 0/8 : Down media - 00eb.f002.0001
  Port 0/9 : Down media - 00eb.f002.0001
  Port 0/10: Down media - 00eb.f002.0001
```

```
  Port 0/11: Down media - 00eb.f002.0001
  Port 0/25: Down media - 00eb.f002.0001
  Port 0/26: Down media - 00eb.f002.0001
  Time-since-last-status-change: 00:07:35
  Last down at: 2012/03/03 13:44:29
  VLAN: 1
VLAN0010: Down
  mtu 0
  inet 192.168.10.100/24 broadcast 192.168.10.255
  Time-since-last-status-change: 00:06:41
  Last down at: 2012/03/03 13:45:24
  VLAN: 10
VLAN3005: Up
  mtu 1500
  inet 192.168.5.10/24 broadcast 192.168.5.255
  inet 192.168.6.10/24 broadcast 192.168.6.255
  Port 0/4 : Down media - 00eb.f002.0001
  Port 0/5 : Up media 1000BASE-T full(auto) 00eb.f002.0001 ChGr:7 (Up)
  Port 0/7 : Down media - 00eb.f002.0001 ChGr:7 (Up)
  Time-since-last-status-change: 00:06:30
  Last down at: 2012/03/03 13:45:29
  VLAN: 3005

                        :

>
```

Display items in Example 3

The explanation is the same as in *Display items 2*. For details, see *Table 20-5 Contents of the displayed detailed information*.

Impact on communication

None

Response messages

Table 20-6 List of response messages for the show ip interface command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no information. (ip interface)	There is no ip interface information.

Notes

None

show ip arp

Displays ARP information.

Syntax

```
show ip arp
show ip arp interface vlan <vlan id>
show ip arp <ip address>
```

Input mode

User mode and administrator mode

Parameters

interface vlan *<vlan id>*

Specifies a VLAN ID.

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

<ip address>

Specifies an IP address.

Operation when all parameters are omitted:

Displays the ARP information registered on all interfaces.

Example

Figure 20-6 Execution result when a VLAN interface is specified

```
> show ip arp interface vlan 4094

Date 2012/03/03 12:19:01 UTC
Total: 6
IP Address      Linklayer Address  Interface  Expire     Type
192.168.254.53  0090.cc42.2dc4     VLAN4094   13min      arpa
192.168.254.77  000f.fefa.f721     VLAN4094   3min       arpa
192.168.254.98  001b.7888.1ffd     VLAN4094   19min      arpa
192.168.254.99  1cc1.de64.f234     VLAN4094   12min      arpa
192.168.254.102 00ce.a4bd.aad8     VLAN4094   Static     arpa
192.168.254.250 0000.8768.b663     VLAN4094   19min      arpa

>
```

Figure 20-7 Execution result when all ARP information is displayed

```
> show ip arp

Date 2012/03/03 12:16:02 UTC
Total: 9
IP Address      Linklayer Address  Interface  Expire     Type
10.0.0.6        00eb.f002.0001     VLAN2000   19min      arpa
10.10.10.3      (incomplete)       VLAN3333   --         arpa
192.168.254.53  0090.cc42.2dc4     VLAN4094   16min      arpa
192.168.254.77  000f.fefa.f721     VLAN4094   6min       arpa
192.168.254.98  001b.7888.1ffd     VLAN4094   19min      arpa
192.168.254.99  1cc1.de64.f234     VLAN4094   15min      arpa
192.168.254.102 00ce.a4bd.aad8     VLAN4094   Static     arpa
192.168.254.250 0000.8768.b663     VLAN4094   17min      arpa
192.168.254.252 0012.e282.680d     VLAN4094   2min       arpa

>
```

Figure 20-8 Execution result when an IP address is specified

```
> show ip arp 10.0.0.6

Date 2012/03/03 12:20:20 UTC
Total: 1
IP Address      Linklayer Address  Interface  Expire     Type
10.0.0.6        00eb.f002.0001     VLAN2000   19min      arpa

>
```

Display items

Table 20-7 Contents of the displayed ARP information

Item	Meaning	Displayed detailed information
Total	Number of ARP entries	Number of used ARP table entries
IP Address	Next Hop IP address	--
Linklayer Address	Next Hop MAC address	`(incomplete)`: The address has not been resolved by ARP.
Interface	Interface name	`VLAN`*xxxx* is displayed. *xxxx*: VLAN ID
Expire	The remaining aging time is displayed in minutes.	`Static`: Created in a configuration `--`: The address has not been resolved by ARP.
Type	Category	`arpa`: Fixed (always the Ethernet interface)

Impact on communication

None

Response messages

Table 20-8 List of response messages for the show ip arp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no information. (ip arp)	There is no ARP information.

Notes

The entries that are created after learning from other devices are not displayed in the following cases:

- There has been no communication since the interface started up.
- The aging time since registration in the ARP cache table has been exceeded.

clear arp-cache

Clears the ARP information registered dynamically.

Syntax

```
clear arp-cache
clear arp-cache interface vlan <vlan id>
```

Input mode

User mode and administrator mode

Parameters

interface vlan <*vlan id*>

Specifies a VLAN ID.

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

Operation when this parameter is omitted:

Clears the ARP information for all interfaces registered dynamically.

Example

- Clearing the ARP information (when deleting the ARP information for a specific VLAN interface)

  The following shows an example of clearing the ARP information registered dynamically on a specific VLAN interface.

Figure 20-9 Execution result of clearing the ARP information (deleting the ARP information for a specific VLAN interface)

```
> show ip arp interface vlan 4094

Date 2012/03/07 10:42:38 UTC
Total: 6
IP Address      Linklayer Address  Interface  Expire     Type
192.168.254.44  00aa.34cc.78d9     VLAN4094   Static     arpa
192.168.254.53  0090.cc42.2dc4     VLAN4094   1min       arpa
192.168.254.98  001b.7888.1ffd     VLAN4094   19min      arpa
192.168.254.99  1cc1.de64.f234     VLAN4094   16min      arpa
192.168.254.102 00ce.a4bd.aad8     VLAN4094   Static     arpa
192.168.254.236 0024.a78b.b349     VLAN4094   Static     arpa

> clear arp-cache interface vlan 4094

> show ip arp interface vlan 4094

Date 2012/03/07 10:43:59 UTC
Total: 3
IP Address      Linklayer Address  Interface  Expire     Type
192.168.254.44  00aa.34cc.78d9     VLAN4094   Static     arpa
192.168.254.102 00ce.a4bd.aad8     VLAN4094   Static     arpa
192.168.254.236 0024.a78b.b349     VLAN4094   Static     arpa

>
```

- Clearing the ARP information (when deleting all the ARP information)

  The following shows an example of clearing all ARP information registered dynamically on the Switch.

Figure 20-10 Execution result of clearing the ARP information (deleting all the ARP information)

```
> show ip arp interface vlan 4094

Date 2012/03/07 10:45:39 UTC
Total: 6
IP Address      Linklayer Address  Interface  Expire     Type
192.168.254.44  00aa.34cc.78d9     VLAN4094   Static     arpa
192.168.254.53  0090.cc42.2dc4     VLAN4094   19min      arpa
192.168.254.98  001b.7888.1ffd     VLAN4094   19min      arpa
192.168.254.99  1cc1.de64.f234     VLAN4094   20min      arpa
192.168.254.102 00ce.a4bd.aad8     VLAN4094   Static     arpa
192.168.254.236 0024.a78b.b349     VLAN4094   Static     arpa

> clear arp-cache

> show ip arp interface vlan 4094

Date 2012/03/07 10:46:58 UTC
Total: 3
IP Address      Linklayer Address  Interface  Expire     Type
192.168.254.44  00aa.34cc.78d9     VLAN4094   Static     arpa
192.168.254.102 00ce.a4bd.aad8     VLAN4094   Static     arpa
192.168.254.236 0024.a78b.b349     VLAN4094   Static     arpa

>
```

Display items

None

Impact on communication

None

Response messages

Table 20-9 List of response messages for the clear arp-cache command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
No such interface.	The specified interface does not exist. Make sure the specified parameter is correct, and then try again.

Notes

None

show ip route

Displays the IPv4 routing table.

Syntax

```
show ip route
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 20-11 Execution result of displaying IP routing information

```
> show ip route

Date 2010/09/14 17:32:39 UTC
Total: 5
Destination         Nexthop           Interface    Protocol
192.168.0.0/24      192.168.0.100     VLAN0001     Connected
192.168.4.0/24      192.168.4.10      VLAN4094     Connected
192.168.5.0/24      192.168.5.10      VLAN3005     Connected
192.168.54.0/24     192.168.54.100    VLAN3254     Connected
192.168.55.0/24     192.168.55.100    VLAN3255     Connected

>
```

Display items

Table 20-10 Contents of the displayed IP routing information

Item	Meaning	Displayed detailed information
Total	Number of registered routes	--
Destination	Destination network (IP address/mask)	--
Next Hop	Next Hop IP address	--
Interface	Interface name	`VLAN`*xxxx* is displayed. *xxxx*: VLAN ID
Protocol	Protocol	`Static`: Interface with static entries, `Connected`: Directly connected interface

Impact on communication

None

Response messages

Table 20-11 List of response messages for the show ip route command

Message	Description
There is no information. (ip route)	There is no IP routing information.

Notes

None

ping

The `ping` command is used to determine whether communication is possible to the device with the specified IP address. This command is used with IPv4 only.

Syntax

```
ping <host> [count <count>] [interval <wait>] [packetsize <size>]
```

Input mode

User mode and administrator mode

Parameters

<host>

Specifies the host name or unicast IP address for the destination host.

count *<count>*

Sends packets for the number of times specified for *<count>*, and then finishes the processing. To interrupt the processing, press **Ctrl** + **C**. The specifiable values are from 1 to 99999.

Operation when this parameter is omitted:

Sends packets indefinitely.

interval *<wait>*

Sets the packet sending interval to the number of seconds specified for *<wait>*. The specifiable values are from 1 to 60.

Operation when this parameter is omitted:

The sending interval defaults to 1 second.

packetsize *<size>*

Specifies how many bytes of data are to be sent. The specifiable values are from 18 to 1472.

Operation when this parameter is omitted:

The number of bytes of data to be sent is 56. By adding 8 bytes of ICMP header data, a total of 64 bytes will be sent.

Operation when all parameters are omitted:

The same as described in *Operation when this parameter is omitted* for each parameter.

Example

- Execute an echo test by specifying the default values (unlimited attempts, sending interval of 1 second, and data size of 56 bytes).

  `> ping 192.168.100.2` Press the **Enter** key.

  ```
  PING 192.168.100.2 (192.168.100.2): 56 data bytes
  64 bytes from 192.168.100.2: icmp_seq=0 ttl=128 time=17 ms
  64 bytes from 192.168.100.2: icmp_seq=1 ttl=128 time=0 ms
  64 bytes from 192.168.100.2: icmp_seq=2 ttl=128 time=0 ms
  64 bytes from 192.168.100.2: icmp_seq=3 ttl=128 time=0 ms
  64 bytes from 192.168.100.2: icmp_seq=4 ttl=128 time=0 ms
  64 bytes from 192.168.100.2: icmp_seq=5 ttl=128 time=0 ms
  ```

```
64 bytes from 192.168.100.2: icmp_seq=6 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=7 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=8 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=9 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=10 ttl=128 time=0 ms
^C                                          <---- To interrupt the processing, press Ctrl+C.
----192.168.100.2 PING Statistics----
11 packets transmitted, 11 packets received, 0.0% packet loss
round-trip min/avg/max = 0/2/17 ms
>
```

- Execute an echo test by specifying the following conditions: 3 attempts, sending interval of 2 seconds, and data size of 120 bytes.

  `> ping 192.168.100.2 count 3 interval 2 packetsize 120` Press the **Enter** key.

Display items

None

Impact on communication

None

Response messages

Table 20-12 List of response messages for the ping command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Unknown host.	An address corresponding to the host name was not found. The host name is not correct. Specify the correct host name.

Notes

- To halt execution of the `ping` command, press **Ctrl** + **C**.
- The precision of the response time is one sixtieth of a second. If the response time is less than a second, the time might be displayed as 0 milliseconds.

traceroute

Displays the route (route of the passed gateways and response time between the gateways) over which ICMP messages are sent to the destination host. This command is used with IPv4 only.

Syntax

```
traceroute <host> [ttl <ttl>] [waittime <time>]
```

Input mode

User mode and administrator mode

Parameters

<host>

Specifies the host name or unicast IP address for the destination host.

ttl *<ttl>*

Specify the maximum `time-to-live` (the maximum number of hops) for the probe packets to be sent. The specifiable values are from 1 to 255.

Operation when this parameter is omitted:

The maximum number of hops is 30.

waittime *<time>*

Specify the time (in seconds) to wait for a probe packet. The specifiable values are from 1 to 60.

Operation when this parameter is omitted:

The wait time for a response is 5 seconds.

Operation when all parameters are omitted:

The same as described in *Operation when this parameter is omitted* for each parameter.

Example

Figure 20-12 Normal end

```
> traceroute 192.168.30.1 waittime 1 ttl 2
traceroute to 192.168.30.1 (192.168.30.1), 2 hops max, 8 byte packets
 1  192.168.30.1 (192.168.30.1)  0 ms  0 ms  0 ms
>
```

Figure 20-13 Destination in the same subnet

```
> traceroute 192.168.30.100 waittime 3 ttl 5
traceroute to 192.168.30.100 (192.168.30.100), 5 hops max, 8 byte packets
 1  *  192.168.30.2 (192.168.30.2)  467 ms !H  *
 2  *  *  192.168.30.2 (192.168.30.2)  1750 ms !H
 3  *  *  *
 4  192.168.30.2 (192.168.30.2)  1750 ms !H  *  *
 5  *  192.168.30.2 (192.168.30.2)  1750 ms !H  *
>
```

(`!H` is displayed if Host Unreachable is received or ARP resolution fails.)

Figure 20-14 Destination in another subnet

```
> traceroute 192.168.50.1 waittime 7 ttl 5
traceroute to 192.168.50.1 (192.168.50.1), 5 hops max, 8 byte packets
 1  *  192.168.30.1 (192.168.30.1)  3967 ms !H  *
 2  192.168.30.1 (192.168.30.1)  3817 ms !H  *  3817 ms !H
```

```
>
```
(A majority of probes stop if the state changes to Host Unreachable.)

Display items

None

Impact on communication

None

Response messages

Table 20-13 List of response messages for the traceroute command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Unknown host.	An address corresponding to the host name was not found. The host name is not correct. Specify the correct host name.

Notes

- ICMP packets are sent when the `traceroute` operation command was executed on the Switch.

  The `traceroute` packets might not reach to the destination, if there is a device that does not forward ICPM exists in the route.

21. IPv6, NDP, and ICMPv6

show ip-dual interface
show ipv6 interface
show ipv6 neighbors
clear ipv6 neighbors
show ipv6 router-advertisement
ping ipv6
traceroute ipv6

show ip-dual interface

Displays the status of IPv4 and IPv6 interfaces.

Syntax

```
show ip-dual interface
show ip-dual interface summary
show ip-dual interface up
show ip-dual interface down
show ip-dual interface vlan <vlan id>
```

Input mode

User mode and administrator mode

Parameters

summary

Displays a summary of the status of all interfaces.

up

Displays detailed information about interfaces in the `Up` status.

down

Displays detailed information about interfaces in the `Down` status.

vlan <*vlan id*>

Displays detailed information about the applicable interface.

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

Operation when all parameters are omitted:

Displays the detailed status of all interfaces.

Example 1

This example shows how to display a summary of the status of all interfaces.

`>show ip-dual interface summary` Press the **Enter** key.

Figure 21-1 Example of displaying a summary of all interfaces

```
> show ip-dual interface summary

Date 2012/03/03 14:49:28 UTC
VLAN0004: Up  2001:254::249/64
              fe80::2eb:f0ff:fe02:1%VLAN0004/64
VLAN0010: Up  192.168.253.44/24
              2001::1:10/64
              fe80::2eb:f0ff:fe02:1%VLAN0010/64

>
```

Display items in Example 1

Table 21-1 Information displayed for a summary of all interfaces

Item	Meaning	Displayed detailed information
VLANxxxx	Interface name	--

Item	Meaning	Displayed detailed information
Up/Down	Status of the interface	--
Dot notation	IPv4 address/subnet mask length	If the secondary IP address is set, it is displayed followed by the primary IP address.
Colon notation	IPv6 address/prefix length	`duplicated`: The address is duplicated. `tentative`: The address is being checked for duplication. `autonomous`: Automatically generated triggered by reception of RA.

Example 2

- Display detailed information about interfaces in the `Up` status.

  `>show ip-dual interface up` Press the **Enter** key.

- Display the detailed status of an interface.

  `> show ip-dual interface vlan 10` Press the **Enter** key.

The following shows an example of executing the command with an interface specified.

Figure 21-2 Example of executing the command with an interface specified

```
> show ip-dual interface vlan 10

Date 2012/03/03 14:50:20 UTC
VLAN0010: Up
  mtu 1500
  inet 192.168.253.44/24 broadcast 192.168.253.255
  inet6 2001::1:10/64
  inet6 fe80::2eb:f0ff:fe02:1%VLAN0010/64
  Port 0/1 : Up media 1000BASE-T full(auto) 00eb.f002.0001
  Port 0/2 : Up media 1000BASE-T full(auto) 00eb.f002.0001 ChGr:5 (Up)
  Port 0/4 : Down media - 00eb.f002.0001 ChGr:5 (Up)
  Time-since-last-status-change: 00:17:11
  Last down at: 2012/03/03 14:32:52
  VLAN: 10

>
```

Display items in Example 2

Table 21-2 Contents of the displayed detailed information

Item	Meaning	Displayed detailed information
VLANxxxx	Interface name	--
Up/Down	Status of the interface	--
mtu	MTU for the interface	--
inet	IPv4 address/subnet mask length	If the secondary IP address is set, it is displayed followed by the primary IP address.

Item	Meaning	Displayed detailed information
broadcast	Broadcast address	--
inet6	IPv6 address/prefix length	`duplicated`: The address is duplicated. `tentative`: The address is being checked for duplication. `autonomous`: Automatically generated triggered by reception of RA.
Port	Port number that belongs to the applicable VLAN	--
Up/Down	Port status	`Up`: In operation (normal operating state) `Down`: In operation (line has failed), or not in operation
media	Line type	For details about the line type, see the display item *<line type>* in `show interfaces` command.
xxxx.xxxx.xxxx	MAC address	The MAC address used by packets sent from the interface.
ChGr	Channel group number and channel status	Displayed for a link aggregation line. `Up`: Indicates that the channel status is Up. `Down`: Indicates that the channel status is Down.
Time-since-last-status-change	Time elapsed since the status changed to `Up` or `Down`.	Time elapsed since the status of the VLAN interface last changed. The display format is *hour*`:`*minute*`:`*second* or *number-of-days*`,`*hour*`:`*minute*`:`*second*. `Over 100 days` is displayed if the number of days exceeds 100. `-----` is displayed if there has never been an `Up`/`Down` status change. This is not cleared by adding, deleting, or changing IP addresses.
Last down at	Status of the interface	Time the VLAN interface last went down. The display format is *year*`/`*month*`/`*day* *hour*`:`*minute*`:`*second*. `-----` is displayed if the interface has never gone down. This is not cleared by adding, deleting, or changing IP addresses.
VLAN	VLAN ID	1 to 4094

Impact on communication

None

Response messages

Table 21-3 List of response messages for the show ip-dual interface command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no information. (ip-dual interface)	There is no ip-dual interface information.

Notes

None

show ipv6 interface

Displays the status of the IPv6 interface.

Syntax

```
show ipv6 interface
show ipv6 interface summary
show ipv6 interface up
show ipv6 interface down
show ipv6 interface vlan <vlan id>
```

Input mode

User mode and administrator mode

Parameters

summary

Displays a summary of the status of all interfaces.

up

Displays detailed information about interfaces in the `Up` status.

down

Displays detailed information about interfaces in the `Down` status.

vlan *<vlan id>*

Displays detailed information about the applicable interface.

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

Operation when all parameters are omitted:

Displays the detailed status of all interfaces.

Example 1

This example shows how to display a summary of the status of all interfaces.

`>show ipv6 interface summary` Press the **Enter** key.

Figure 21-3 Example of displaying a summary of all interfaces

```
> show ipv6 interface summary

Date 2012/03/03 14:33:50 UTC
VLAN0010: Up  2001::1:10/64
              fe80::2eb:f0ff:fe02:1%VLAN0010/64

>
```

Display items in Example 1

Table 21-4 Information displayed for a summary of all interfaces

Item	Meaning	Displayed detailed information
VLANxxxx	Interface name	--
Up/Down	Status of the interface	--

Item	Meaning	Displayed detailed information
Colon notation	IPv6 address/prefix length	`duplicated`: The address is duplicated. `tentative`: The address is being checked for duplication. `autonomous`: Automatically generated triggered by reception of RA.

Example 2

- This example shows how to display detailed information about interfaces in the `Up` status.

  `>show ipv6 interface up` Press the **Enter** key.

- Display the detailed status of an interface.

  `> show ipv6 interface vlan 10` Press the **Enter** key.

The following figure shows an example of executing the command with an interface specified.

Figure 21-4 Example of executing the command with an interface specified

```
> show ipv6 interface vlan 10

Date 2012/03/03 14:34:28 UTC
VLAN0010: Up
  mtu 1500
  inet6 2001::1:10/64
  inet6 fe80::2eb:f0ff:fe02:1%VLAN0010/64
  Port 0/1 : Up media 1000BASE-T full(auto) 00eb.f002.0001
  Port 0/2 : Up media 1000BASE-T full(auto) 00eb.f002.0001 ChGr:5 (Up)
  Port 0/4 : Down media - 00eb.f002.0001 ChGr:5 (Up)
  Time-since-last-status-change: 00:01:19
  Last down at: 2012/03/03 14:32:52
  VLAN: 10

>
```

Display items in Example 2

The following describes the detailed information items.

Table 21-5 Contents of the displayed detailed information

Item	Meaning	Displayed detailed information
VLANxxxx	Interface name	--
Up/Down	Status of the interface	--
mtu	MTU for the interface	--
inet6	IPv6 address/prefix length	`duplicated`: The address is duplicated. `tentative`: The address is being checked for duplication. `autonomous`: Automatically generated triggered by reception of RA.

Item	Meaning	Displayed detailed information
Port	Port number that belongs to the applicable VLAN	--
Up/Down	Port status	`Up`: In operation (Normal operating state) `Down`: In operation (line has failed), or not in operation
media	Line type	For details about the line type, see the display item *<line type>* in `show interfaces` command.
xxxx.xxxx.xxxx	MAC address	The MAC address used by packets sent from the interface.
ChGr	Channel group number and channel status	Displayed for a link aggregation line. `Up`: Indicates that the channel status is Up. `Down`: Indicates that the channel status is Down.
Time-since-last-status-change	Time elapsed since the status changed to `Up` or `Down`.	Time elapsed since the status of the VLAN interface last changed. The display format is *hour*`:`*minute*`:`*second* or *number-of-days*`,`*hour*`:`*minute*`:`*second*. `Over 100 days` is displayed if the number of days exceeds 100. `-----` is displayed if there has never been an `Up`/`Down` status change. This is not cleared by adding, deleting, or changing IP addresses.
Last down at	Status of the interface	Time the VLAN interface last went down. The display format is *year/month/day hour*`:`*minute*`:`*second*. `-----` is displayed if the interface has never gone down. This is not cleared by adding, deleting, or changing IP addresses.
VLAN	VLAN ID	1 to 4094

Impact on communication

None

Response messages

Table 21-6 Response messages for the show ipv6 interface command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no information. (ipv6 interface)	There is no ipv6 interface information.

Notes

None

show ipv6 neighbors

Displays NDP information.

Syntax

```
show ipv6 neighbors [detail]
show ipv6 neighbors interface vlan <vlan id> [detail]
```

Input mode

User mode and administrator mode

Parameters

detail

Displays the IPv6 address without omission.

As a result, information exceeding the display width might be displayed.

Operation when this parameter is omitted:

For IPv6 addresses, only the first 31 characters are displayed.

interface vlan <*vlan id*>

Specifies a VLAN ID.

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

Operation when all parameters are omitted:

Displays all registered NDP information.

Example

Figure 21-5 Execution result when a VLAN interface is specified

```
> show ipv6 neighbors interface vlan 4094

Date 2012/03/07 11:05:51 UTC
Total: 7
Neighbor                        Linklayer Address Interface  Expire    S Flgs
2001:254::2                     782b.cb7f.7fa1    VLAN4094   1s        R
2001:254::99                    1cc1.de64.f234    VLAN4094   14s       R
2001:254::252                   0012.e282.680d    VLAN4094   permanent R S
2001:254::951:b8c:84bd:9cd3     1cc1.de64.f234    VLAN4094   6s        R
fe80::1bc:91af:3b96:2f72%VLAN40 782b.cb7f.7fa1    VLAN4094   19m56s    S
fe80::212:e2ff:fe82:680d%VLAN40 0012.e282.680d    VLAN4094   permanent R S
fe80::951:b8c:84bd:9cd3%VLAN409 1cc1.de64.f234    VLAN4094   19m56s    S

>
> show ipv6 neighbors interface vlan 4094 detail

Date 2012/03/07 11:06:10 UTC
Total: 8
Neighbor                          Linklayer Address Interface  Expire    S Flgs
2001:254::2                       782b.cb7f.7fa1    VLAN4094   24s       R
2001:254::99                      1cc1.de64.f234    VLAN4094   19m55s    S
2001:254::252                     0012.e282.680d    VLAN4094   permanent R S
2001:254::951:b8c:84bd:9cd3       1cc1.de64.f234    VLAN4094   19m47s    S
2001:254::aca8:3ee1:bfe9:1bef     782b.cb7f.7fa1    VLAN4094   18s       R
fe80::1bc:91af:3b96:2f72%VLAN4094 782b.cb7f.7fa1    VLAN4094   19m37s    S
fe80::212:e2ff:fe82:680d%VLAN4094 0012.e282.680d    VLAN4094   permanent R S
fe80::951:b8c:84bd:9cd3%VLAN4094  1cc1.de64.f234    VLAN4094   19m37s    S
```

>

Display items

Table 21-7 Displaying interface information

Item	Meaning	Displayed detailed information
Total	Number of entries	Number of used NDP table entries
Neighbor	Next Hop IP address	--
Linklayer Address	MAC address of a neighboring device	`(incomplete)` is displayed when the status information of the displayed item `S` shows `I`.
Interface	Interface name	Interface name for the switch
Expire	XXmXXs permanent expired	Remaining time before the entry expires (minute and second) Permanent entry Expired entry
S	I,R,S,D,P	Status information `I`: Incomplete `R`: Reachable `S`: Stale `D`: Delay `P`: Probe
Flgs	S	Entry information `S`: Static

Impact on communication

None

Response messages

Table 21-8 List of response messages for the show ipv6 neighbors command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
No such interface.	The specified interface has not been configured. Make sure the specified parameter is correct, and then try again.
There is no information. (ipv6 neighbors)	The neighbor information was not found.

Notes

None

clear ipv6 neighbors

Clears dynamic NDP information.

Syntax

```
clear ipv6 neighbors
clear ipv6 neighbors interface vlan <vlan id>
```

Input mode

User mode and administrator mode

Parameters

interface vlan <*vlan id*>

Specifies a VLAN ID.

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

Operation when this parameter is omitted:

Clears the registered NDP information.

Example

Figure 21-6 Execution result of clearing the NDP information (deleting the NDP information for a specific VLAN interface)

```
> show ipv6 neighbors interface vlan 4094

Date 2012/03/07 11:10:13 UTC
Total: 8
Neighbor                        Linklayer Address Interface  Expire    S Flgs
2001:254::2                     782b.cb7f.7fa1    VLAN4094   17s       R
2001:254::99                    1cc1.de64.f234    VLAN4094   19s       R
2001:254::252                   0012.e282.680d    VLAN4094   permanent R S
2001:254::951:b8c:84bd:9cd3     1cc1.de64.f234    VLAN4094   23s       R
2001:254::aca8:3ee1:bfe9:1bef   782b.cb7f.7fa1    VLAN4094   19m46s    S
fe80::1bc:91af:3b96:2f72%VLAN40 782b.cb7f.7fa1    VLAN4094   15m34s    S
fe80::212:e2ff:fe82:680d%VLAN40 0012.e282.680d    VLAN4094   permanent R S
fe80::951:b8c:84bd:9cd3%VLAN409 1cc1.de64.f234    VLAN4094   15m34s    S

> clear ipv6 neighbors interface vlan 4094

> show ipv6 neighbors interface vlan 4094

Date 2012/03/07 11:11:18 UTC
Total: 2
Neighbor                        Linklayer Address Interface  Expire    S Flgs
2001:254::252                   0012.e282.680d    VLAN4094   permanent R S
fe80::212:e2ff:fe82:680d%VLAN40 0012.e282.680d    VLAN4094   permanent R S

>
```

Display items

None

Impact on communication

None

Response messages

Table 21-9 List of response messages for the clear ipv6 neighbors command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
No such interface.	The specified interface has not been configured. Make sure the specified parameter is correct, and then try again.

Notes

None

show ipv6 router-advertisement

Displays RA information.

Syntax

```
show ipv6 router-advertisement
```

Input mode

User mode and administrator mode

Parameters

None

Example and Display items

Figure 21-7 Execution result of displaying RA information

```
> show ipv6 router-advertisement

Date 2012/03/07 10:37:06 UTC
Default gateway: fe80::212:e2ff:fe82:680d%VLAN4094
Current hop limit: 64

>
```

Table 21-10 Displaying RA information

Item	Meaning	Displayed detailed information
Default gateway	IPv6 default gateway	The gateway specified in `ipv6 default-gateway` configuration command is displayed when the RA information is not received, If no IPv6 default gateway exists, `none` is displayed.
Current hop limit	Hop limit of IPv6 packets (excluding that of ping and traceroute) sent from the Switch	The default value 64 is displayed when the RA information is not received,

Impact on communication

None

Response messages

Table 21-11 List of response messages for the show ipv6 router-advertisement command

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

Notes

None

ping ipv6

The `ping ipv6` command is used to determine whether communication is possible with the device with the specified IPv6 address. This command is used with IPv6 only.

Syntax

```
ping ipv6 <host> [numeric] [summary] [hostname] [count <count>]
          [interval <wait>] [preload <preload>] [pad-byte <pattern>]
          [source <source address>] [packetsize <size>] [hoplimit <hops>]
ping ipv6 <host> compact [numeric] [hostname] [count <count>] [interval <wait>]
          [pad-byte <pattern>] [source <source address>] [packetsize <size>]
          [hoplimit <hops>]
ping ipv6 <host> simple [numeric] [hostname] [count <count>] [interval <wait>]
          [pad-byte <pattern>] [source <source address>] [packetsize <size>]
          [hoplimit <hops>]
```

Input mode

User mode and administrator mode

Parameters

<host>

Specifies the destination host name, an IPv6 address, or an IPv6 address with an interface name (for a link-local address only).

compact

Displays the execution results in a simplified format using the following symbols. If this parameter is specified, the initial value of the `ping ipv6` transmission count is set to `5`. ICMP error messages are not displayed if those are not related to `Ping` currently executing.

`!`: Response received (ICMPv6 Echo Reply)

`.`: No response

`U`: No route (ICMPv6 Destination Unreachable: No route to destination)

`A`: Access denied

(ICMPv6 Destination Unreachable: Communication with destination administratively prohibited)

`N`: Beyond the scope of addresses

(ICMPv6 Destination Unreachable: Beyond scope of source address)

`H`: Address unreachable

(ICMPv6 Destination Unreachable: Address unreachable)

`S`: Port unreachable (ICMPv6 Destination Unreachable: Port unreachable)

`@`: Unreachable destinations other than above (ICMPv6 Destination Unreachable: Undefined code)

`B`: Packet too big (ICMPv6 Packet too big)

`T`: Time exceeded (ICMPv6 Time exceeded)

`P`: Parameter problem (ICMPv6 Parameter problem)

If no response is sent within the sending interval, it is determined that no response (a timeout) occurred. When a response is received after the timeout, ! is displayed followed by period (`.`).

This parameter cannot be specified together with the `simple`, `summary`, or `preload`

parameter.

simple

Displays the execution results in a simplified format using the following symbols. If this parameter is specified, the initial value of the transmission count is set to `5`.

`!`: Response received (ICMP Echo Reply)

`.`: No response

Note that "no response" symbols are displayed together with a "response received" symbol when a response is received after the time that no response was received (Echo Reply was missing). Therefore, no-response symbols are displayed real-time while no response is received. If a response is passed by another response (a response to the echo request sent later is received first before that to the echo request sent earlier is received), `!` is not displayed for the response that has to be received first.

This parameter cannot be specified together with the `compact`, `summary`, or `preload` parameter.

numeric

Displays the host IPv6 address without converting it to a name.

This parameter cannot be specified togeher with the `numeric` or `hostname` parameter.

Operation when this parameter is omitted:

If the `hostname` parameter is specified, the name converted from the IPv6 address of the host is displayed.

If the `hostname` parameter is not specified, the IPv6 address of the host is displayed without being converted to a name.

hostname

Displays the output results as a host name.

This parameter cannot be specified togeher with the `numeric` or `hostname` parameter.

Operation when this parameter is omitted:

Displays the host IPv6 address without converting it to a name.

summary

Restricts the output. Only the summary lines of the first and last lines are displayed.

Operation when this parameter is omitted:

Displays one line for one response as regular display mode.

count *<count>*

Sends packets for the number of times specified for *<count>*, and then finishes the processing. To interrupt the processing, press **Ctrl** + **C**. The specifiable values are from 1 to 2147483647. Note that if the `simple` parameter is specified, packets are sent a maximum of 65536 times.

After packets for the specified count are sent, when the responses to all the packets are received or the next sending interval and additional 10 seconds elapse, the reception stops.

Operation when this parameter is omitted:

Sends packets indefinitely. However, if the `compact` or `simple` parameter is specified, packets are sent five times.

interval *<wait>*

Sets the packet sending interval to the number of seconds specified for *<wait>*. The specifiable values are from 0.1 to 0.9, and from 1 to 2147483647. Values smaller

than one second can be specified in units of 0.1 seconds. Values from 1 to 2147483647 seconds can be specified in seconds.

Operation when this parameter is omitted:

The sending interval defaults to 1 second.

preload *<preload>*

Sends the number of packets specified in *<preload>* without any transmission interval *<wait>*, and then returns to normal operation. The specifiable values are from 1 to 2147483647.

<preload> is an included number of *<count>*. If the value specified for *<count>* is lower than *<preload>*, the transmission is carried out only for the count of *<count>*.

Operation when this parameter is omitted:

Preload sending is not performed.

pad-byte *<pattern>*

Specifies the pad bytes for packets to be sent. The maximum size of the pad is 16 bytes. This is effective for diagnosing data-dependent problems on the network. For example, specify `pad-byte ff` to generate an all-ones packet to be sent. You can specify a hexadecimal number consisting of 1 to 32 digits.

Operation when this parameter is omitted:

Generates pad characters by incrementing from 00 to ff.

source *<source address>*

Uses the IPv6 address specified for *<source address>* as the source address of an output packet. Only the IPv6 addresses set on the Switch can be specified.

Operation when this parameter is omitted:

The source IPv6 address selected by the Switch is used.

packetsize *<size>*

Specifies how many bytes of data are to be sent. The size of a packet to be sent is the sum of this value, 40 bytes of the IPv6 header, and 8 bytes of the ICMPv6 header. The specifiable values are from 1 to 65527.

Operation when this parameter is omitted:

The number of bytes of data to be sent is 8 (24 if pad bytes are specified).

hoplimit *<hops>*

Sets the value specified for *<hops>* to the Hop Limit field of the IPv6 header. The specifiable values are from 1 to 255.

Operation when this parameter is omitted:

`64` is set.

Operation when all parameters are omitted:

Displays one line for one response as regular display mode. ICMP error messages are also displayed to the echo requests sent by the ping command that is running.

Example

- Execute an echo test by specifying the default values (unlimited attempts, sending interval of 1 second, and data size of 8 bytes).

Figure 21-8 Example of executing the ping ipv6 command with default values

```
> ping ipv6 3000::1
PING6(56=40+8+8 bytes) 3000::2 --> 3000::1
16 bytes from 3000::1, icmp_seq=0 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=1 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=2 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=3 hlim=64 time=0 ms
```

```
16 bytes from 3000::1, icmp_seq=4 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=5 hlim=64 time=0 ms
16 bytes from 3000::1, icmp_seq=6 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=7 hlim=64 time=0 ms
16 bytes from 3000::1, icmp_seq=8 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=9 hlim=64 time=0 ms
16 bytes from 3000::1, icmp_seq=10 hlim=64 time=0 ms
^C                                  <---- To interrupt the processing, press Ctrl+C.
--- 3000::1 ping6 statistics ---
11 packets transmitted, 11 packets received, 0.0% packet loss
round-trip min/avg/max = 0/9/17 ms
>
```

- Execute an echo test by specifying the following conditions: 3 attempts, data size of 120 bytes, and a reply wait time of 2 seconds.

Figure 21-9 Example of executing the ping ipv6 command by specifying 3 attempts, data size of 120 bytes, and a reply wait time of 2 seconds

```
> ping ipv6 3000::1 count 3 packetsize 120 interval 2
```

- Execute an echo test by specifying the `compact` parameter and 10 attempts.

Figure 21-10 Example of executing the ping ipv6 command by specifying the compact parameter and 10 attempts

```
> ping ipv6 3000::1 compact count 10
PING6(56=40+8+8 bytes) 3000::2 --> 3000::1
!!!!!!!!!!
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max = 17/20/33 ms
>
```

- Execute an echo test by specifying the `simple` parameter, 100 attempts, and a sending interval of 0.5 seconds.

Figure 21-11 Example of executing the ping ipv6 command by specifying the simple parameter, 100 attempts, and a sending interval of 0.5 seconds

```
> ping ipv6 3000::1 simple count 100 interval 0.5
PING6(56=40+8+8 bytes) 3000::2 --> 3000::1
!!!!!!!!!!!!!!!!!!!!!.........................!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!
--- 3000::1 ping6 statistics ---
100 packets transmitted, 72 packets received, 28.0% packet loss
round-trip min/avg/max = 0/18/383 ms
>
```

Impact on communication

When the `preload` parameter is used, the rate of CPU utilization becomes high and transmission bandwidth is employed much, and this might give negative impacts to other processes, services, and communication.

Response messages

Table 21-12 List of messages for the ping ipv6 command

Message	Description
Can't assign requested address.	The specified IPv6 address has not been set on the Switch (when the `source` option is specified).

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Can't select a source address.	The source address could not be selected. If there is no route to the destination host, the source address cannot be selected.
Bad/invalid number of packets.	The sending count specified for `count` is too large. Reduce the sending count.
Unknown host.	An address corresponding to the host name was not found. The host name is not correct. Specify the correct host name.

Notes

- To halt execution of the `ping ipv6` command, press **Ctrl** + **C**.
- In IPv6, unlike IPv4, the address defined for the sending interface might not be a starting point address.

  To use the `ping ipv6` command to perform continuity confirmation, make sure that which address is selected for the starting point address. If a connection cannot be established, use the `source` parameter to specify another IPv6 address set on the interface for the device, and then perform continuity confirmation again.
- If the `ping ipv6` command is executed for an IPv6 address that is also used by another device, an IPv6 address that is different from the specified IPv6 address might return response messages.

  In addition, if the command is executed for the IPv6 address of an interface that has just started, response messages might be sent from a different IPv6 address for several seconds after the command is executed.
- When the `compact` or `simple` parameter is specified, you cannot specify the sending of unlimited numbers of ping transmissions.
- If a small value is specified for `interval`, "no response" might be displayed and no data is sent or received. Therefore, adjust the value according to the usage environment.
- If a small value is specified for `interval` and the command is executed on a terminal with a slow communication data rate, such as a console, "no response" might be displayed because the display takes time. In such a case, execute the command on a remote operation terminal with a fast communication data rate.
- If a small value is specified for `interval`, the actual sending of interval for packets depends on the load on the device. Therefore, the sending interval is not exactly the same as the time specified for `interval`. Packets are sent at the sending interval specified for `interval` when viewed as the average time for the entire ping test. However, a delay over 1 second (sending interval when the transmission interval is less than 1 second) is not compensatable.
- The precision of the response time is 1/60 second. When the response time is less than 1/60 seconds, the response time indication might be 0 millisecond.
- If `packetsize` exceeds 65487 bytes (9952 bytes when the destination is this Switch), no packet is sent and this consequently results in "no response".

traceroute ipv6

Displays the route (route of the passed gateways and response time between the gateways) over which ICMPv6 messages are sent to the destination host. This command is used with IPv6 only.

Syntax

```
traceroute ipv6 <host> [numeric] [hoplimit <hops>] [probes <nqueries>]
[source <source address>] [waittime <time>] [packetsize <size>]
```

Input mode

User mode and administrator mode

Parameters

<host>

Specifies the destination host name, an IPv6 global unicast address, or an IPv6 link local unicast address with an interface name (for `fe80::/64` only).

numeric

Displays the gateway address by the IPv6 address, not by the host name.

Operation when this parameter is omitted:

Displays the name converted from the host IPv6 address.

hoplimit *<hops>*

Sets the maximum number of hops for the probe packets to be sent. The specifiable values are from 1 to 255.

Operation when this parameter is omitted:

The maximum number of hops is 30.

probes *<nqueries>*

Specify the number of times a search is performed for each hop in *<nqueries>*. The specifiable values are from 1 to 4294967295.

Operation when this parameter is omitted:

A search is performed 3 times.

source *<source address>*

Uses the IPv6 address specified for *<source address>* as the source address of an output packet. Only the IPv6 addresses set on the Switch can be specified.

Operation when this parameter is omitted:

The source IPv6 address selected by the Switch is used.

waittime *<time>*

Specify the time (in seconds) to wait for a probe packet. The specifiable values are from 2 to 2147483647.

Operation when this parameter is omitted:

The wait time for a response is 5 seconds.

packetsize *<size>*

Specify, in bytes, the data size of a probe packet. The specifiable values are from 8 to 65527.

Operation when this parameter is omitted:

The data size is set to 8 bytes.

Operation when all parameters are omitted:

The same as described in *Operation when this parameter is omitted* for each parameter.

Example

Figure 21-12 Execution result of the traceroute ipv6 command

```
> traceroute ipv6 100::2 numeric
traceroute6 to 100::2 (100::2) from 3000::2, 30 hops max, 8 byte packets
 1  3000::1  33 ms  0 ms  0 ms
 2  100::2  33 ms  33 ms  17 ms
>
```

Impact on communication

None

Response messages

Table 21-13 List of response messages for the traceroute ipv6 command

Message	Description
Can't assign requested address.	The specified IPv6 address has not been set on the Switch (when the `source` option is specified).
Can't execute.	The command could not be executed. Re-execute the command.
Can't select a source address.	The source address could not be selected. If there is no route to the destination host, the source address cannot be selected.
Unknown host.	An address corresponding to the host name was not found. The host name is not correct. Specify the correct host name.

Notes

- In IPv6, unlike IPv4, the address defined for the sending interface might not be a starting point address. To use the `traceroute ipv6` command to perform forwarding route confirmation, check which address is selected for the starting point address. If a connection cannot be established, use the `source` parameter to specify another IPv6 address set on the interface for the device, and then confirm everything again.
- If the `traceroute ipv6` command is executed for an IPv6 address that is also used by another device, an IPv6 address that is different from the specified IPv6 address might return response messages.

  In addition, if the command is executed for the IPv6 address of an interface that has just started, response messages might be sent from a different IPv6 address.
- The precision of the response time is 1/60 second. When the response time is less than 1/60 seconds, the response time indication might be 0 millisecond.
- If `packetsize` exceeds 65487 bytes (9952 bytes when the destination is this Switch), no packet is sent and this consequently results in "no response".

22. DHCP Server Functionality

show ip dhcp binding
clear ip dhcp binding
show ip dhcp conflict
clear ip dhcp conflict
show ip dhcp server statistics
clear ip dhcp server statistics

show ip dhcp binding

Displays the binding information on the DHCP server.

Syntax

```
show ip dhcp binding [{<IP address> | sort}]
```

Input mode

User mode and administrator mode

Parameters

{*<IP address>* | sort}

<IP address>

Displays the binding information for the specified IP address.

sort

Displays the binding information sorted in ascending order using the IP address as the key.

Operation when this parameter is omitted:

Displays all binding information on the DHCP server without sorting.

Example

Figure 22-1 Execution result of displaying binding information on the DHCP server

```
> show ip dhcp binding

Date 2010/07/23 08:41:12 UTC
 No   IP Address        MAC Address      Lease Expiration       Type
    1 192.168.1.1       0012.e2c4.a8c7                          Manual
    2 192.168.1.0       0012.e26a.015c   2010/07/24 08:34:05    Automatic
    3 192.168.1.2       0012.e26a.015f   2010/07/24 08:34:06    Automatic

>
```

Display items

Table 22-1 Items displayed for the binding information on the DHCP server

Item	Meaning	Displayed detailed information
No	Entry number	--
IP Address	Current IP address connected to the DHCP server	--
MAC Address	MAC address	--
Lease Expiration	Lease expiration date and time	*year*/*month*/*day* *hour*:*minute*:*second* A hyphen (-) is displayed when this item is set to infinity.

Item	Meaning	Displayed detailed information
Type	Connection type (Manual or Automatic)	Manual: Binding information assigned based on host settings Automatic: Binding information assigned dynamically

Impact on communication

None

Response messages

Table 22-2 List of response messages for the show ip dhcp binding command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
No such IP Address.	The specified IP address could not be found.
There is no information. (binding)	There is no binding information.

Notes

Binding information for which the lease has been expired is not displayed.

clear ip dhcp binding

Deletes the binding information from the DHCP server database.

Syntax

```
clear ip dhcp binding [{<IP address> | all}]
```

Input mode

User mode and administrator mode

Parameters

{*<IP address>* | all}

<IP address>

Deletes binding information for the specified IP address.

all

All IP addresses in the binding information are deleted.

Operation when this parameter is omitted:

All IP addresses in the binding information are deleted.

Example

Figure 22-2 Execution result of deleting all IP addresses in the binding information

```
> clear ip dhcp binding all

>
```

Display items

None

Impact on communication

None

Response messages

Table 22-3 List of response messages for the clear ip dhcp binding command

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

Notes

None

show ip dhcp conflict

Displays an IP address conflict detected by the DHCP server. An IP address conflict refers to an IP address assigned to a terminal over the network, although it is blank as a pool IP address on the DHCP server. Before the DHCP server assigns the IP address to a DHCP client, the DHCP server detects an IP address conflict by checking for a response to a sent ICMP packet, or DECLINE message reception.

Syntax

```
show ip dhcp conflict [<IP address>]
```

Input mode

User mode and administrator mode

Parameters

<IP address>

Displays the IP address conflict information for the specified IP address.

Operation when this parameter is omitted:

All IP address conflict information detected by the DHCP server is displayed.

Example

Figure 22-3 Execution result of displaying IP address conflict information detected by the DHCP server

```
> show ip dhcp conflict

Date 2010/08/06 06:09:04 UTC
 No   IP Address        Detection Time
    1 192.168.1.0       2010/08/06 06:02:17
    2 192.168.1.1       2010/08/06 06:02:18
    3 192.168.1.2       2010/08/06 06:02:18

>
```

Display items

Table 22-4 Items displayed for IP address conflict information detected by DHCP server

Item	Meaning	Displayed detailed information
No	Entry number	--
IP Address	IP address conflict detected by the DHCP server	--
Detection Time	Detection time	*year*/*month*/*day* *hour*:*minute*:*second*

Impact on communication

None

Response messages

Table 22-5 List of response messages for the show ip dhcp conflict command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
No such IP Address.	The specified IP address could not be found.
There is no information. (conflict)	There is no IP address conflict information.

Notes

None

clear ip dhcp conflict

Clears the IP address conflict information from the DHCP server.

Syntax

```
clear ip dhcp conflict [{<IP address> | all}]
```

Input mode

User mode and administrator mode

Parameters

{*<IP address>* | all}

<IP address>

Deletes IP address conflict information for the specified IP address.

all

All IP address conflict information is deleted.

Operation when this parameter is omitted:

All IP address conflict information is deleted.

Example

Figure 22-4 Execution result of deleting all IP address conflict information detected by the DHCP server

```
> clear ip dhcp conflict all

>
```

Display items

None

Impact on communication

None

Response messages

Table 22-6 List of response messages for the clear ip dhcp conflict command

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

Notes

An entry that duplicates the local IP address cannot be cleared.

show ip dhcp server statistics

Displays statistics about the DHCP server.

Syntax

```
show ip dhcp server statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 22-5 Execution result of displaying DHCP server statistics

```
> show ip dhcp server statistics

Date 2010/07/23 08:34:35 UTC
   < DHCP Server use statistics >
     address pools          : 1010
     automatic bindings     : 13
     manual bindings        : 1
     expired bindings       : 0
     over pools request     : 0
     discard packets        : 0
   < Receive Packets >
     DHCPDISCOVER           : 14
     DHCPREQUEST            : 14
     DHCPDECLINE            : 0
     DHCPRELEASE            : 0
     DHCPINFORM             : 1
   < Send Packets >
     DHCPOFFER              : 14
     DHCPACK                : 15
     DHCPNAK                : 0

>
```

Display items

Table 22-7 Items displayed for the DHCP server statistics

Item	Meaning	Displayed detailed information
< DHCP Server use statistics >	Statistics about the DHCP server	--
address pools	Number of pooled IP addresses (the number of remaining IP addresses)	--
automatic bindings	Number of automatic bindings	--
manual bindings	Number of static bindings	--
expired bindings	Number of completed releases	--

Item	Meaning	Displayed detailed information
over pools request	Number of insufficient pooled IP addresses that has been detected	--
discard packets	Number of discarded packets	--
< Receive Packets >	The number of received packets	--
DHCPDISCOVER	Number of received DHCPDISCOVER packets	--
DHCPREQUEST	Number of received DHCPREQUEST packets	--
DHCPDECLINE	Number of received DHCPDECLINE packets	--
DHCPRELEASE	Number of received DHCPRELEASE packets	--
DHCPINFORM	Number of received DHCPINFORM packets	--
< Send Packets >	Send packet information	--
DHCPOFFER	Number of sent DHCPOFFER packets	--
DHCPACK	Number of sent DHCPACK packets	--
DHCPNAK	Number of sent DHCPNAK packets	--

Impact on communication

None

Response messages

Table 22-8 List of response messages for the show ip dhcp server statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
DHCP Server is not configured.	A DHCP server has not been configured. Check the configuration.

Notes

None

clear ip dhcp server statistics

Clears the DHCP server statistics.

Syntax

```
clear ip dhcp server statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 22-6 Result of executing the command for clearing DHCP statistics

```
> clear ip dhcp server statistics

>
```

Display items

None

Impact on communication

None

Response messages

Table 22-9 List of response messages for the clear ip dhcp server statistics command

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

Notes

None

23. Filters

show access-filter
clear access-filter

show access-filter

Displays the filter conditions applied on the Ethernet interface or VLAN interface by the access group commands (`mac access-group`, `ipv6 traffic-filter`, and `ip access-group`), the number of packets that met the filter conditions, and the number of packets discarded because they did not match any filter conditions in the access list.

Syntax

```
show access-filter [{<IF#> | interface vlan <vlan id>}[<access list name>]][{in | out}]
```

Input mode

User mode and administrator mode

Parameters

{*<IF#>* | interface vlan *<vlan id>*}[*<access list name>*]

<IF#>

Displays statistics for the specified Ethernet interface. For the specifiable range of *<IF#>* 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 name>

<access list name>: Specifies the ID

Displays statistics for the specified ID for the specified interface.

Operation when this parameter is omitted:

Displays statistics for all access lists applied to the specified interface.

{ in | out }

`in`: Inbound (Specifies the receiving side)

`out`: Outbound (Specifies the sending side)

Displays statistics for the receiving side or the sending side of the specified interface.

Operation when this parameter is omitted:

Displays statistics for the receiving side and the sending side of the specified interface.

Operation when all parameters are omitted:

Displays statistics for all interfaces.

Example

Figure 23-1 Result of displaying the extended MAC access list

```
> show access-filter 0/3 in only-appletalk

Date 2011/06/16 16:28:03 UTC
Using Port:0/3 in
Extended MAC access-list:only-appletalk
  remark "permit only appletalk"
  10 permit any any appletalk
    matched packets         :      23741
  20 permit any any 0x80f3
    matched packets         :        363
  implicitly denied packets :       2883
```

```
>
```

Figure 23-2 Result of displaying the standard IPv4 access list

```
> show access-filter 0/7 in No12

Date 2011/06/16 16:38:56 UTC
Using Port:0/7 in
Standard IP access-list:No12
  remark "permit only host pc"
  10 permit host 10.10.10.1
    matched packets         :       2987
  20 permit host 10.10.10.254
    matched packets         :          0
  implicitly denied packets :       5676

>
```

Figure 23-3 Result of displaying the extended IPv4 access list

```
> show access-filter 0/11 in No128

Date 2011/06/16 16:51:55 UTC
Using Port:0/11 in
Extended IP access-list:No128
  remark "permit only http server"
  10 permit tcp any host 10.10.10.2 eq http
    matched packets         :   19370343
  implicitly denied packets :       8061

>
```

Figure 23-4 Result of displaying the extended IPv6 access list

```
> show access-filter 0/13 in only-ra

Date 2011/06/16 17:12:40 UTC
Using Port:0/13 in
IPv6 access-list:only-ra
  remark "permit only Router-11"
  10 permit icmp host fe80::213:20ff:fea5:24ab any router-advertisement
    matched packets         :         18
  implicitly denied packets :       1140

>
```

Figure 23-5 Result of displaying information when In or Out is omitted

```
> show access-filter interface vlan 1500

Date 2011/06/16 17:33:23 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         :   50310935
  implicitly denied packets :      31394
IPv6 access-list:only-ra
  remark "permit only Router-11"
  10 permit icmp host fe80::213:20ff:fea5:24ab any router-advertisement
    matched packets         :          9
  implicitly denied packets :        268

Using Interface:vlan 1500 out
Extended IP access-list:only-https
  remark "permit only https"
```

```
  10 permit tcp any any eq https
    matched packets         :   52826479
  implicitly denied packets :       6794

>
```

Display items

Table 23-1 Statistical items for the access list

Item	Displayed information	
	Detailed information	**Meaning**
Interface information	Using Port:<*IF#*> in	Information about an interface to which an access list has been applied on the inbound side
	Using Port:<*IF#*> out	Information about an interface to which an access list has been applied on the outbound side
	Using Interface:vlan<*vlan id*> in	Information about a VLAN interface to which an access list has been applied on the inbound side
	Using Interface:vlan<*vlan id*> out	Information about a VLAN interface to which an access list has been applied on the outbound side
Access list ID	Extended MAC access-list:<*access list name*>	Extended MAC access list ID
	Standard IP access-list:<*access list name*>	Standard IPv4 access list ID
	Extended IP access-list:<*access list name*>	Extended IPv4 access list ID
	IPv6 access-list:<*access list name*>	IPv6 access list ID
Access list information	Displays the supplementary explanation and the filter conditions that have been set by the access list command (see *21 Access Lists* in the manual *Configuration Command Reference*).	
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 23-2 List of response messages for the show access-filter command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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.	No access group was set for the access group for the specified ID *<access list name>*. Make sure the specified parameter is correct, and then try again.
No such interface.	The specified VLAN interface has not been configured. Make sure the specified parameter is correct, and then try again.

Notes

- When `layer2-1-out` or `layer2-2-out` is specified by the `flow-detection out mode` configuration command, the sent packets applied to the follwoiing conditions are discarded, however, counted only by the counter at the `permit` .
  - Specified as `permit` in the access list to the Ethernet interface
  - Specified as `deny` (including implicit discard) in the access list to the VLAN Ethernet interface
- Some packets are not supported by the filter functionality, however, they might be counted only by the counter displayed by this command (including `deny`). For details, see *1. Filters* in the *Configuration Guide Vol. 2*.
- Packets with a reception error (such as an FCS error) are discarded, however they might be counted on the counter displayed by this command.

clear access-filter

For the access list information displayed by the `show access-filter` command, this command clears, to zero, 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
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 23-6 Result of clearing the access list statistics to zero

```
> clear access-filter

>
```

Display items

None

Impact on communication

None

Response messages

Table 23-3 List of response messages for the clear access-filter command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
No configuration.	No access group was set for the Ethernet interface or VLAN interface. Make sure the access group setting is correct, and then try again.

Notes

None

24. QoS

show qos-flow
clear qos-flow
show qos queueing
clear qos queueing

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 [{<IF#> | interface vlan <vlan id>} [<qos flow list name>]]
```

Input mode

User mode and administrator mode

Parameters

{*<IF#>* | interface vlan *<vlan id>*} [*<qos flow list name>*]

<IF#>

Displays statistics for the specified Ethernet interface. For the specifiable range of *<IF#>* values, see *Specifiable values for parameters*.

intereface 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.

Displays statistics for the specified QoS flow list of the specified interface.

Operation when this parameter is omitted:

Displays statistics for all QoS flow lists applied to the specified interface.

Operation when all parameters are omitted:

Displays statistics for all interfaces.

Example

- The following shows an example of displaying QoS flow list information.

Figure 24-1 Result of displaying MAC QoS flow list information

```
> show qos-flow 0/1 QOS_LIST_MAC

Date 2011/06/16 17:40:31 UTC
Using Port:0/1 in
MAC qos-flow-list:QOS_LIST_MAC
  remark "user priority 6"
  10 qos 0012.f104.0001 0012.0000.0001 any action replace-user-priority 6
    matched packets         :        587

>
```

Figure 24-2 Result of displaying IPv4 QoS flow list information

```
> show qos-flow 0/1 QOS_LIST_IP

Date 2011/06/16 17:45:06 UTC
Using Port:0/1 in
IP qos-flow-list:QOS_LIST_IP
  remark "cos 1"
```

```
  10 qos udp any range 10000 65535 any action cos 1
    matched packets         :       2531

>
```

Figure 24-3 Result of displaying IPv6 QoS flow list information

```
> show qos-flow 0/1 QOS_LIST_IPv6

Date 2011/06/16 17:55:45 UTC
Using Port:0/1 in
IPv6 qos-flow-list:QOS_LIST_IPv6
  remark "nd is cos 7"
  10 qos icmp any any nd-na action cos 7
    matched packets         :          5
  20 qos icmp any any nd-ns action cos 7
    matched packets         :         12

>
```

Display items

Table 24-1 Display of statistics on the QoS flow list

Item	Displayed information	
	Detailed information	**Meaning**
Interface information	Using Port:<*IF#*> in	Information about an interface to which a QoS flow list is applied.
	Using Interface:vlan <*vlan id*> in	Information about a VLAN interface to which a QoS flow list is applied.
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 the supplementary explanation and the flow detection conditions that are set by the QoS flow list command (See *22. QoS* in the manual *Configuration Command Reference*).	
Statistics	matched packets:<*packets*>	Number of packets that meet the flow detection conditions in the QoS flow list

Impact on communication

None

Response messages

Table 24-2 List of response messages for the show qos-flow command

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

Message	Description
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 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 interface.	The specified VLAN interface has not been configured. Make sure the specified parameter is correct, and then try again.

Notes

- Some packets are not supported by the QoS functionality, however, they might be counted only by the counter displayed by this command. For details, see *3. Flow Control* in the *Configuration Guide Vol. 2*.
- Packets with a reception error (such as an FCS error) are discarded, however they might be counted on the counter displayed by this command.

clear qos-flow

Clears, to zero, the number of packets (indicated by `matched packets`) that met the flow detection conditions in the QoS flow list, which is displayed by the `show qos-flow` command.

Syntax

```
clear qos-flow
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 24-4 Result of clearing information

```
> clear qos-flow

>
```

Display items

None

Impact on communication

None

Response messages

Table 24-3 List of response messages for the clear qos-flow command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
No configuration.	No QoS flow group was set for the Ethernet interface or VLAN interface. Make sure the QoS flow group setting is correct, and then try again.

Notes

None

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 [<IF#>]
```

Input mode

User mode and administrator mode

Parameters

<IF#>

Displays information about the send queue of the specified port. For the specifiable range of *<IF#>* values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Displays information about the send queues of all ports implemented on the device, the send queues for traffic from the ports to the CPU, and the send queues for traffic among the internal LSIs (for AX2530S-48T, AX2530S-48T2X, and AX2530S-48TD switches).

Example

Figure 24-5 Result of displaying information about all send queues

```
> show qos queueing

Date 2012/07/02 21:02:34 UTC
To-CPU (outbound)
 Max_Queue=16
  Queue 1: Qlen=    0, Limit_Qlen=   64
  Queue 2: Qlen=    0, Limit_Qlen=   64
  Queue 3: Qlen=    0, Limit_Qlen=   64
  Queue 4: Qlen=    0, Limit_Qlen=   64
  Queue 5: Qlen=    0, Limit_Qlen=   64
  Queue 6: Qlen=    0, Limit_Qlen=   64
  Queue 7: Qlen=    0, Limit_Qlen=  256
  Queue 8: Qlen=    0, Limit_Qlen=  256
   discard packets
    HOL1=         0, HOL2=         0
  Queue 9: Qlen=    0, Limit_Qlen=   64
  Queue10: Qlen=    0, Limit_Qlen=   64
  Queue11: Qlen=    0, Limit_Qlen=   64
  Queue12: Qlen=    0, Limit_Qlen=   64
  Queue13: Qlen=    0, Limit_Qlen=   64
  Queue14: Qlen=    0, Limit_Qlen=   64
  Queue15: Qlen=    0, Limit_Qlen=  256
  Queue16: Qlen=    0, Limit_Qlen=  256
   discard packets
    HOL1=         0, HOL2=         0

SW (outbound)
 Max_Queue=32
  Queue 1: Qlen=    0, Limit_Qlen=   64
  Queue 2: Qlen=    0, Limit_Qlen=   64
```

```
  Queue 3: Qlen=    0, Limit_Qlen=   64
  Queue 4: Qlen=    0, Limit_Qlen=   64
  Queue 5: Qlen=    0, Limit_Qlen=   64
  Queue 6: Qlen=    0, Limit_Qlen=   64
  Queue 7: Qlen=    0, Limit_Qlen=   64
  Queue 8: Qlen=    0, Limit_Qlen=   64
   discard packets
    HOL1=         0, HOL2=         0
  Queue 9: Qlen=    0, Limit_Qlen=   64
  Queue10: Qlen=    0, Limit_Qlen=   64
  Queue11: Qlen=    0, Limit_Qlen=   64
  Queue12: Qlen=    0, Limit_Qlen=   64
  Queue13: Qlen=    0, Limit_Qlen=   64
  Queue14: Qlen=    0, Limit_Qlen=   64
  Queue15: Qlen=    0, Limit_Qlen=   64
  Queue16: Qlen=    0, Limit_Qlen=   64
   discard packets
    HOL1=         0, HOL2=         0
  Queue17: Qlen=    0, Limit_Qlen=   64
  Queue18: Qlen=    0, Limit_Qlen=   64
  Queue19: Qlen=    0, Limit_Qlen=   64
  Queue20: Qlen=    0, Limit_Qlen=   64
  Queue21: Qlen=    0, Limit_Qlen=   64
  Queue22: Qlen=    0, Limit_Qlen=   64
  Queue23: Qlen=    0, Limit_Qlen=   64
  Queue24: Qlen=    0, Limit_Qlen=   64
   discard packets
    HOL1=         0, HOL2=         0
  Queue25: Qlen=    0, Limit_Qlen=   64
  Queue26: Qlen=    0, Limit_Qlen=   64
  Queue27: Qlen=    0, Limit_Qlen=   64
  Queue28: Qlen=    0, Limit_Qlen=   64
  Queue29: Qlen=    0, Limit_Qlen=   64
  Queue30: Qlen=    0, Limit_Qlen=   64
  Queue31: Qlen=    0, Limit_Qlen=   64
  Queue32: Qlen=    0, Limit_Qlen=   64
   discard packets
    HOL1=         0, HOL2=         0

Port 0/1 (outbound)
 Status : Active
 Max_Queue=8, Rate_limit=100000kbit/s, Qmode=pq
  Queue 1: Qlen=    0, Limit_Qlen=   64
  Queue 2: Qlen=    0, Limit_Qlen=   64
  Queue 3: Qlen=    0, Limit_Qlen=   64
  Queue 4: Qlen=    0, Limit_Qlen=   64
  Queue 5: Qlen=    0, Limit_Qlen=   64
  Queue 6: Qlen=    0, Limit_Qlen=   64
  Queue 7: Qlen=    0, Limit_Qlen=   64
  Queue 8: Qlen=    0, Limit_Qlen=   64
   discard packets
    HOL1=         0, HOL2=         0

          :              :

>
```

Display items

Table 24-4 Display items of statistics

Item	Displayed information	
	Detailed information	**Meaning**
Interface information	Port*<IF#>* (outbound)	Port send queues
	To-CPU (outbound)	Send queues for traffic from the ports to the CPU
	SW (outbound)	Send queues for traffic among internal LSIs [48T] [48T2X] [48TD]
QoS information	Status	Operating status of the port ● `Active`: Operation in normal. ● `Inactive (The port is half duplex.)`: Unable to operate normally (The port is half duplex.) ● `Inactive (The shaping rate exceeds it.)`: Unable to operate normally (The shaping rate exceeds the line speed.) ● `Inactive (Two or more causes exist.)`: Unable to operate normally.(There are multiple causes.)
	Max_Queue=*<No.>*	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.
	Qmode=*<schedule_name>*	For details about the scheduling (pq,wrr,wfq,2pq+6drr), see the `qos-queue-list` configuration command in *22. QoS* in the manual *Configuration Command Reference*.
Queue information	Queue*<No.>*	Send queue number
	Qlen=*<length>*	Number of packet buffers used by the send queue
	Limit_Qlen=*<length>*	Maximum number of send queues

Item	Displayed information	
	Detailed information	**Meaning**
Port statistics	discard packets	Number of packets discarded without being accumulated in the send queue
	HOL1=*<packets>*	Number of packets discarded because the send queue or the packet buffer of the send port was full at the time of determination of the destination port after the packets were received. HOL is an abbreviation for head of line blocking.
	HOL2=*<packets>*	Number of packets discarded because there was no space for storing received packets in the send port packet buffer at the time of determination of the destination port after the packets were received.

Impact on communication

None

Response messages

Table 24-5 List of response messages for the show qos queueing command

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

Notes

None

clear qos queueing

For the information displayed by the `show qos queueing` command, this command clears, to zero, the number of packets (`HOL1`, `HOL2`, and `Tail_drop`) that were not placed in the send queue and were discarded.

Syntax

```
clear qos queueing
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 24-6 Result of clearing statistics for a port to zero

```
> clear qos queueing

>
```

Display items

None

Impact on communication

None

Response messages

Table 24-6 List of response messages for the clear qos queueing command

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

Notes

None

25. Common to Layer 2 Authentication

show authentication fail-list
clear authentication fail-list
show authentication logging
clear authentication logging

show authentication fail-list

Displays information related to terminals that failed to be authenticated by Layer 2 authentication in ascending order of MAC address.

Syntax

```
show authentication fail-list [mac <MAC>]
```

Input mode

Administrator mode

Parameters

mac *<MAC>*

Displays information related to terminals that failed to be authenticated for the specified MAC address.

Operation when this parameter is omitted:

Displays all information related to terminals that failed to be authenticated.

Example

Figure 25-1 Displaying information related to terminals that failed to be authenticated

```
# show authentication fail-list

Date 2010/09/16 13:30:17 UTC
Fail list total entry :   3
  No MAC address    Port VLAN First fail time     Last fail time          Count
   1 0000.e227.6812 0/15  400 2010/09/16 13:29:20 2010/09/16 13:29:20         1
   2 0013.20a5.3e1a 0/13  400 2010/09/16 13:29:20 2010/09/16 13:29:20         1
   3 00bb.cc01.0202 0/17  400 2010/09/16 13:29:20 2010/09/16 13:29:20         1

#
```

Display items

Table 25-1 Display items for the information related to terminals that failed to be authenticated

Item	Meaning	Displayed detailed information
Fail list total entry	Total number of entries related to terminals failing to be authenticated	Maximum of 256 entries
No	Entry number	--
MAC address	MAC address	--
Port	Port number or channel group number	`-` is displayed when this item is not set.
VLAN	VLAN ID	`1` to `4094`: Indicates a VLAN ID. A hyphen (`-`) is displayed when this item is not set.
First fail time	Date and time first authentication	*year/month/day*

Item	Meaning	Displayed detailed information
	attempt failed	*hour*:*minute*:*second*
Last fail time	Date and time last authentication attempt failed	*year*/*month*/*day* *hour*:*minute*:*second*
Count	Number of authentication failures	--

Impact on communication

None

Response messages

Table 25-2 List of response messages for the show authentication fail-list command

Message	Description
There is no information.	There is no information about terminals that failed to be authenticated.
Authentication is not configured.	The authentication functionality has not been configured. Check the configuration.

Notes

If the number of entries related to terminals that failed to be authenticated is 256 or more, the oldest entries are overwritten first.

clear authentication fail-list

Clears information related to terminals that failed to be authenticated by Layer 2 authentication.

Syntax

```
clear authentication fail-list
```

Input mode

Administrator mode

None

Parameters

None

Example

The following shows an example of clearing information related to terminals that failed to be authenticated by Layer 2 authentication.

```
# clear authentication fail-list

#
```

Display items

None

Impact on communication

None

Response messages

Table 25-3 List of response messages for the clear authentication fail-list command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Authentication is not configured.	The authentication functionality has not been configured. Check the configuration.

Notes

None

show authentication logging

Displays operational log messages logged for each type of Layer 2 authentication in chronological order.

Syntax

```
show authentication logging [search <string>]
```

Input mode

Administrator mode

Parameters

search *<string>*

Specifies the search string.

If you specify this parameter, the operation log message that includes the search string will be displayed.

Specify the string with 1 to 64 characters. The characters are case sensitive. For details, see *Any character string* in *Specifiable values for parameters*.

Operation when this parameter is omitted:

Displays all the operation log messages.

Example

Figure 25-2 Displayed operation log (When the parameter is omitted)

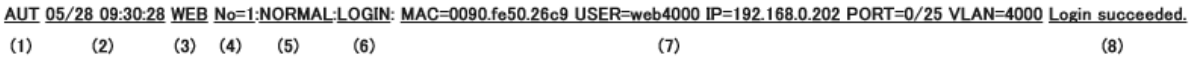
```
# show authentication logging

Date 2011/02/23 15:04:08 UTC
AUT 02/23 15:04:03 WEB No=84:NORMAL:SYSTEM: Accepted commit command.
AUT 02/23 15:03:17 MAC No=1:NORMAL:LOGIN: MAC=0013.20a5.3e2e PORT=0/22 VLAN=40 Login
succeeded.
AUT 02/23 15:03:17 MAC No=270:NOTICE:SYSTEM: MAC=0013.20a5.3e2e PORT=0/22 MAC address
was force-authorized.
AUT 02/23 15:02:57 MAC No=265:NORMAL:SYSTEM: MAC=0013.20a5.3e2e Start authenticating
for MAC address.
AUT 02/23 15:00:39 1X  No=1:NORMAL:LOGIN: MAC=18a9.051d.4931 PORT=0/5 VLAN=4 Login
succeeded. ; New Supplicant Auth Success.

#
```

Figure 25-3 Displayed operation log (When SYSTEM is specified for the parameter)

```
# show authentication logging search SYSTEM

Date 2011/02/23 15:06:08 UTC
AUT 02/23 15:04:03 WEB No=84:NORMAL:SYSTEM: Accepted commit command.
AUT 02/23 15:03:17 MAC No=270:NOTICE:SYSTEM: MAC=0013.20a5.3e2e PORT=0/22 MAC address
was force-authorized.
AUT 02/23 15:02:57 MAC No=265:NORMAL:SYSTEM: MAC=0013.20a5.3e2e Start authenticating
for MAC address.

 3 events matched.

#
```

Display items

The following shows the display format of a message. (Example: Web authentication)



(1) Log functionality type: Indicates the type of authentication functionality. (Fixed at `AUT`.)

(2) Date and time: Indicates the date and time (*month*`/`*date* *hour*`:`*minute*`:`*second*) an event occurred.

(3) Authentication ID: Indicates the type of Layer 2 authentication.

- `1X`: IEEE 802.1X
- `WEB`: Web authentication
- `MAC`: MAC-based authentication

For the meaning of (4), (5), (6), (7), and (8) in the example message, see the following:

IEEE 802.1X: `show dot1x logging` command

Web authentication: `show web-authentication logging` command

MAC-based authentication: `show mac-authentication logging` command

Impact on communication

None

Response messages

Table 25-4 List of response messages for the show authentication logging command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no logging data.	There is no log data.
There is no log data to match.	Log data matching the specified character string could not be found.
There is no memory.	There is not enough memory to collect data.

Notes

If you execute this command with the `search` parameter set and if information that matches the specified character string exists, the number of matched operation log messages is displayed at the end.

Example: 3 events matched.

clear authentication logging

Clears the operation log information for each type of Layer 2 authentication.

Syntax

```
clear authentication logging
```

Input mode

Administrator mode

Parameters

None

Example

The following shows an example of clearing operation log information for Layer 2 authentication.

```
# clear authentication logging

#
```

Display items

None

Impact on communication

None

Response messages

Table 25-5 List of response messages for the clear authentication logging command

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

Notes

None

26. IEEE 802.1X

show dot1x statistics
show dot1x
clear dot1x statistics
clear dot1x auth-state
reauthenticate dot1x
show dot1x logging
clear dot1x logging

show dot1x statistics

Displays statistics about IEEE 802.1X authentication.

Syntax

```
show dot1x statistics [{port <Port# list> | channel-group-number <Channel group# list>}]
```

Input mode

User mode and administrator mode

Parameters

{port *<Port# list>* | channel-group-number *<Channel group# list>*}

port *<Port# list>*

Displays statistics for the 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*.

channel-group-number *<Channel group# list>*

Displays statistics for the channel groups specified in list format. For details about how to specify *<Channel group# list>*, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Statistics for all the above types are displayed.

Example

Figure 26-1 Displaying the statistics for each port that uses IEEE 802.1X port-based authentication (static)

```
> show dot1x statistics port 0/1

Date 2010/09/01 00:53:41 UTC
[EAPOL frames]
Port 0/1   TxTotal   :        11 TxReq/Id  :         5 TxReq     :         2
           TxSuccess :         2 TxFailure :         2 TxNotify  :         0
           RxTotal   :         7 RxStart   :         3 RxLogoff  :         0
           RxResp/Id :         2 RxResp    :         2 RxInvalid :         0
           RxLenErr  :         0

[EAPoverRADIUS frames]
Port 0/1   TxTotal   :         4 TxNakResp :         0 TxNoNakRsp:         4
           RxTotal   :         4 RxAccAccpt:         2 RxAccRejct:         0
           RxAccChllg:         2 RxInvalid :         0

>
```

Figure 26-2 Displaying the statistics for each port that uses IEEE 802.1X port-based authentication (dynamic)

```
> show dot1x statistics port 0/4

Date 2010/09/01 00:53:47 UTC
[EAPOL frames]
Port 0/4   TxTotal   :         6 TxReq/Id  :         4 TxReq     :         0
(Dynamic)  TxSuccess :         0 TxFailure :         2 TxNotify  :         0
           RxTotal   :        10 RxStart   :         6 RxLogoff  :         0
           RxResp/Id :         4 RxResp    :         0 RxInvalid :         0
           RxLenErr  :         0
```

```
[EAPoverRADIUS frames]
Port 0/4   TxTotal   :         4 TxNakResp :         0 TxNoNakRsp:         4
(Dynamic)  RxTotal   :         0 RxAccAccpt:         0 RxAccRejct:         0
           RxAccChllg:         0 RxInvalid :         0

>
```

Figure 26-3 Displaying the statistics for each channel that uses IEEE 802.1X port-based authentication (static)

```
> show dot1x statistics channel-group-number 1

Date 2010/09/01 00:53:52 UTC
[EAPOL frames]
ChGr 1     TxTotal   :         7 TxReq/Id  :         4 TxReq     :         1
           TxSuccess :         1 TxFailure :         1 TxNotify  :         0
           RxTotal   :         4 RxStart   :         2 RxLogoff  :         0
           RxResp/Id :         1 RxResp    :         1 RxInvalid :         0
           RxLenErr  :         0

[EAPoverRADIUS frames]
ChGr 1     TxTotal   :         2 TxNakResp :         0 TxNoNakRsp:         2
           RxTotal   :         2 RxAccAccpt:         1 RxAccRejct:         0
           RxAccChllg:         1 RxInvalid :         0

>
```

Figure 26-4 Displaying the statistics for each channel group that uses IEEE 802.1X port-based authentication (dynamic)

```
> show dot1x statistics channel-group-number 64

Date 2010/09/01 00:53:56 UTC
[EAPOL frames]
ChGr 64    TxTotal   :        10 TxReq/Id  :         3 TxReq     :         3
(Dynamic)  TxSuccess :         3 TxFailure :         1 TxNotify  :         0
           RxTotal   :        10 RxStart   :         3 RxLogoff  :         1
           RxResp/Id :         3 RxResp    :         3 RxInvalid :         0
           RxLenErr  :         0

[EAPoverRADIUS frames]
ChGr 64    TxTotal   :         6 TxNakResp :         0 TxNoNakRsp:         6
(Dynamic)  RxTotal   :         6 RxAccAccpt:         3 RxAccRejct:         0
           RxAccChllg:         3 RxInvalid :         0

>
```

Figure 26-5 Displaying the statistics for all types of IEEE 802.1X authentication

```
> show dot1x statistics

Date 2010/09/01 00:53:29 UTC
[EAPOL frames]
Port 0/1   TxTotal   :        11 TxReq/Id  :         5 TxReq     :         2
           TxSuccess :         2 TxFailure :         2 TxNotify  :         0
           RxTotal   :         7 RxStart   :         3 RxLogoff  :         0
           RxResp/Id :         2 RxResp    :         2 RxInvalid :         0
           RxLenErr  :         0
Port 0/4   TxTotal   :         6 TxReq/Id  :         4 TxReq     :         0
(Dynamic)  TxSuccess :         0 TxFailure :         2 TxNotify  :         0
           RxTotal   :        10 RxStart   :         6 RxLogoff  :         0
           RxResp/Id :         4 RxResp    :         0 RxInvalid :         0
           RxLenErr  :         0
ChGr 1     TxTotal   :         7 TxReq/Id  :         4 TxReq     :         1
           TxSuccess :         1 TxFailure :         1 TxNotify  :         0
           RxTotal   :         4 RxStart   :         2 RxLogoff  :         0
```

```
            RxResp/Id :         1 RxResp    :         1 RxInvalid :         0
            RxLenErr  :         0
ChGr 64     TxTotal   :        10 TxReq/Id  :         3 TxReq     :         3
(Dynamic)   TxSuccess :         3 TxFailure :         1 TxNotify  :         0
            RxTotal   :        10 RxStart   :         3 RxLogoff  :         1
            RxResp/Id :         3 RxResp    :         3 RxInvalid :         0
            RxLenErr  :         0

[EAPoverRADIUS frames]
Port 0/1    TxTotal   :         4 TxNakResp :         0 TxNoNakRsp:         4
            RxTotal   :         4 RxAccAccpt:         2 RxAccRejct:         0
            RxAccChllg:         2 RxInvalid :         0
Port 0/4    TxTotal   :         4 TxNakResp :         0 TxNoNakRsp:         4
(Dynamic)   RxTotal   :         0 RxAccAccpt:         0 RxAccRejct:         0
            RxAccChllg:         0 RxInvalid :         0
ChGr 1      TxTotal   :         2 TxNakResp :         0 TxNoNakRsp:         2
            RxTotal   :         2 RxAccAccpt:         1 RxAccRejct:         0
            RxAccChllg:         1 RxInvalid :         0
ChGr 64     TxTotal   :         6 TxNakResp :         0 TxNoNakRsp:         6
(Dynamic)   RxTotal   :         6 RxAccAccpt:         3 RxAccRejct:         0
            RxAccChllg:         3 RxInvalid :         0

>
```

Display items

Table 26-1 Display items for statistics concerning IEEE 802.1X authentication

Item	Meaning
Port/ChGr/VLAN(Dynamic)	Indicates the type of authentication. `Port` *<IF#>*: Indicates port-based authentication (static). `Port` *<IF#>*`(Dynamic)`: Indicates port-based authentication (dynamic). `ChGr` *<Channel Group number>*: Indicates the channel group for port-based authentication (static). `ChGr` *<Channel Group number>*`(dynamic)`: Indicates the channel group for port-based authentication.
[EAPOL frames]	Statistics for EAPOL frames. For details about the items, see the following.
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 Identify 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

Item	Meaning
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 frames) that have been received
RxInvalid	The number of invalid EAPOL frames that have been received (the number of discarded frames)#
RxLenErr	The number of invalid-length EAPOL frames that have been received (the number of discarded frames)
[EAPoverRADIUS frames]	Statistics for EAPoverRADIUS frames. For details about the items, see the following.
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

#: If an EAPoL frame with a tag is received and discarded, it is not counted for the number of discarded frames.

Impact on communication

None

Response messages

Table 26-2 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.

Message	Description
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.

Notes

None

show dot1x

Displays status information about IEEE 802.1X authentication.

Syntax

```
show dot1x [{port <Port# list> | channel-group-number <Channel group# list>}] [detail]
```

Input mode

User mode and administrator mode

Parameters

{port *<Port# list>* | channel-group-number *<Channel group# list>* }

port *<Port# list>*

Displays status information 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*.

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*.

detail

Displays detailed information. The status information about each supplicant (user) that has already been authenticated is displayed.

Operation when all parameters are omitted:

The status information for the entire switch is displayed.

Example

Figure 26-6 Displaying the status information for the IEEE 802.1X switch (summary display)

```
> show dot1x

Date 2012/11/30 17:05:03 UTC
System 802.1X : Enable
   AAA Authentication Dot1x   : Enable
       Accounting Dot1x       : Enable
                  Auto-logout  : Enable

Authentication Default     : RADIUS
Authentication dot1x_auth1 : RADIUS dot1x_auth1
Accounting Default         : RADIUS

Port/ChGr          AccessControl  PortControl        Status        Supplicants
Port 0/4           Multiple-Auth  Auto               ---           1
Port 0/5           Multiple-Auth  Auto               ---           0
Port 0/36(Dynamic) Multiple-Auth  Auto               ---           0
ChGr 64            Multiple-Auth  Auto               ---           0

>
```

Figure 26-7 Displaying the status information for all types of IEEE 802.1X authentication

```
> show dot1x detail

Date 2012/11/30 17:06:48 UTC
System 802.1X : Enable
```

```
   AAA Authentication Dot1x   : Enable
       Accounting Dot1x       : Enable
                  Auto-logout  : Enable

Authentication Default     : RADIUS
Authentication dot1x_auth1 : RADIUS dot1x_auth1
Accounting Default         : RADIUS

Port 0/4
AccessControl  : Multiple-Auth            PortControl   : Auto
Status         : ---                      Last EAPOL    : 000a.e460.af39
Supplicants    : 1 / 1 / 1024             ReAuthMode    : Enable
TxTimer        : 300                      ReAuthTimer   : 300
ReAuthSuccess  : 1                        ReAuthFail    : 0
SuppDetection  : Auto
VLAN(s): 200

 Supplicants MAC  F  Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time                   SubState     Class
 [VLAN 200]          Port(Static)  Supplicants : 1
 000a.e460.af39      Authorized     Authenticated  Idle           1
                     192           2012/11/30 17:03:36          Full            30

Port 0/5
AccessControl  : Multiple-Auth            PortControl   : Auto
Status         : ---                      Last EAPOL    : ----.----.----
Supplicants    : 0 / 0 / 1024             ReAuthMode    : Disable
TxTimer        : 1800                     ReAuthTimer   : 3600
ReAuthSuccess  : 0                        ReAuthFail    : 0
SuppDetection  : Shortcut

Port 0/36 (Dynamic)
AccessControl  : Multiple-Auth            PortControl   : Auto
Status         : ---                      Last EAPOL    : ----.----.----
Supplicants    : 0 / 0 / 1024             ReAuthMode    : Enable
TxTimer        : 30                       ReAuthTimer   : 10
ReAuthSuccess  : 0                        ReAuthFail    : 0
SuppDetection  : Auto

ChGr 64
AccessControl  : Multiple-Auth            PortControl   : Auto
Status         : ---                      Last EAPOL    : ----.----.----
Supplicants    : 0 / 0 / 1024             ReAuthMode    : Enable
TxTimer        : 30                       ReAuthTimer   : 3600
ReAuthSuccess  : 0                        ReAuthFail    : 0
SuppDetection  : Auto

>
```

Figure 26-8 Displaying the status information for each port that uses IEEE 802.1X port-based authentication (static) (no display type is specified)

```
> show dot1x port 0/4

Date 2012/11/30 17:08:32 UTC
Port 0/4
AccessControl  : Multiple-Auth            PortControl   : Auto
Status         : ---                      Last EAPOL    : 000a.e460.af39
Supplicants    : 1 / 1 / 1024             ReAuthMode    : Enable
TxTimer        : 300                      ReAuthTimer   : 300
ReAuthSuccess  : 1                        ReAuthFail    : 0
SuppDetection  : Auto
VLAN(s): 200
```

```
Port(Static)  Supplicants
VLAN 200  1

>
```

Figure 26-9 Displaying the status information for each port that uses IEEE 802.1X port-based authentication (static) (detail display)

```
> show dot1x port 0/4 detail

Date 2012/11/30 17:10:21 UTC
Port 0/4
AccessControl  : Multiple-Auth            PortControl   : Auto
Status         : ---                      Last EAPOL    : 000a.e460.af39
Supplicants    : 1 / 1 / 1024             ReAuthMode    : Enable
TxTimer        : 300                      ReAuthTimer   : 300
ReAuthSuccess  : 1                        ReAuthFail    : 0
SuppDetection  : Auto
VLAN(s): 200

 Supplicants MAC  F  Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time                   SubState     Class
 [VLAN 200]          Port(Static)  Supplicants : 1
 000a.e460.af39      Authorized     Authenticated  Idle           1
                     192           2012/11/30 17:03:36          Full           30

>
```

Display items

Table 26-3 Display items for the status information about IEEE 802.1X authentication

Item		Meaning	Displayed detailed information
System 802.1X		Displays the operating status of IEEE 802.1X authentication.	`Enabled`: Running `Disable`: Disabled
AAA	Authentication Dot1x	Displays the operating status of authentication requests to RADIUS.	`Enable`: Enabled `Disable`: Disabled
	Accounting Dot1x	Displays the operating status of the accounting functionality.	`Enable`: Enabled `Disable`: Disabled
Auto-logout		Displays the operating status of automatic cancellation of authentication when non-communication monitoring is used.	`Enable`: Enabled `Disable`: Disabled
Authentication Default		Displays the default authentication method for the device. This item is not displayed if it is not set.	`RADIUS`: Indicates RADIUS authentication
Authentication *<List name>*		Displays the list name and authentication method for the authentication method list. This item is not displayed if it is not set.	`RADIUS` *<Group name>*: RADIUS server group name `RADIUS` *<Group name>*`(Not defined)`: The RADIUS server group name is invalid.
Accounting Default		Displays the accounting server setting. This item is not displayed if it is not set.	`RADIUS`: General-use RADIUS server or RADIUS server dedicated to IEEE 802.1X authentication

Item	Meaning	Displayed detailed information
Port/ChGr	Indicates the type of authentication. `Port` *<IF#>*: Port-based authentication (static) port `Port` *<IF#>*`(Dynamic)`: Port-based authentication (dynamic) port `ChGr` *<Channel Group number>*: The channel group for port-based authentication (static) `ChGr` *<Channel Group number>*`(Dynamic)`: The channel group for port-based authentication (dynamic)	
AccessControl	Displays the authentication submode set for the relevant type of authentication.	`---`: Indicates single mode. `Multiple-Auth`: Indicates terminal authentication mode.
PortControl	Displays the authentication control setting.	`Auto`: Authentication control is applied. `Force-Authorized`: Communication is always authorized. `Force-Unauthorized`: Communication is never authorized.
Status	Displays the authentication status of the port.	`Authorized`: Already authenticated. `Unauthorized`: Not authenticated. `---`: Terminal authentication mode
Last EAPOL	Displays the source MAC address of the last received EAPOL. `----.----.----` is displayed when authentication has not been completed.	
Supplicants (summary display)	Displays the number of supplicants that have already been authenticated or assigned for authentication. The number of supplicants to be authenticated is displayed.	
Supplicants (display except for summary)	Displays the number of supplicants that have already been authenticated or assigned for authentication. Single mode: *<number of authenticated supplicants> / <number of supplicants to be authenticated>* For terminal authentication mode: *<number of authenticated supplicants> / <number of supplicants to be authenticated> / <maximum number of supplicants within an authentication type>*	
ReAuthMode	Displays the status of the self-issuance of EAPOL Request/ID re-authentication requests.	`Enable`: Enabled `Disable`: Disabled
TxTimer	Displays the interval for sending authentication requests EAPOL Request/ID prior to authentication. *<tx_period in seconds>*	
ReAuthTimer	Displays the interval for sending EAPOL Request/ID re-authentication requests after a successful authentication. *<reauth_period in seconds>*	

Item	Meaning	Displayed detailed information
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 unauthenticated status 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. *<keepunauth_period in seconds>*	
SuppDetection	(For terminal authentication mode only) This item displays the mode for detecting a new terminal.	`Disable`: The detection operation is stopped. `Shortcut`: Omission mode `Auto`: Automatic detection mode
Authentication	This item displays the name of the authentication method list for the port-based authentication method. This item is not displayed if it is not set.	*<List name>*: The name of the authentication method list *<List name>* `(Not defined)`: The name of the authentication method list is invalid.
VLAN(s)	This item displays the list of VLANs to be authenticated. Note that the list does not include VLANs registered by automatic VLAN assignment.	
Port(Dynamic)Supplicants	This item displays the number of supplicants already authenticated by dynamic VLAN assignment.	
Port(Static)Supplicants	This item displays the number of supplicants already authenticated by static VLAN assignment.	
Port(Unknown)Supplicants	This item displays the number of supplicants not yet authenticated.	
Supplicant MAC	The supplicant's MAC address.	
F	*: A terminal authenticated by the forced authentication functionality. When the authentication time is updated, a displayed asterisk (`*`) disappears if a request is sent to the RADIUS server and the RADIUS server accepts the request.	
Status	Displays the authentication status of the supplicants.	`Authorized`: Already authenticated. `Unauthorized`: Not authenticated.
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

Item	Meaning	Displayed detailed information
		processing has stopped. `Held`: The authentication request has been rejected.
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.
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 first time that authentication of the supplicant was successful.	
SubState	(For port-based authentication (static or dynamic) only) This item displays the authentication sub-status of the supplicant.	`Full`: Full access is permitted (when `AuthState` is `Authenticated`) `Protection`: Limited access is permitted (when `AuthState` is `Authenticated`) # In multistep authentication, even if the first step of terminal authentication succeeds and user authentication is being awaited in the second step, `Protection` is displayed. `---`: There is no sub-status because authentication has not been completed (`AuthState` is not `Authenticated`.)
Class	Displays the user class of the supplicant. A hyphen (`-`) is displayed for the first step of multistep authentication or restricted access permission.	

Impact on communication

None

Response messages

Table 26-4 List of response messages for the show dot1x command

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

Notes

None

clear dot1x statistics

Clears the IEEE 802.1X authentication statistics to zero.

Syntax

```
clear dot1x statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 26-10 Clearing IEEE 802.1X authentication statistics to zero

```
> clear dot1x statistics

>
```

Display items

None

Impact on communication

None

Response messages

Table 26-5 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.
Dot1x doesn't seem to be running.	The IEEE 802.1X setting has not been enabled. Check the configuration.

Notes

None

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> |
supplicant-mac <MAC>}][-f]
```

Input mode

User mode and administrator mode

Parameters

{port *<Port# list>* | channel-group-number *<Channel group# list>* | supplicant-mac *<MAC>*}

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*.

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*.

supplicant-mac *<MAC>*

Initializes the authentication status for the specified MAC address.

-f

Initializes the authentication status without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Operation when all parameters are omitted:

After confirmation message for initialization is displayed, all IEEE 802.1X authentication statuses are initialized.

Example

Figure 26-11 Initializing all IEEE 802.1X authentication statuses on a Switch

```
> clear dot1x auth-state
Do you wish to initialize all 802.1X authentication information? (y/n) : y

>
```

Display items

None

Impact on communication

If initialization is performed, the IEEE 802.1X authentication status on the relevant ports or VLANs is initialized, and communication is lost. To restore communication, re-authentication is necessary.

Response messages

Table 26-6 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.
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 authenticated user.	The specified unit of authentication exists, but there is no authenticated user registered.

Notes

When authentication status is initialized, EAP-Req/Id might be sent according to the specified parameter.

- If the parameter is omitted, EAP-Req/Id is multicasted once to all units of IEEE 802.1X authentication in the device.
- If the parameter is `port` <*Port# list*> or `channel-group-number` <*Channel group# list*>, EAP-Req/Id is multicasted once to the specified unit of IEEE 802.1X authentication.
- If the parameter is `supplicant-mac` <*MAC*>, and if there is no authentication terminal under the IEEE 802.1X authentication to which the specified authentication terminal belongs, EAP-Req/Id is multicasted once to the unit of IEEE 802.1X authentication to which the specified authentication terminal belongs.

reauthenticate dot1x

Re-authenticates the status of IEEE 802.1X authentication. Even if re-authentication timer (reauth-period) is 0 (disabled), re-authentication is forcibly performed.

Syntax

```
reauthenticate dot1x [{port <Port# list> | channel-group-number <Channel group# list>} |
supplicant-mac <MAC>}] [-f]
```

Input mode

User mode and administrator mode

Parameters

{port *<Port# list>* | channel-group-number *<Channel group# list>*} | supplicant-mac *<MAC>*}

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*.

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*.

supplicant-mac *<MAC>*

Re-authenticates the authentication status of the specified MAC address.

-f

Initiates re-authentication without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Operation when all parameters are omitted:

After a confirmation message for re-authentication is displayed, re-authenticates all the IEEE 802.1X authentication statuses.

Example

Figure 26-12 Re-authentication for all IEEE 802.1X-authenticated ports and VLANs on a Switch

```
> reauthenticate dot1x
Do you wish to reauthenticate all 802.1X ports and VLANs? (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 26-7 List of response messages for the reauthenticate dot1x command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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 authenticated user.	The specified unit of authentication exists, but there is no authenticated user registered.

Notes

None

show dot1x logging

Displays the operation log messages collected by IEEE 802.1X authentication.

Syntax

```
show dot1x logging [search <Search string>]
```

Input mode

User mode and administrator mode

Parameters

search *<Search string>*

Specifies the search string.

If you specify this parameter, only information that includes the search string will be displayed.

Specify the string with 1 to 64 characters. The characters are case sensitive.

Operation when this parameter is omitted:

Displays all the operation log messages output by IEEE 802.1X.

Example

Figure 26-13 Displaying IEEE 802.1X operation log messages

- When the parameter is omitted:

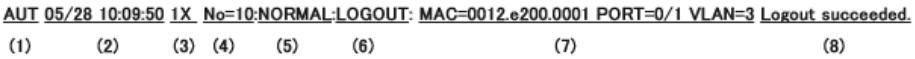
```
> show dot1x logging

Date 2010/09/01 01:00:38 UTC
AUT 09/01 00:53:12 1X  No=30:NOTICE:LOGIN: MAC=0013.20a5.3e4f PORT=0/4 Login
failed. ; RADIUS authentication failed.
AUT 09/01 00:52:02 1X  No=1:NORMAL:LOGIN: MAC=0013.20a5.3e50 CHGR=64 VLAN=40
Login succeeded. ; New Supplicant Auth Success.
AUT 09/01 00:51:49 1X  No=10:NORMAL:LOGOUT: MAC=0013.20a5.3e50 CHGR=64 VLAN=40
Logout succeeded.
AUT 09/01 00:51:36 1X  No=2:NORMAL:LOGIN: MAC=0013.20a5.3e50 CHGR=64 VLAN=40
Login succeeded. ; Supplicant Re-Auth Success.
AUT 09/01 00:45:57 1X  No=16:NORMAL:LOGOUT: MAC=0013.20a5.3e1a PORT=0/1 VLAN=4
Force logout. ; Port link down.
AUT 09/01 00:45:39 1X  No=1:NORMAL:LOGIN: MAC=0013.20a5.3e1a PORT=0/1 VLAN=4
Login succeeded. ; New Supplicant Auth Success.

>
```

- Specifying `LOGOUT` for the parameter:

```
> show dot1x logging search LOGOUT

Date 2010/09/01 01:01:07 UTC
AUT 09/01 00:51:49 1X  No=10:NORMAL:LOGOUT: MAC=0013.20a5.3e50 CHGR=64 VLAN=40
Logout succeeded.
AUT 09/01 00:45:57 1X  No=16:NORMAL:LOGOUT: MAC=0013.20a5.3e1a PORT=0/1 VLAN=4
Force logout. ; Port link down.

 2 events matched.

>
```

Display items

The following shows the display format of a message.



(1) Log functionality type: Indicates the type of authentication functionality. (Fixed at AUT.)

(2) Date and time: Indicates the date and time (*month*/*date* *hour*:*minute*:*second*) an event occurred.

(3) Authentication ID: Indicates IEEE 802.1X.

(4) Message number: Indicates the number assigned to each message shown in *Table 26-10 List of operation log messages*.

(5) Log ID: Indicates the level of the operation log message.

(6) Log type: Indicates the type of operation that outputs the log message.

(7) Additional information: Indicates supplementary information provided in the message.

(8) Message body

Operation log messages show the following information:

- Log ID and type: See *Table 26-8 Log ID and type in operation log messages*.
- Additional information: See *Table 26-9 Additional information*.
- List of messages: See *Table 26-10 List of operation log messages*.

Table 26-8 Log ID and type in operation log messages

Log ID	Log type	Description
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 the attempt to cancel authentication failed.
WARNING	SYSTEM	Indicates an alternate operation when a communication failure occurs.
ERROR	SYSTEM	Indicates that a communication or operation failure of the IEEE 802.1X functionality occurred.

Table 26-9 Additional information

Display format	Meaning
MAC=*xxxx*.*xxxx*.*xxxx*	Indicates the MAC address.

Display format	Meaning
PORT=*xx/xx* CHGR=*x*	Indicates the port number or channel group number
VLAN=*xx*	Indicates the VLAN ID.
ServerIP=*xxx.xxx.xxx*	Indicates the server IP address.
ServerIPv6=*xxx.xxx.xxx*	Indicates the server IPv6 address.

Table 26-10 List of operation log messages

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
1	NORMAL	LOGIN	Login succeeded. ; New Supplicant Auth Success.
	Port-based authentication (static) Port-based authentication (dynamic)		A new supplicant was authenticated successfully. [Action] None
			MAC, PORT or CHGR, VLAN ID#
2	NORMAL	LOGIN	Login succeeded. ; Supplicant Re-Auth Success.
	Port-based authentication (static) Port-based authentication (dynamic)		A supplicant was re-authenticated successfully. [Action] None
			MAC, PORT or CHGR, VLAN ID#
3	NORMAL	LOGIN	Login succeeded. ; Limited by ACL.
	Port-based authentication (static)		A supplicant was authenticated, but a pre-authentication filter is enabled. [Action] Clear the quarantine conditions.
			MAC, PORT or CHGR, VLAN ID
10	NORMAL	LOGOUT	Logout succeeded.
	Port-based authentication (static) Port-based		Authentication has been canceled by a request from the supplicant or because the terminal was moved. [Action] None

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
	authentication (dynamic)		MAC, PORT or CHGR, VLAN ID#
11	NORMAL	LOGOUT	Force logout. ; "clear dot1x auth-state" command succeeded.
	Port-based authentication (static) Port-based authentication (dynamic)		Authentication has been canceled by a command. [Action] None
			MAC, PORT or CHGR, VLAN ID#
12	NORMAL	LOGOUT	Force logout. ; The supplicant was cleared, because it was registered to MAC VLAN with the configuration.
	Port-based authentication (dynamic)		An attempt to authenticate the relevant suppliant was canceled because a MAC address was configured for the MAC VLAN. [Action] None
			MAC, PORT or CHGR, VLAN ID#
13	NORMAL	LOGOUT	Force logout. ; The supplicant was cleared, because it was registered to mac-address-table with the configuration.
	Port-based authentication (static) Port-based authentication (dynamic)		An attempt to authenticate the relevant suppliant was canceled because a MAC address was configured for the MAC address table. [Action] None
			MAC, PORT or CHGR, VLAN ID#
14	NORMAL	LOGOUT	Force logout. ; The status of port was changed to Unauthorized, because another supplicant was detection in single mode.
	Port-based authentication (static) Port-based authentication (dynamic)		The authentication status has been changed to Unauthorized because multiple supplicants were detected on a single-mode port. [Action] None
			MAC, PORT or CHGR, VLAN ID#

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
15	NORMAL	LOGOUT	Force logout. ; Dot1x configuration deleted.
	Port-based authentication (static) Port-based authentication (dynamic)		Authentication has been canceled because the IEEE 802.1X authentication configuration was deleted. [Action] If you want to use IEEE 802.1X authentication, configure it.
			MAC, PORT or CHGR, VLAN ID#
16	NORMAL	LOGOUT	Force logout. ; Port link down.
	Port-based authentication (static) Port-based authentication (dynamic)		Authentication has been canceled because the port is in the link-down state. [Action] None
			MAC, PORT or CHGR, VLAN ID#
17	NORMAL	LOGOUT	Force logout. ; VLAN status down.
	Port-based authentication (static) Port-based authentication (dynamic)		Authentication has been canceled because the VLAN has gone down. [Action] None
			MAC, PORT or CHGR, VLAN ID#
18	NORMAL	LOGOUT	Force logout. ; Re-Auth failed.
	Port-based authentication (static) Port-based authentication (dynamic)		Re-authentication processing failed. [Action] None
			MAC, PORT or CHGR, VLAN ID#
30	NOTICE	LOGIN	Login failed. ; RADIUS authentication failed.
	Port-based authentication (static) Port-based authentication (dynamic)		Authentication of a new supplicant failed. [Action] Correctly set the user ID and password to be sent from the supplicant and the user settings on the RADIUS server.
			MAC, PORT or CHGR, VLAN ID#

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
31	NOTICE	LOGIN	Login failed. ; RADIUS authentication failed. (Re-Auth)
	Port-based authentication (static) Port-based authentication (dynamic)		Re-authentication of a supplicant failed. This log is collected due to no response from a terminal or a RADIUS authentication failure. (Up to version 3.0) Re-authentication of a supplicant failed. This log is collected due to RADIUS authentication failure. (Ver. 3.1 or later) [Action] Correctly set the user ID and password to be sent from the supplicant and the user settings on the RADIUS server.
			MAC, PORT or CHGR, VLAN ID[#]
33	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: No Tunnel-Type Attribute.)
	Port-based authentication (dynamic)		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, PORT or CHGR
34	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Tunnel-Type Attribute is not VLAN(13).)
	Port-based authentication (dynamic)		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, PORT or CHGR
35	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: No Tunnel-Medium-Type Attribute.)
	Port-based authentication (dynamic)		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, PORT or CHGR

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
36	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Tunnel-Medium-Type Attribute is not IEEE 802(6).)
	Port-based authentication (dynamic)		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, PORT or CHGR
38	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Invalid Tunnel-Private-Group-ID Attribute.)
	Port-based authentication (dynamic)		VLAN dynamic assignment has 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, PORT or CHGR
39	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The VLAN ID is out of range.)
	Port-based authentication (dynamic)		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, PORT or CHGR, VLAN ID#
40	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The Port doesn't belong to VLAN.)
	Port-based authentication (dynamic)		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 vlan` configuration command.
			MAC, PORT or CHGR, VLAN ID#

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
42	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The VLAN status is disabled.)
	Port-based authentication (static) Port-based authentication (dynamic)		VLAN dynamic assignment failed because the VLAN was disabled. [Action] Execute the `state` configuration command to set the status of the VLAN to be assigned to `active`.
			MAC, PORT or CHGR, VLAN ID#
43	NOTICE	LOGIN	Login failed. ; The number of supplicants on the switch is full.
	Port-based authentication (static) Port-based authentication (dynamic)		Authentication was not available because there were too many supplicants for the Switch. [Action] Attempt authentication again when the total number of authenticated supplicants is below the capacity limit.
			MAC, PORT or CHGR, VLAN ID#
45	NOTICE	LOGIN	Login failed. ; Failed to authenticate the supplicant because it could not be registered to mac-address-table.
	Port-based authentication (static) Port-based authentication (dynamic)		Authentication failed because registration of a supplicant in the MAC address table failed. [Action] Attempt authentication again when the total number of current authentications, including those of other authentication types, is below the capacity limit.
			MAC, PORT or CHGR, VLAN ID#
46	NOTICE	LOGIN	Login failed. ; Failed to authenticate the supplicant because it could not be registered to MAC VLAN.
	Port-based authentication (dynamic)		Authentication failed because the registration of a supplicant in the MAC VLAN failed. [Action] Attempt authentication again when the total number of current authentications, including those of other authentication types, is below the capacity limit.
			MAC, PORT or CHGR, VLAN ID#

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
47	NOTICE	LOGIN	Login failed. ; Failed to connect to RADIUS server.
	Port-based authentication (static) Port-based authentication (dynamic)		Authentication failed because an attempt to connect to the RADIUS server failed. [Action] Confirm the following: ● The RADIUS server functionality is enabled. ● Communication between the Switch and the RADIUS server is available.
			MAC, PORT or CHGR, VLAN ID#
80	WARNING	SYSTEM	Invalid EAPOL frame received.
	Port-based authentication (static) Port-based authentication (dynamic)		An invalid EAPOL frame has been received. [Action] Check whether there is any problems with the following: ● The contents of EAPOL frames sent by the supplicant ● Transmission line quality
			--
81	WARNING	SYSTEM	Invalid EAP over RADIUS frame received.
	Port-based authentication (static) Port-based authentication (dynamic)		An invalid EAPoverRADIUS frame has been received. [Action] Check whether there is any problems with the following: ● The contents of packets sent by the RADIUS server ● Transmission line quality
			--
82	WARNING	SYSTEM	Failed to connect to RADIUS server.
	Port-based authentication (static) Port-based authentication (dynamic)		An attempt to connect to the RADIUS server failed. [Action] Confirm the following: ● Communication between the Switch and the RADIUS server is available. ● The RADIUS server functionality is enabled.
			ServerIP

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
83	WARNING	SYSTEM	Failed to connect to RADIUS server.
	Port-based authentication (static) Port-based authentication (dynamic)		An attempt to connect to the RADIUS server failed. [Action] Confirm the following: ● The RADIUS server functionality is enabled. ● Communication between the Switch and the RADIUS server is available.
			ServerIPv6
84	WARNING	SYSTEM	Failed to connect to Accounting server.
	Port-based authentication (static) Port-based authentication (dynamic)		An attempt to connect to the accounting server failed. [Action] Confirm the following: ● The accounting server functionality is enabled. ● Communication between the Switch and the accounting server is available.
			ServerIP
85	WARNING	SYSTEM	Failed to connect to Accounting server.
	Port-based authentication (static) Port-based authentication (dynamic)		An attempt to connect to the accounting server failed. [Action] Confirm the following: ● The accounting server functionality is enabled. ● Communication between the Switch and the accounting server is available.
			ServerIPv6
301	NORMAL	LOGIN	New Supplicant force-Authorized.
	Port-based authentication (static) Port-based authentication (dynamic)		The client initiated forced authentication because of a failure between RADIUS servers. [Action] None
			MAC, PORT or CHGR, VLAN ID#

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
310	NORMAL	LOGOUT	Force logout. ; The supplicant was cleared, because auto-logout.
	Port-based authentication (static) Port-based authentication (dynamic)		Authentication of the supplicant has been canceled because a timeout was detected by non-communication monitoring. [Action] None
			MAC, PORT or CHGR, VLAN ID#
311	NORMAL	LOGOUT	Force logout. ; Multi-step finished.
	Port-based authentication (static) Port-based authentication (dynamic)		Authentication has been canceled because multistep authentication either succeeded or failed. [Action] None
			MAC, PORT or CHGR, VLAN ID#
330	NOTICE	LOGIN	Login failed. ; Failed to authenticate the supplicant because MAC authentication reject.
	Port-based authentication (static) Port-based authentication (dynamic)		Authentication was not performed because MAC-based authentication failed in multistep authentication. [Action] Set the MAC address to the RADIUS server.
			MAC, PORT or CHGR, VLAN ID#
332	NOTICE	LOGIN	Login failed. ; Failed to authenticate the supplicant because it is already registered by other method.
	Port-based authentication (static) Port-based authentication (dynamic)		Authentication failed because the terminal had already been registered for another type of authentication. [Action] To register in IEEE 802.1X authentication, cancel registration of the other authentication mode, and then attempt authentication again.
			MAC, PORT or CHGR, VLAN ID#

No.	Log ID	Log type	Message text
	Authentication mode		Description
			Additional information
380	WARNING	SYSTEM	Invalid user class. [Class]
	Port-based authentication (static) Port-based authentication (dynamic)		The user class set for the RADIUS server is invalid. [Action] Review the RADIUS server setting.
			--

#: For port-based authentication (dynamic), the VLAN ID might not be displayed until the VLAN to be accommodated has been decided.

Impact on communication

None

Response messages

Table 26-11 List of response messages for the show dot1x logging command

Message	Description
There is no logging data.	There is no log data.
There is no log data to match.	Log data matching the specified character string could not be found.
There is no memory.	There is not enough memory to collect data.

Notes

If you execute this command with the `search` parameter set and if information that matches the specified character string exists, the number of matched operation log messages is displayed at the end.

Example: 3 events matched.

clear dot1x logging

Clears the operation log messages collected by IEEE 802.1X authentication.

Syntax

```
clear dot1x logging
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 26-14 Clearing IEEE 802.1X operation log messages

```
> clear dot1x logging

>
```

Display items

None

Impact on communication

None

Response messages

Table 26-12 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.

Notes

None

27. Web Authentication

set web-authentication user
set web-authentication passwd
set web-authentication vlan
remove web-authentication user
show web-authentication user
show web-authentication login
show web-authentication login select-option
show web-authentication login summary
show web-authentication logging
clear web-authentication logging
show web-authentication
show web-authentication statistics
clear web-authentication statistics
commit web-authentication
store web-authentication
load web-authentication
clear web-authentication auth-state
set web-authentication html-files
store web-authentication html-files
show web-authentication html-files
clear web-authentication html-files
show web-authentication redirect target

For details such as a description of the authentication modes, see the *Configuration Guide Vol. 2*.

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 <Web auth user name> <Password> <VLAN ID>
```

Input mode

Administrator mode

Parameters

<Web auth user name>

Specify a user name to be registered.

Specify 1 to 128 characters. You can use alphanumeric characters (case sensitive), at marks (`@`), hyphens (`-`), underscores (`_`), and periods (`.`).

<Password>

Specify a password.

Specify 1 to 32 characters. You can use alphanumeric characters (case sensitive), at marks (`@`), hyphens (`-`), underscores (`_`), and periods (`.`).

<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 dynamic VLAN mode is used:

  Specify the VLAN ID of the VLAN to which the user will move after authentication.

- When fixed VLAN mode is used

  Specify the VLAN ID of the VLAN to which the user requesting authentication belongs.

Example

Adding `USER01` as the user name, `123456abcde` as the password, and `4094` as the VLAN ID:

```
# set web-authentication user USER01 123456abcde 4094

#
```

Display items

None

Impact on communication

None

Response messages

Table 27-1 List of response messages for the set web-authentication user command

Message	Description
Already user '*<Web auth user name>*' exists.	The specified user has already been registered.
The number of users exceeds 300.	The number of users to be registered exceeds 300.
Web-Authentication is not configured.	The Web authentication functionality 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 <Web auth user name> <Old password> <New password>
```

Input mode

Administrator mode

Parameters

<Web auth user name>

Specify the name of the user whose password is to be changed.

<Old password>

Specify the current password.

<New password>

Specify the new password.

Specify 1 to 32 characters. You can use alphanumeric characters (case sensitive), at marks (`@`), hyphens (`-`), underscores (`_`), and periods (`.`).

Example

Changing the password for user `USER01`:

```
# set web-authentication passwd USER01 123456abcde 456789abcde

#
```

Display items

None

Impact on communication

None

Response messages

Table 27-2 List of response messages for the set web-authentication passwd command

Message	Description
The old-password is different.	The old password for the specified user is incorrect.
Unknown user '*<Web auth user name>*'.	The specified user has not been registered.
Web-Authentication is not configured.	The Web authentication functionality 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 <Web auth user name> <VLAN ID>
```

Input mode

Administrator mode

Parameters

<Web auth user name>

Specify the name of the user for which the VLAN is being changed.

<VLAN ID>

Specify the VLAN that is to be changed. For *<VLAN ID>*, specify the VLAN ID set by the `interface vlan` command.

For details about the specifiable range of values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

Example

Changing the VLAN to which user `USER01` belongs to `2`:

```
# set web-authentication vlan USER01 2

#
```

Display items

None

Impact on communication

None

Response messages

Table 27-3 List of response messages for the set web-authentication vlan command

Message	Description
Unknown user '*<Web auth user name>*'.	The specified user has not been registered.
Web-Authentication is not configured.	The Web authentication functionality 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 {<Web auth user name> | -all} [-f]
```

Input mode

Administrator mode

Parameters

{*<Web auth user name>* | -all}

<Web auth user name>

Deletes the specified user.

-all

Deletes all users.

-f

Deletes the user without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

- When deleting the user `USER01`:

```
# remove web-authentication user USER01
Remove web-authentication user.  Are you sure? (y/n): y


#
```

- When deleting 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 27-4 List of response messages for the remove web-authentication user command

Message	Description
Unknown user '<*Web auth user name*>'.	The specified user has not been registered. (when a single MAC address is specified)
User does not exist.	The user was not found (when `-all` is specified)
Web-Authentication is not configured.	The Web authentication functionality 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 the user information registered on the Switch 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` command
- `set web-authentication passwd` command
- `set web-authentication Vlan` command
- `remove web-authentication user` command

User information is displayed in ascending order of user name.

Syntax

```
show web-authentication user {edit | commit}
```

Input mode

Administrator mode

Parameters

{edit | commit}

edit

Displays user information being edited.

commit

Displays operating user information.

Example

- When displaying the user information being edited:

```
# show web-authentication user edit

Date 2010/09/19 07:26:27 UTC
 Total user counts: 4
 No  VLAN User name
 1    999 123
 2   4094 USER02-honsha_floor10-test1@example.com
 3    200 admin
 4    100 operator

#
```

Display items

Table 27-5 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

Item	Meaning	Displayed detailed information
No	Entry number	--
VLAN	VLAN	The VLAN set for the registered user
User name	user name	A registered user name

Impact on communication

None

Response messages

Table 27-6 List of response messages for the show web-authentication user command

Message	Description
There is no information. (edit)	There was no information in the edit area of the internal Web authentication DB.
There is no information. (commit)	There was no information in the commit area of the internal Web authentication DB.
Web-Authentication is not configured.	The Web authentication functionality 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 login date and time.

Syntax

```
show web-authentication login
```

Input mode

Administrator mode

Parameters

None

Example

```
# show web-authentication login

Date 2012/12/03 09:40:10 UTC
 Dynamic VLAN mode total login counts(Login/Max):   1 / 1000
  Authenticating client counts :    0
  Port roaming : Enable
   No F User name                Port  VLAN Class Login time          Limit
    1   web1000                  0/13  1000    24 2012/12/03 09:39:24 infinity

 Static VLAN mode total login counts(Login/Max):    1 / 1024
  Authenticating client counts :    0
  Port roaming : Enable
   No F User name                Port  VLAN Class Login time          Limit
    1   web024                   0/9    200    24 2012/12/03 09:37:43 infinity

#
```

Display items

Table 27-7 Information displayed for logged-in users

Item	Meaning	Displayed detailed information
Dynamic VLAN mode total login counts	The number of users currently logged in	`(Login / Max)`: The number of users currently logged in / the maximum number of users set for the device If a maximum number of registered users has not been set, the default value is displayed.
Static VLAN mode total login counts		
Authenticating client counts	The number of terminals on which authentication is being processed	--
Port roaming	Roaming information	Changing of ports within the same VLAN. `Enable`: Enabled `Disable`: Disabled (default)
No	Entry number	The entry number for an authenticated, currently logged-in user. This is just the displayed number, which changes

Item	Meaning	Displayed detailed information
		depending on such factors as the filter conditions.
F	Forced authentication indication	*: Indicates a user logged in by using the forced authentication functionality. When the authentication time is updated, a displayed asterisk (*) disappears if a request is sent to the RADIUS server and the RADIUS server accepts the request.
User name	User name	The name of the authenticated, currently logged-in user. Up to 23 characters are displayed. (If the name exceeds 23 characters, part of the name is replaced with three periods (...).) If the authentication method by user ID is enabled, the user name is displayed without *@authentication-method-list-name*. If the user is being switched by the user switching option functionality, the user name before the switch is displayed.
Port	Port number or channel group number	The port number or channel group number at the time the authenticated, currently logged-in user logged in (CH: xx)
VLAN	VLAN	The VLAN ID of the VLAN that is accommodating the authenticated, currently logged-in user
Class	User class	The user class is displayed.
Login time	Login date and time	The first time the authenticated, currently logged-in user logged in *year*/*month*/*day hour*:*minute*:*second*
Limit	Remaining login time	The remaining login time (*hours*:*minutes*:*seconds*) for the currently logged-in user. 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 set to unlimited: infinity

Impact on communication

None

Response messages

Table 27-8 List of response messages for the show web-authentication login command

Message	Description
There is no information. (web-auth login user)	Information for a Web authentication login user was not found.

Message	Description
Web-Authentication is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

None

show web-authentication login select-option

Extracts a portion of the authenticated users currently logged in based on selected items and displays those users in ascending order by login date and time.

If you execute the command with the `detail` option specified, the entries being authenticated are also displayed as the entries to be extracted.

Syntax

```
show web-authentication login select-option [mode {dynamic | static}]
[{port <Port# list> | channel-group-number <Channel group# list>}] [vlan <VLAN ID list>] [user
<Web auth user name>] [mac <MAC>] [type force] [detail]
```

Input mode

Administrator mode

Parameters

When this command is executed, at least one parameter must be specified. Specify at least one of the parameters.

mode {dynamic | static}

dynamic

Displays information about authenticated users currently logged in to Web authentication dynamic VLAN mode.

static

Displays information about authenticated users currently logged in to Web authentication static VLAN mode.

Operation when this parameter is omitted:

Information about authenticated users currently logged in to dynamic VLAN mode and in to static VLAN mode is displayed.

{port *<Port# list>* | channel-group-number *<Channel group# list>*}

port *<Port# list>*

Displays information about authenticated users currently logged in 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 information about authenticated users currently logged in for the specified channel group. For details about how to specify *<Channel group# list>*, see *Specifiable values for parameters*.

vlan *<VLAN ID list>*

Displays information about authenticated users currently logged in for the specified VLAN ID. For details about how to specify *<VLAN ID list>*, see *Specifiable values for parameters.*

user *<Web auth user name>*

Displays information about the authenticated, currently logged-in user specified by the user name in this parameter.

mac *<MAC>*

Displays information about the authenticated, currently logged-in user specified by the MAC address in this parameter.

type force

Displays information about the users that have been authenticated by forced

authentication.

detail

Displays detailed information that includes the MAC addresses and IP addresses of user terminals that have already been authenticated and are currently logged in as well as user terminals in the process of being authenticated.

Example 1

Figure 27-1 Displaying information when specifying ports

```
# show web-authentication login select-option port 0/13

Date 2012/12/03 09:42:39 UTC
 Dynamic VLAN mode total login counts(Login/Max):   1 / 1000
  Authenticating client counts :    0
  Port roaming : Enable
   No F User name                Port  VLAN Class Login time          Limit
    1   web10d24                 0/13  1000    24 2012/12/03 09:42:24 infinity

#
```

Display items in Example 1

Table 27-9 Items in the display of authentication status for Web authentication

Item	Meaning	Displayed detailed information
Dynamic VLAN mode total login counts	The number of users currently logged in	`(Login / Max)`: The number of users currently logged in / the maximum number of users set for the device If a maximum number of registered users has not been set, the default value is displayed.
Static VLAN mode total login counts		
Authenticating client counts	The number of terminals on which authentication is being processed	--
Port roaming	Roaming information	Changing of ports within the same VLAN. `Enable`: Enabled `Disable`: Disabled (default)
No	Entry number	The entry number for an authenticated, currently logged-in user. This is just the displayed number, which changes depending on such factors as the filter conditions.
F	Forced authentication indication	*: Indicates a user logged in by using the forced authentication functionality. When the authentication time is updated, a displayed asterisk (`*`) disappears if a request is sent to the RADIUS server and the RADIUS server accepts the request.

Item	Meaning	Displayed detailed information
User name	User name	The name of the authenticated, currently logged-in user. Up to 23 characters are displayed. (If the name exceeds 23 characters, part of the name is replaced with three periods (...).) If the authentication method by user ID is enabled, the user name is displayed without *@authentication-method-list-name*. If the user is being switched by the user switching option functionality, the user name before the switch is displayed.
Port	Port number or channel group number	The port number or channel group number at the time the authenticated, currently logged-in user logged in (CH: xx)
VLAN	VLAN	The VLAN ID of the VLAN that is accommodating the authenticated, currently logged-in user
Class	User class	The user class is displayed.
Login time	Login date and time	The first time the authenticated, currently logged-in user logged in *year*/*month*/*day hour*:*minute*:*second*
Limit	Remaining login time	The remaining login time (*hours*:*minutes*:*seconds*) for the currently logged-in user. 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 set to unlimited: infinity

Example 2

Figure 27-2 Display of authentication status details for Web authentication

```
# show web-authentication login select-option detail

Date 2012/12/03 09:42:27 UTC
 Dynamic VLAN mode total login counts(Login/Max):   1 / 1000
  Authenticating client counts :    0
  Port roaming : Enable
   No F User name
    1   web10d24
         MAC address                  Port  VLAN Class Login time          Limit
         000a.e460.af52              0/13  1000    24 2012/12/03 09:42:24 infinity

 Static VLAN mode total login counts(Login/Max):    1 / 1024
  Authenticating client counts :    0
  Port roaming : Enable
   No F User name
    1   web024
         MAC address    IP address      Port  VLAN Class Login time          Limit
         0025.64c2.4725 192.168.2.221   0/9   200    24 2012/12/03 09:37:43 infinity

#
```

Display items in Example 2

Table 27-10 Items in the display of authentication status details for Web authentication

Item	Meaning	Displayed detailed information
Dynamic VLAN mode total login counts	The number of users currently logged in	`(Login / Max)`: The number of users currently logged in / the maximum number of users set for the device If a maximum number of registered users has not been set, the default value is displayed.
Static VLAN mode total login counts		
Authenticating client counts	The number of terminals on which authentication is being processed	--
Port roaming	Roaming information	Changing of ports within the same VLAN. `Enable`: Enabled `Disable`: Disabled (default)
No	Entry number	The entry number for an authenticated, currently logged-in user. This is just the displayed number, which changes depending on such factors as the filter conditions.
F	Forced authentication indication	*: Indicates a user logged in by using the forced authentication functionality. When the authentication time is updated, a displayed asterisk (`*`) disappears if a request is sent to the RADIUS server and the RADIUS server accepts the request.
User name	User name	The name of the authenticated, currently logged-in user. If the authentication method by user ID is enabled, the user name is displayed without *@authentication-method-list-name*. If the user is being switched by the user switching option functionality, the user name before the switch is displayed.
MAC address	MAC address	The MAC address of the authenticated, currently logged-in user
IP address	IP addresses	The IP address of the authenticated, currently logged-in user. (This item is displayed for fixed VLAN mode only.)
Port	Port number or channel group number	The port number or channel group number at the time the authenticated, currently logged-in user logged in (CH: xx)
VLAN	VLAN	The VLAN ID of the VLAN that is accommodating the authenticated, currently logged-in user
Class	User class	The user class is displayed.
Login time	Login date and time	The first time the authenticated, currently logged-in user logged in *year*/*month*/*day hour*:*minute*:*second*

Item	Meaning	Displayed detailed information
Limit	Remaining login time	The remaining login time (*hours*`:`*minutes*`:`*seconds*) for the currently logged-in user. 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 set to unlimited: infinity
Authenticating client list	List of terminals on which authentication is being processed	Information about terminals on which Web authentication is being processed
No	Entry number	The entry number of a user for which Web authentication is being processed. This is just the displayed number, which changes depending on such factors as the filter conditions.
User name	user name	The name of a user for which authentication is currently being processed If the authentication method by user ID is enabled, the user name is displayed without *@authentication-method-list-name*.
MAC address	MAC address	The MAC address of a user terminal on which authentication is currently being processed
Port	Port number	The port number or channel group number at the time the currently logged-in user logged in (CH: xx)
Status	Status of a terminal for which authentication is being suspended	`Authenticating`: Authentication is in progress.

Impact on communication

None

Response messages

Table 27-11 List of response messages for the show web-authentication login select-option command

Message	Description
There is no information. (web-auth login user)	Information for a Web authentication login user was not found.
Web-Authentication is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

None

show web-authentication login summary

Displays the number of authenticated, currently logged-in users.

Syntax

```
show web-authentication login summary {port [<Port# list>] | channel-group-number
[<Channel group# list>] | vlan [<VLAN ID list>]}
```

Input mode

Administrator mode

Parameters

{port [*<Port# list>*] | channel-group-number [*<Channel group# list>*] | vlan [*<VLAN ID list>*] }

port [*<Port# list>*]

Displays the number of authenticated, currently logged-in users for the specified port. For details about how to specify *<Port# list>* and the specifiable range of values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

The number of authenticated, currently logged-in users is displayed for all ports.

channel-group-number [*<Channel group# list>*]

Displays the number of authenticated, currently logged-in users for the specified channel group.

For details about how to specify *<Channel group# list>*, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

The number of authenticated, currently logged-in users is displayed for all channel groups.

vlan [*<VLAN ID list>*]

Displays the number of authenticated, currently logged-in users for the specified VLAN ID. For details about how to specify *<VLAN ID list>*, see *Specifiable values for parameters.*

Operation when this parameter is omitted:

The number of authenticated, currently logged-in users is displayed for all VLANs.

Example 1

Figure 27-3 Displaying information when specifying ports

```
# show web-authentication login summary port

Date 2012/12/03 09:42:51 UTC
 Dynamic VLAN mode total login counts(Login/Max):   1 / 1000
  Port roaming : Enable
   No  Port  Login /  Max
    1  0/13      1 / 1000

 Static VLAN mode total login counts(Login/Max):    1 / 1024
  Port roaming : Enable
   No  Port  Login /  Max
    1  0/9       1 / 1024
```

```
#
```

Display items in Example 1

Table 27-12 Display items for each port

Item	Meaning	Displayed detailed information
Dynamic VLAN mode total login counts	The number of users currently logged in	`(Login / Max)`: The number of users currently logged in / the maximum number of users set for the device If a maximum number of registered users has not been set, the default value is displayed.
Static VLAN mode total login counts		
Port roaming	Roaming information	Changing of ports within the same VLAN. `Enable`: Enabled `Disable`: Disabled (default)
No	Entry number	The entry number for an authenticated, currently logged-in user. This is just the displayed number, which changes depending on such factors as the filter conditions.
Port	Port number or channel group number	The port number or channel group number at the time the authenticated, currently logged-in user logged in (CH: xx)
Login	The number of logins	The number of authenticated, currently logged-in users for the port
Max	The maximum number of registered users on the port	The maximum number of users set for the port

Example 2

Figure 27-4 Displaying information for VLANs

```
# show web-authentication login summary vlan

Date 2012/12/03 09:42:55 UTC
 Dynamic VLAN mode total login counts(Login/Max):   1 / 1000
  Port roaming : Enable
   No  VLAN  Login
    1  1000      1

 Static VLAN mode total login counts(Login/Max):    1 / 1024
  Port roaming : Enable
   No  VLAN  Login
    1   200      1

#
```

Display items in Example 2

Table 27-13 Items displayed for a VLAN

Item	Meaning	Displayed detailed information
Dynamic VLAN mode total login counts	The number of users currently logged in	`(Login / Max)`: The number of users currently logged in / the maximum number of users set for the device If a maximum number of registered users has not been set, the default value is displayed.
Static VLAN mode total login counts		
Port roaming	Roaming information	Changing of ports within the same VLAN. `Enable`: Enabled `Disable`: Disabled (default)
No	Entry number	The entry number for an authenticated, currently logged-in user. This is just the displayed number, which changes depending on such factors as the filter conditions.
VLAN	VLAN	The VLAN ID of the VLAN that is accommodating the authenticated, currently logged-in user
Login	The number of logins	The number of authenticated, currently logged-in users for the port

Impact on communication

None

Response messages

Table 27-14 List of response messages for the show web-authentication login summary command

Message	Description
Web-Authentication is not configured.	The Web authentication functionality is not enabled. Check the configuration.
There is no information. (web-auth login user)	Information for a Web authentication login user was not found.

Notes

None

show web-authentication logging

Displays the operation log messages collected by the Web authentication functionality.

Syntax

```
show web-authentication logging [search <Search string>]
```

Input mode

Administrator mode

Parameters

search *<Search string>*

Specifies the search string.

If you specify this parameter, only information that includes the search string will be displayed.

Specify the string with 1 to 64 characters. The characters are case sensitive.

Operation when this parameter is omitted:

All the operation log messages output by Web authentication are displayed.

Example

- When the parameter is omitted:

```
# show web-authentication logging


Date 2010/08/06 11:31:07 UTC
AUT 08/06 11:30:59 WEB No=99:ERROR:SYSTEM: MAC=0013.20a5.ee74
USER=web4 Accounting failed ; RADIUS accounting.
AUT 08/06 11:30:59 WEB No=2:NORMAL:LOGOUT: MAC=0013.20a5.ee74
USER=web4 IP=192.168.4.5 PORT=0/5 VLAN=4 Logout succeeded.
AUT 08/06 11:30:59 WEB No=265:NORMAL:SYSTEM: IP=192.168.4.5 Received
logout request.
AUT 08/06 11:30:59 WEB No=99:ERROR:SYSTEM: MAC=0013.20a5.ee74
USER=web4 Accounting failed ; RADIUS accounting.
AUT 08/06 11:30:39 WEB No=1:NORMAL:LOGIN: MAC=0013.20a5.ee74 USER=web4
IP=192.168.4.5 PORT=0/5 VLAN=4 Login succeeded.
AUT 08/06 11:30:39 WEB No=267:NOTICE:SYSTEM: MAC=0013.20a5.ee74
USER=web4 PORT=0/5 Client was force-authorized.


#
```

- Specifying `LOGOUT` for the parameter:

```
# show web-authentication logging search "LOGOUT"


Date 2010/08/06 11:32:32 UTC
AUT 08/06 11:30:59 WEB No=2:NORMAL:LOGOUT: MAC=0013.20a5.ee74
USER=web4 IP=192.168.4.5 PORT=0/5 VLAN=4 Logout succeeded.


 1 events matched.
```

```
#
```

Display items

The following shows the display format of a message.

```
AUT 05/28 09:30:28 WEB No=1:NORMAL:LOGIN: MAC=0090.fe50.26c9 USER=web4000 IP=192.168.0.202 PORT=0/25 VLAN=4000 Login succeeded.
(1)      (2)        (3)  (4)    (5)     (6)                       (7)                                        (8)
```

(1) Log functionality type: Indicates the type of authentication functionality. (Fixed at AUT.)

(2) Date and time: Indicates the date and time (*month/date hour:minute:second*) an event occurred.

(3) Authentication ID: Indicates Web authentication.

(4) Message number: Indicates the number assigned to each message shown in *Table 27-17 List of operation log messages*.

(5) Log ID: Indicates the level of the operation log message.

(6) Log type: Indicates the type of operation that outputs the log message.

(7) Additional information: Indicates supplementary information provided in the message.

(8) Message body

Operation log messages show the following information:

- Log ID/Type: See *Table 27-15 Log ID and type in operation log messages*.
- Additional information: See *Table 27-16 Additional information*.
- Message list: See *Table 27-17 List of operation log messages*.

Table 27-15 Log ID and type in operation log messages

Log ID	Log type	Description
NORMAL	LOGIN	Indicates that login was successful.
	LOGOUT	Indicates that logout was successful.
	SYSTEM	Indicates a runtime notification.
NOTICE	LOGIN	Indicates that authentication failed.
	LOGOUT	Indicates that logout failed.
	SYSTEM	Indicates an alternate operation when a communication failure occurs.
ERROR	SYSTEM	Indicates a communication or operation failure in the Web authentication functionality occurred.

Table 27-16 Additional information

Display format	Meaning
MAC=*xxxx.xxxx.xxxx*	Indicates the MAC address.

Display format	Meaning
USER=*xxxxxxxxxx*	Indicates the user ID.
IP=*xxx.xxx.xxx*	Indicates the IP address.
PORT=*xx/xx* CHGR=*x*	Indicates the port number or channel group number
VLAN=*xxxx*	Indicates the VLAN ID.

Table 27-17 List of operation log messages

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
1	NORMAL	LOGIN	Login succeeded.
	Dynamic VLAN Fixed VLAN		The client was successfully authenticated. [Action] None
			MAC, USER, IP, PORT or CHGR, VLAN[#2]
2	NORMAL	LOGOUT	Logout succeeded.
	Dynamic VLAN Fixed VLAN		Client successfully canceled authentication. [Action] None
			MAC, USER, IP, PORT or CHGR, VLAN[#2]
3	NORMAL	LOGIN	Login update succeeded.
	Dynamic VLAN Fixed VLAN		The user's login time was successfully updated. [Action] None
			MAC, USER, IP, PORT or CHGR, VLAN[#2]
4	NORMAL	LOGOUT	Force logout ; clear web-authentication command succeeded.
	Dynamic VLAN Fixed VLAN		Authentication was canceled by an operation command. [Action] None

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
			MAC, USER, IP, PORT or CHGR, VLAN[#2]
5	NORMAL	LOGOUT	Force logout ; Connection time was beyond a limit.
	Dynamic VLAN Fixed VLAN		Authentication was canceled because the maximum connection time was exceeded. [Action] None
			MAC, USER, IP, PORT or CHGR, VLAN[#2]
6	NORMAL	LOGOUT	Force logout ; mac-address-table aging.
	Dynamic VLAN Fixed VLAN		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, USER, IP, PORT or CHGR, VLAN[#2]
8	NORMAL	LOGOUT	Force logout ; Authentic method changed (RADIUS <-> Local).
	Dynamic VLAN Fixed VLAN		Authentication was canceled because the authentication methods were switched. This log data is collected when the setting of the following commands are changed: ● aaa authentication web-authentication ● aaa authentication web-authentication end-by-reject ● web-authentication authentication ● web-authentication user-group [Action] None
			MAC, USER, IP, PORT or CHGR, VLAN[#2]
10	NOTICE	LOGIN	Login failed ; User name not found to web authentication DB.
	Dynamic VLAN Fixed VLAN		Authentication failed because the specified user ID was not registered in the internal Web authentication DB, or the number of characters for the user ID was out of range. [Action] Use the correct user ID to log in.
			USER

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
11	NOTICE	LOGIN	Login failed ; Password not found to web authentication DB. [Password=[*password*]]
	Dynamic VLAN Fixed VLAN		Authentication failed because a password was not entered or the entered password was incorrect. [Action] Use the correct password to log in.
			USER, password
12	NOTICE	LOGIN	Login failed ; ARP resolution.
	Dynamic VLAN Fixed VLAN		Authentication failed because ARP resolution of the client PC's IP address failed. [Action] Log in again.
			USER, IP
13	NOTICE	LOGOUT	Logout failed ; ARP resolution.
	Dynamic VLAN Fixed VLAN		Authentication could not be canceled because ARP resolution of the client PC's IP address failed. [Action] Log out again.
			USER, IP
14	NOTICE	LOGIN	Login failed ; Double login.
	Dynamic VLAN Fixed VLAN		Authentication failed because another user ID had already logged in from the same client PC. [Action] Log in from another PC.
			MAC, USER
15	NOTICE	LOGIN	Login failed ; Number of login was beyond limit.
	Dynamic VLAN Fixed VLAN		Authentication could not be performed because the number of logins exceeded the maximum allowable number. [Action] Log in again when the number of authenticated users drops low enough.
			MAC, USER

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
16	NOTICE	LOGIN	Login failed ; The login failed because of hardware restriction.
	Dynamic VLAN Fixed VLAN		Authentication could not be performed because the MAC address could not be registered due to hardware limitations. There are no available hash entries. [Action] Log in from another PC.
			MAC, USER
17	NOTICE	LOGIN	Login failed ; VLAN not specified.
	Dynamic VLAN		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, USER, VLAN[#2]
18	NOTICE	LOGIN	Login failed ; MAC address could not register.
	Dynamic VLAN Fixed VLAN		Authentication could not be performed because registration of the MAC address failed. [Action] Log in again.
			MAC, USER
20	NOTICE	LOGIN	Login failed ; RADIUS authentication failed.
	Dynamic VLAN Fixed VLAN		Authentication could not be performed because RADIUS authentication failed. [Action] Use the correct user ID to log in.
			MAC, USER, IP, PORT or CHGR, VLAN[#1]
21	NOTICE	LOGIN	Login failed ; Failed to connection to RADIUS server.
	Dynamic VLAN Fixed VLAN		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 is able to communicate with the RADIUS server, log in again.
			MAC, USER, IP, PORT or CHGR, VLAN[#1]

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
25	NOTICE	LOGIN	Login failed ; Double login. (L2MacManager)
	Dynamic VLAN Fixed VLAN		Authentication failed because a notification that could not be authenticated by the VLAN functionality was received. The cause is either of the following: ● The terminal for which Web authentication was performed had already been authenticated by IEEE 802.1X 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, USER, VLAN[#2]
26	NORMAL	LOGOUT	Force logout ; VLAN deleted.
	Dynamic VLAN Fixed VLAN		● Dynamic VLAN mode The MAC address of the user logged in to the VLAN was deleted because the VLAN set in the configuration was deleted. ● Fixed VLAN mode The MAC address of the user logged in to the VLAN was deleted because the VLAN set for the interface was deleted. [Action] Configure the VLAN again.
			MAC, USER, IP, PORT or CHGR, VLAN[#2]
28	NORMAL	LOGOUT	Force logout ; Polling time out.
	Fixed VLAN		Authentication was canceled because disconnection of an authenticated terminal was detected. [Action] None
			MAC, USER, IP, PORT or CHGR, VLAN
29	NORMAL	LOGOUT	Force logout ; Client moved.
	Dynamic VLAN Fixed VLAN		Authentication was canceled because it was detected that the port of an authenticated terminal was moved. [Action] Log in again.
			MAC, USER, IP, PORT or CHGR, VLAN[#2]

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
31	NORMAL	LOGOUT	Force logout ; Port not specified.
	Dynamic VLAN Fixed VLAN		Authentication has been canceled because the setting for the authentication port was deleted. [Action] Check the configuration.
			MAC, USER, IP, PORT or CHGR, VLAN
32	NOTICE	LOGIN	Login update failed.
	Dynamic VLAN Fixed VLAN		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, USER, IP
33	NORMAL	LOGOUT	Force logout ; Port link down.
	Dynamic VLAN Fixed VLAN		The 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, USER, IP, PORT or CHGR, VLAN[#2]
34	NOTICE	LOGIN	Login failed ; Port not specified.
	Dynamic VLAN Fixed VLAN		Authentication cannot be performed because the request was not issued from the port set for fixed VLAN mode or dynamic VLAN mode. [Action] Connect the terminal to the port to be authenticated, and then log in again.
			MAC, USER, PORT or CHGR
39	NOTICE	LOGIN	Login failed ; VLAN not specified.
	Dynamic VLAN Fixed VLAN		Authentication could not be performed because the authentication request was sent from a VLAN that was not set for the interface. [Action] Set a correct configuration, and log in again.

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
			MAC, USER, IP, PORT or CHGR, VLAN
40	NORMAL	LOGOUT	Force logout ; Ping packet accepted.
	Dynamic VLAN Fixed VLAN		Authentication of the user was canceled because a logout ping was received. [Action] None
			MAC, USER, IP, PORT or CHGR, VLAN[#2]
41	NORMAL	LOGOUT	Force logout ; Other authentication program.
	Dynamic VLAN Fixed VLAN		Authentication was canceled because it was overwritten by another authentication operation. [Action] Make sure that other authentication methods are not used for login from the same terminal.
			MAC, USER, IP, PORT or CHGR, VLAN[#2]
48	NORMAL	LOGOUT	Force logout ; Program stopped.
	Dynamic VLAN Fixed VLAN		The authentication of all users was canceled because the Web authentication functionality stopped. [Action] To use Web authentication uninterruptedly for authentication, set the configuration.
			MAC, USER, IP, PORT or CHGR, VLAN[#2]
56	NOTICE	LOGIN	Login failed ; Number of login was beyond limit of port.
	Dynamic VLAN Fixed VLAN		Authentication cannot be performed because the maximum login limit for a port was exceeded. [Action] Reduce the number of terminals to be authenticated.
			MAC, USER, IP, PORT or CHGR, VLAN

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
57	NORMAL	LOGOUT	Force logout ; Number of login was beyond limit of port.
	Dynamic VLAN Fixed VLAN		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, USER, IP, PORT or CHGR, VLAN
82	NORMAL	SYSTEM	Accepted clear auth-state command.
	Dynamic VLAN Fixed VLAN		A request issued by the `clear web-authentication auth-state` command to cancel authentication was received. [Action] None
			--
83	NORMAL	SYSTEM	Accepted clear statistics command.
	Dynamic VLAN Fixed VLAN		A request issued by the `clear web-authentication statistics` command to clear statistics was received. [Action] None
			--
84	NORMAL	SYSTEM	Accepted commit command.
	Dynamic VLAN Fixed VLAN		A commit notification issued by the `commit web-authentication` command for internal Web authentication DB was received. [Action] None
			--
98	NOTICE	LOGOUT	Logout failed ; User is not authenticating.
	Dynamic VLAN Fixed VLAN		Logout failed because the user had not been authenticated by Web authentication. [Action] Use the `show web-authentication login` command to check the authentication status.
			MAC

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
99	ERROR	SYSTEM	Accounting failed ; RADIUS accounting.
	Dynamic VLAN Fixed VLAN		A response to an accounting request was not received from the RADIUS server. [Action] Check whether communication is available between the Switch and the RADIUS server.
			MAC, USER
105	NOTICE	LOGIN	Login failed ; VLAN suspended.
	Dynamic VLAN		An authentication error occurred because the VLAN that was to be used for the login user after authentication was in the `suspend` status. [Action] After authentication, execute the `state` command to activate the VLAN, and then log in again.
			MAC, USER, VLAN[#2]
106	NORMAL	LOGOUT	Force logout ; VLAN suspended.
	Dynamic VLAN Fixed VLAN		Authentication was canceled because the status of VLAN for the login user changed to `suspend`. [Action] After authentication, execute the `state` command to activate the VLAN, and then log in again.
			MAC, USER, IP, PORT or CHGR, VLAN[#2]
255	ERROR	SYSTEM	The other error.
	Dynamic VLAN Fixed VLAN		An internal Web authentication error occurred. [Action] None
			--
256	NOTICE	LOGIN	Login failed ; Invalid attribute received from RADIUS server.
	Dynamic VLAN Fixed VLAN		A login attempt failed because the attribute of an Accept packet received from the RADIUS server could not be analyzed. [Action] Check the RADIUS server settings.

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
			MAC, USER, PORT or CHGR
260	NOTICE	LOGIN	Login failed ; Multiple login sessions.
	Dynamic VLAN Fixed VLAN		A login attempt failed because duplicate authentication requests were issued. [Action] Open only one login page, and log in again. Also, press the **Login** button only once.
			MAC, USER, PORT or CHGR
264	NORMAL	SYSTEM	Received login request.
	Dynamic VLAN Fixed VLAN		A login request was received. [Action] None
			USER, IP
265	NORMAL	SYSTEM	Received logout request.
	Dynamic VLAN Fixed VLAN		A logout request was received. [Action] None
			IP
266	NORMAL	SYSTEM	Received RADIUS server message.[Message]
	Dynamic VLAN Fixed VLAN		This is Reply-Message Attribute message sent from the RADIUS server (up to 80 characters are displayed). [Action] None
			Message
267	NOTICE	SYSTEM	Client was force-authorized.
	Dynamic VLAN Fixed VLAN		Forced authentication has started because an error occurred when a request was sent to the RADIUS server. [Action] None

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
			MAC, USER, PORT or CHGR
268	NORMAL	SYSTEM	Client port roaming.
	Dynamic VLAN Fixed VLAN		The terminal is roaming. [Action] None
			MAC, USER, PORT or CHGR
270	NOTICE	LOGIN	Login failed ; login-process time out.
	Dynamic VLAN Fixed VLAN		Authentication was canceled because a timeout occurred during authentication. [Action] Log in again.
			MAC, USER, IP
271	NOTICE	LOGIN	Login failed ; login-process sequence error.
	Dynamic VLAN Fixed VLAN		Authentication failed because the response to the PIN code from the RSA authentication server was not received within the designated waiting time. [Action] Log in again.
			MAC, USER, IP
272	NOTICE	LOGIN	Login failed ; login-process incorrect.
	Dynamic VLAN Fixed VLAN		A change of connection port was detected during terminal authentication. [Action] Log in again.
			MAC, USER, IP, PORT or CHGR
273	NOTICE	LOGIN	Login failed ; login-process invalid.
	Dynamic VLAN Fixed VLAN		Authentication failed due to user invalidation because the response from the RSA authentication server was not received. [Action] Log in again.

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
			MAC, IP
276	NORMAL	LOGOUT	Force logout ; Authentic method changed (single <-> multi-step).
	Dynamic VLAN Fixed VLAN		Authentication for the port was canceled because of a switch between the single authentication and multistep authentication methods. [Action] None
			MAC, USER, IP, PORT or CHGR, VLAN[#2]
277	NOTICE	LOGIN	Login failed ; Multi-step failed.
	Dynamic VLAN Fixed VLAN		Authentication failed because MAC-based authentication failed during multistep authentication. [Action] Log in again.
			MAC, USER, IP, PORT or CHGR, VLAN[#2]
278	NORMAL	LOGOUT	Force logout ; User replacement.
	Dynamic VLAN Fixed VLAN		Authentication for a logged-in user ID was canceled because another user ID logged in to the same client PC. [Action] None
			MAC, USER, IP, PORT or CHGR, VLAN[#2]
279	NOTICE	SYSTEM	Invalid user class. [Class]
	Dynamic VLAN Fixed VLAN		The user class set for the RADIUS server is invalid. [Action] Review the RADIUS server setting.
			--
280	NOTICE	SYSTEM	Detect a failure of redirect web-server.
	Dynamic VLAN Fixed VLAN		A failure was detected at the external Web server. [Action] Check whether communication is possible between the Switch and the external Web server.

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
			--
281	NORMAL	SYSTEM	Redirect web-server has been recovered.
	Dynamic VLAN Fixed VLAN		The external Web server was recovered. [Action] None
			--
1*xxx*	NOTICE	LOGIN	Login aborted ; *<cause of the stop>*
	See operation log message with the three digit number indicated.		Authentication processing has stopped. (*xxx*) Operation log message number For details, see the descriptions of the indicated message number.

#1: Displayed when the mode is in fixed VLAN mode.

#2: For dynamic VLAN mode, the VLAN ID might not be displayed until the VLAN to be accommodated is decided.

Impact on communication

None

Response messages

Table 27-18 List of response messages for the show web-authentication logging command

Message	Description
There is no logging data.	There is no operation log data.
There is no log data to match.	Log data matching the specified character string could not be found.
There is no memory.	There is not enough memory to collect data.

Notes

- Web authentication operation log messages are displayed starting from the newer messages.
- If you execute this command with the `search` parameter set and if information that matches the specified character string exists, the number of matched operation log messages is displayed at the end.

  Example: 3 events matched.

clear web-authentication logging

Clears the operation log information for Web authentication.

Syntax

```
clear web-authentication logging
```

Input mode

Administrator mode

Parameters

None

Example

The following shows an example of clearing the operation log information for Web authentication.

```
# clear web-authentication logging

#
```

Display items

None

Impact on communication

None

Response messages

Table 27-19 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.
Web-Authentication is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

None

show web-authentication

Displays the configuration for Web authentication.

Syntax

```
show web-authentication
```

Input mode

Administrator mode

Parameters

None

Example

The following shows an example of displaying the configuration for Web authentication.

```
# show web-authentication

Date 2012/12/03 07:54:33 UTC
<<<Web-Authentication mode status>>>
  Dynamic-VLAN     : Enable
  Static-VLAN      : Enable

<<<System configuration>>>
 * Authentication parameter
  Authentic-mode   : Dynamic-VLAN
  ip address       : 1.1.1.1
  max-user         : 1024
  user-group       : Disable
  user replacement : Disable
  roaming          : Disable
  html-files       : Default

 * AAA methods
  Authentication Default       : RADIUS
  Authentication port-list-AAA : RADIUS web-group-1
  Authentication End-by-reject : Disable
  Accounting Default           : RADIUS

 * Logout parameter
  max-timer        : 60(min)
  auto-logout      : Enable
  logout ping      : tos-windows:   1  ttl:   1
  logout polling   : -

 * Redirect parameter
  redirect         : Enable
  redirect target  : http://www.example.gaibuserver.co.jp
  redirect queries :
  redirect polling : tcp, interval=60, dead-count=1, alive-count=1
  redirect-mode    : HTTP
  web-port         : HTTP : 80(Fixed)  HTTPS : 443(Fixed)
  jump-url         : original

 * Logging status
  [Syslog send]    : Disable
  [Traps]          : Disable

 * Internal DHCP sever status
```

```
  service dhcp vlan: Disable

<Port configuration>
  Port Count            : 1

  Port                  : 0/4
  VLAN ID               : -
  Forceauth VLAN        : Disable
  Access-list-No        : L2-auth
  ARP relay             : Enable
  Max-user              : 1024
  Authentication method : port-list-AAA
  HTML fileset          : FILESETXYZ

<<<System configuration>>>
 * Authentication parameter
  Authentic-mode    : Static-VLAN
  ip address        : 1.1.1.1
  max-user          : 1024
  user-group        : Disable
  user replacement  : Disable
  roaming           : Disable
  html-files        : Default

 * AAA methods
  Authentication Default       : RADIUS
  Authentication port-list-AAA : RADIUS web-group-1
  Authentication End-by-reject : Disable
  Accounting Default           : RADIUS

 * Logout parameter
  max-timer         : 60(min)
  auto-logout       : Enable
  logout ping       : tos-windows:   1  ttl:   1
  logout polling    : Enable  [ interval: 300, count: 3, retry-interval: 1 ]

 * Redirect parameter
  redirect          : Enable
  redirect target   : http://www.example.gaibuserver.co.jp
  redirect queries  :
  redirect polling  : tcp, interval=60, dead-count=1, alive-count=1
  redirect-mode     : HTTP
  web-port          : HTTP : 80(Fixed)  HTTPS : 443(Fixed)
  jump-url          : original

 * Logging status
  [Syslog send]     : Disable
  [Traps]           : Disable

 * Internal DHCP sever status
  service dhcp vlan: -

<Port configuration>
  Port Count            : 2

  Port                  : 0/3
  VLAN ID               : 100
  Forceauth VLAN        : Disable
  Access-list-No        : L2-auth
  ARP relay             : Enable
  Max-user              : 1024
  Authentication method : port-list-AAA
  HTML fileset          : FILESETXYZ
```

```
Port                  : 0/4
VLAN ID               : 100
Forceauth VLAN        : Disable
Access-list-No        : L2-auth
ARP relay             : Enable
Max-user              : 1024
Authentication method : port-list-AAA
HTML fileset          : FILESETXYZ

#
```

Display items

Table 27-20 Information displayed for the Web authentication configuration

Item	Meaning	Displayed detailed information	Mode	
			D	F
Dynamic-VLAN	Dynamic VLAN mode	Operating status of dynamic VLAN mode `Enable`: Enabled `Disable`: Disabled (If this item is `Disable`, the information that follows `<<<System configuration>>>` is not displayed.)	Y	N
Static-VLAN	Fixed VLAN mode	Operating status of fixed VLAN mode[#1] `Enable`: Enabled `Disable`: Disabled (If this item is `Disable`, the information that follows `<<<System configuration>>>` is not displayed.)	N	Y
* Authentication parameter				
Authentic-mode	Authentication mode	Authentication mode for the Web authentication functionality. `Dynamic-VLAN`: Indicates dynamic VLAN mode `Static-VLAN`: Indicates fixed VLAN mode	Y	Y
ip address	IP addresses	Web authentication IP address `Disable` is displayed when this item is not set.	Y	Y
fqdn	Domain name	Domain name This item is not displayed if it is not set.	Y	Y
max-user	Maximum number of authenticated users	Maximum number of authenticated users for each device	Y	Y
user-group	User ID-based authentication method	Setting status for the user ID-based authentication method `Enable`: Enabled `Disable`: Disabled	Y	Y
user replacement	User switching option	Setting status of the user switching option `Enable`: Enabled `Disable`: Disabled	Y	Y

Item	Meaning	Displayed detailed information	Mode	
			D	F
roaming	Roaming	Setting status for roaming `Enable`: Enabled `Disable`: Disabled	Y	Y
html-files	Page setting	Setting status of the basic Web authentication page `Default`: Default `Custom`: The page was replaced by the authentication page replacement functionality.	Y	Y
* AAA methods				
Authentication Default	Default authentication method on the Switch	`Local`: Indicates local authentication `RADIUS`: Indicates RADIUS authentication `Local, RADIUS`: RADIUS authentication after local authentication `RADIUS, Local`: Local authentication after RADIUS authentication `Local` is displayed when this item is not set.	Y	Y
Authentication *<List name>*	The list name and authentication method for the authentication method list	Displays the RADIUS server group name for the authentication method list. RADIUS *<Group name>* `RADIUS`: Indicates RADIUS authentication *<Group name>*: RADIUS server group name `(Not defined)` is displayed after the group name if the RADIUS server group name that has been set is invalid. This item is not displayed if it is not set.	Y	Y
Authenticaion End-by-reject	Operation of rejected authentication	`Enable`: Terminates authentication as error. The second method specified by the `aaa authentication web-authentication` configuration command is used for authentication. `Disable` is displayed when this item is not set.	Y	Y
Accounting Default	Whether the accounting server is available	`RADIUS`: A general-use RADIUS server or a RADIUS server dedicated to Web authentication `Disable` is displayed when this item is not set.	Y	Y
* Logout parameter				
max-timer	Maximum connection time	Maximum connection time (in minutes) for a login user	Y	Y
auto-logout	Whether forced logout available	Use of the forced logout functionality based on MAC address aging in Web authentication `Enable`: Forced logout can be used. `Disable`: Forced logout cannot be used.	Y	Y
logout ping			Y	Y
tos-windows	TOS value	Conditions for the TOS value for special packet ping operations		

Item	Meaning	Displayed detailed information	Mode	
			D	F
ttl	TTL value	Conditions for the TTL value for special packet ping operations		
logout polling	Monitoring functionality	Setting status of the functionality for monitoring the connection of an authenticated terminal `Enable`: Enabled `Disable`: Disabled	N	Y
interval	Monitoring packet sending interval	The interval for sending connection monitoring packets (in seconds)		
count	The number of monitoring packet retransmissions	The number of times connection monitoring packets retransmitted		
retry-interval	The interval for retransmitting monitoring packets	The interval for retransmitting connection monitoring packets (in seconds)		
* Redirect parameter				
redirect	Redirect functionality	Usage state of URL redirection in Web authentication `Enable`: Enabled `Disable`: Disabled	Y	Y
redirect target	Redirect destination URL	--	Y	Y
redirect queries	Automatically added query	Setting status of automatically added queries switch-hostname: Host name of the Switch (`hostname` command) `switch-mac`: System MAC address of the Switch `switch-ip`: Real IP address of the Switch `client-mac`: MAC address of the terminal to be authenticated `client-vlan`: VLAN number of the terminal to be authenticated `client-ip`: IP address of the terminal to be authenticated `port`: Port to which the terminal to be authenticated is connected `original-url`: URL before redirection	Y	Y
redirect polling	Alive monitoring of the external Web server	Setting status of the alive monitoring of the external Web server. `tcp`: tcp packets are used for monitoring. `interval`: The interval for monitoring (in seconds) `dead-count`: The number of times that a failure was determined to have occurred `alive-count`: The number of times that the status was determined to be normal.	Y	Y

Item	Meaning	Displayed detailed information	Mode	
			D	F
redirect-mode	Redirect mode	A protocol for displaying the Web authentication Login page when the URL redirect functionality is enabled	Y	Y
web-port			Y	Y
HTTP	HTTP port number	The number of the port dedicated to URL redirection `80(Fixed)` is always displayed.		
HTTPS	HTTPS port number	The number of the port dedicated to URL redirection `443(Fixed)` is always displayed.		
jump-url	URL to jump to after authentication	URL to jump to after Web authentication is successful `Disable` is displayed when this item is not set.	Y	Y
* Logging status				
[Syslog send]	syslog	Setting status of syslog information output `Enable`: Enabled `Disable`: Disabled	Y	Y
[Traps]	Traps	SNMP trap setting status `Disable` is displayed when this item is disabled.	Y	Y
* Internal DHCP sever status				
service dhcp vlan	Setting status of the VLAN used for the internal DHCP server	Displays the VLAN for which the internal DHCP server operates. `Disable` is displayed when this item is not set.	Y	N
<Port configuration>				
Port Count	Total number of ports	Number of ports for which Web authentication is set to enabled	Y	Y
Port	Port information	Port number or channel group number (CH:*xx*)	Y	Y
VLAN ID	VLAN information	VLAN ID[#2] registered in Web authentication. `-` is displayed if this item has not been set.	Y	Y
Forceauth VLAN	Forced authentication	Setting status of forced authentication in dynamic VLAN mode[#3] *xxxx*: Enabled. *xxxx* indicates the VLAN ID set in configuration. `VLAN unmatch`: Invalid due to an insufficient setting `Disable`: Disabled	Y	N
		Setting status of forced authentication in fixed VLAN mode `Enable`: Enabled `Disable`: Disabled	N	Y

Item	Meaning	Displayed detailed information	Mode	
			D	F
Access-list-No	Access Lists	Setting status of authentication IP access-group `Disable` is displayed if this item is not set.	Y	Y
Arp relay	ARP relay	Setting status of authentication arp-relay `Enable`: Enabled `Disable`: Disabled	Y	Y
Max-user	Maximum number of authenticated users	The maximum number of authenticated users on each port	Y	Y
Authentication method	Authentication list name for the port-based authentication method	Displays the name of the authentication method list registered for each port. ● `(Not defined)` is displayed after the authentication method list name if the set authentication method list name is invalid. ● This item is not displayed if it is not set.	Y	Y
HTML fileset	File set name	Displays the file set name registered for each port. ● `(Not defined)` is displayed after the file set name if the file set name that has been set is invalid. ● `Default` is displayed if this item has not been set.	Y	Y

Legend:

D: Dynamic VLAN mode

F: Fixed VLAN mode

Y: Applicable

N: Not applicable (`-` is also displayed on the screen)

#1 For details about the conditions for enabling the operating status, see *9.1.2 Procedure of configuration for Web authentication* in the *Configuration Guide Vol. 2*.

#2 VLAN IDs registered by automatic VLAN assignment are not displayed.

However, VLAN IDs are displayed if they are accommodated in the native VLAN (fixed) as the result of automatic VLAN assignment.

#3 `native vlan` is displayed if the `authentication force-authorized enable` command is enabled and the `authentication force-authorized vlan` command is not set.

Impact on communication

None

Response messages

Table 27-21 List of response messages for the show web-authentication command

Message	Description
Web-Authentication is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

None

show web-authentication statistics

Displays statistics for Web authentication.

Syntax

```
show web-authentication statistics
```

Input mode

Administrator mode

Parameters

None

Example

The following shows an example of displaying statistics related to Web authentication.

```
# show web-authentication statistics

Date 2010/08/06 11:40:35 UTC
Web-Authentication Information:
  Authentication Request Total :         17
  Authentication Current Count :          2
  Authentication Error Total   :          1

RADIUS Web-Authentication Information:
[RADIUS frames]
  TxTotal   :        17  TxAccReq  :        17  TxError   :         0
  RxTotal   :        12  RxAccAccpt:        11  RxAccRejct:         1
                         RxAccChllg:         0  RxInvalid :         0
Account Web-Authentication Information:
[Account frames]
  TxTotal   :        24  TxAccReq  :        24  TxError   :         0
  RxTotal   :        19  RxAccResp :        19  RxInvalid :         0

#
```

Display items

Table 27-22 Items displayed for statistics related to Web authentication

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
RADIUS frames	RADIUS server information
TxTotal	The total number of transmissions 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

Item	Meaning
RxTotal	The total number of receptions 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 transmitted 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

Impact on communication

None

Response messages

Table 27-23 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.
Web-Authentication is not configured.	The Web authentication functionality 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

Example

The following shows an example of clearing Web authentication statistics:

```
# clear web-authentication statistics

#
```

Display items

None

Impact on communication

None

Response messages

Table 27-24 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.
Web-Authentication is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

None

commit web-authentication

Stores the internal Web authentication DB in internal flash memory and reflects its contents for operation.

Syntax

```
commit web-authentication [-f]
```

Input mode

Administrator mode

Parameters

-f

Stores the internal Web authentication DB in internal flash memory and reflects its contents for operation. No confirmation message is displayed.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

The following shows an example of storing the internal Web authentication DB.

```
# 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 27-25 List of response messages for the commit web-authentication command

Message	Description
Commit complete.	Storing the DB in internal flash memory and reflecting its contents for Web authentication finished normally.
Flash memory write failed.	Writing of the information to internal flash memory failed.
Web-Authentication is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

The contents of the internal Web authentication DB are not overwritten during operation 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

store web-authentication

Backs up the internal Web authentication DB to a file.

Syntax

```
store web-authentication ramdisk <File name> [-f]
```

Input mode

Administrator mode

Parameters

ramdisk

Backs up the internal Web authentication DB to a file on the RAMDISK.

<File name>

Specify the name of the file to which the internal Web authentication DB is to be backed up.

Specify the file name with 64 or fewer characters.

For the characters that can be specified, see *Specifiable values for parameters.*

-f

Backs up the internal Web authentication DB to a file without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

Backing up the internal Web authentication DB to the `web-DB_data` file:

```
# store web-authentication ramdisk web-DB_data
Backup web-authentication user data.  Are You sure? (y/n): y

Backup complete.
#
```

Display items

None

Impact on communication

None

Response messages

Table 27-26 List of response messages for the store web-authentication command

Message	Description
Backup complete.	A backup file has been created successfully.
Store operation failed.	The command could not be executed because of insufficient RAMDISK capacity.

Message	Description
Command information was damaged.	A backup file could not be generated because the authentication information was corrupted.
Data doesn't exist.	A backup file could not be generated. A commit operation might not have been executed. Execute a commit operation, and then check the result. If the commit operation fails again, the internal flash memory might be corrupted.
Web-Authentication is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

All files on the RAMDISK are deleted when the device restarts. To save backup files, transfer them to a PC via FTP or use the copy command to copy them to the memory card.

load web-authentication

Restores the internal Web authentication DB from a backup file. 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 ramdisk <File name> [-f]
```

Input mode

Administrator mode

Parameters

ramdisk

Restores the internal Web authentication DB from a backup file on the RAMDISK.

<File name>

Specifies the name of the backup file from which the internal Web authentication DB is to be restored.

Specify the file name with 64 or fewer characters.

For the characters that can be specified, see *Specifiable values for parameters.*

-f

Restores the internal Web authentication DB without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

Restoring the internal Web authentication DB from the `web-DB_data` file:

```
# load web-authentication ramdisk web-DB_data
Restore web-authentication user data.  Are you sure? (y/n): y

Restore complete.
#
```

Display items

None

Impact on communication

None

Response messages

Table 27-27 List of response messages for the load web-authentication command

Message	Description
Restore complete.	Restoration from the backup file was successful.
File format error.	The format of the specified backup file is different from the internal Web authentication DB.
Load operation failed.	Restoration from the backup file failed.
Flash memory write failed.	Writing of the information to internal flash memory failed.
Web-Authentication is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

1. 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
2. If the restore information has been saved on a PC, transfer it to the RAMDISK via FTP. If the restore information has been saved on the memory card, use the `copy` operation command to copy it to the RAMDISK. After either operation, execute the `load web-authentication` command. It is not possible to restore the files on a PC or the memory card directly.

clear web-authentication auth-state

Forcibly logs out an authenticated, currently logged-in user.

Syntax

```
clear web-authentication auth-state { user {<Web auth user name> | -all} | mac-address
<MAC>} [-f]
```

Input mode

Administrator mode

Parameters

user {<*Web auth user name*> | -all }

<*Web auth user name*>

Forces user logout by specifying an authenticated user that is currently logged in.

-all

Forces the logout of all authenticated uses that are currently logged in.

mac-address <*MAC*>

Forces user logout by specifying the MAC address of an authenticated user that is currently logged in.

-f

Forces user logout without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

- Forcing logout of authenticated user `USR01` who is currently logged in:

```
# clear web-authentication auth-state user USER01
Logout user web-authentication.  Are you sure? (y/n): y
```

- Forces logout of all authenticated uses that are currently logged in:

```
# clear web-authentication auth-state user -all
Logout all user web-authentication.  Are you sure? (y/n): y
```

- Forcing logout of an authenticated user that is currently logged in 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 27-28 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.
Web-Authentication is not configured.	The Web authentication functionality is not enabled. Check the configuration.
The specified user is not login user.	The specified user is not a login user.
The specified MAC address does not exist.	The specified MAC address does not exist.
User does not exist.	The user was not found

Notes

If the user is being replaced by the user switching option functionality, specify the user name used before the switch.

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 a directory on the RAMDISK beforehand. Note that if you execute this command with a new file specified, all registered information will be all cleared and the new information will take its place.

Syntax

```
set web-authentication html-files ramdisk <Directory name> [html-fileset <Name>][-f]
```

Input mode

Administrator mode

Parameters

ramdisk

Specify a directory on the RAMDISK.

<Directory name>

Specify a directory that stores a custom file.

For details about how to specify a directory, see *Specifiable values for parameters*.

Specify the directory that stores the page images, messages, or icons to be displayed on the **Favorites** menu of the Web browser that you want to register.

Page images, messages, and icons to be displayed in the **Favorites** menu of the Web browser that you want to register must be stored on the RAMDISK according to the following conditions:

- 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`

  Authentication-in-progress 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 on the **Favorites** menu of the Web browser: `favicon.ico`

  Other stored files, such as GIF files, can have any name.

html-fileset *<Name>*

Specify the custom file set name that holds the files for individual Web authentication

pages.

Specify the name with 1 to 16 characters. Use only uppercase alphanumeric characters.

Operation when this parameter is omitted:

The basic Web authentication page is replaced with the custom file set.

-f

Replaces pages, messages, and icons without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

- When a confirmation message is displayed:

```
# set web-authentication html-files ramdisk "web-file"
Do you wish to install new html-files? (y/n): y
executing...
Install complete.
```

- When a confirmation message is not displayed:

```
# set web-authentication html-files ramdisk "web-file" -f
executing...
Install complete.
```

Display items

None

Impact on communication

None

Response messages

Table 27-29 List of response messages for the set web-authentication html-files command

Message	Description
Can't execute.	The command could not be executed. Clear all registered information by using the `clear` command, and then try again.
Can't put a sub directory in the directory.	The specified directory contains a subdirectory.
Directory size over.	The capacity of the specified directory exceeds the limit (1024KB).
File name is too long.	The total number of characters in a directory name and its subordinate file name exceeds the limit of 64 characters.
File name 'xxx' is reserved.	The file name *xxx* is a reserved word and cannot be used. The `wol` file is included in the directory specified for *<Directory name>*. Use the `del` command to delete the `wol` file in this

Message	Description
	directory, and then try again.
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.
The number of html-filesets exceeds 4.	The number of the registered custom file sets exceeds 4.
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.
- The pages, messages, and icons registered by this command remain in use if the device is restarted.
- For details about the total size of files and the number of the files that can be registered, see *3.2 Capacity Limit* in the *Configuration Guide Vol. 1*.
- An error occurs if the specified directory contains a subdirectory or if the `login.html` file does not exist.
- The default Web page is displayed while this command is being executed.
- An error occurs if the total number of characters in a directory name and its subordinate file name exceeds 64.
- You can register no more than 4 custom file set names.
- In dynamic VLAN mode, if the `loginOK.html` file contains a reference to another file, the Login Success page might not be correctly displayed.

store web-authentication html-files

Retrieves the images of Web authentication pages (such as login and logout pages), the messages output for authentication errors, and the icons displayed on the **Favorites** menu of the Web browser, all of which are in current use, and stores them in any directory on the RAMDISK. Related files are also retrieved at the same time. Specific files cannot be specified.

Syntax

```
store web-authentication html-files ramdisk <Directory name> [html-fileset <Name>][-f]
```

Input mode

Administrator mode

Parameters

ramdisk

Specifies the RAMDISK.

<Directory name>

Specify the directory that holds the applicable files.

For details about how to specify a directory, see *Specifiable values for parameters*.

html-fileset *<Name>*

Specify the name of the custom file set configured for an individual Web authentication page.

Files related to the specified custom file set are also retrieved at the same time.

Operation when this parameter is omitted:

The files related to the file set configured for the basic Web authentication page are retrieved at the same time.

-f

Stores the pages, messages, and icons without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

- When a confirmation message is displayed:

```
# store web-authentication html-files ramdisk "web-file"
Do you wish to store html-files? (y/n): y
executing...
Store complete.
```

- When a confirmation message is not displayed:

```
# store web-authentication html-files ramdisk "web-file" -f
executing...
Store complete.
```

Display items

None

Impact on communication

None

Response messages

Table 27-30 List of response messages for the store web-authentication html-files command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Directory isn't empty.	The specified directory is not empty. Make sure there is no files or subdirectories in the directory.
File name is too long.	The total number of characters in a directory name and its subordinate file name exceeds the limit of 64 characters.
No such directory.	The specified directory does not exist.
No such html-fileset 'xxx'.	The specified custom file set was not found. *xxx*: Custom file set name
Store complete.	File retrieval was completed successfully.

Notes

- This command can be executed regardless of whether or not the configuration command for Web authentication has been set.
- An error occurs if the specified directory contains a file or subdirectory.
- The default page and the registered page are not distinguished with regard to the page image file.
- If the free capacity on the RAMDISK is insufficient (1024 KB or more), use the `del` command to delete unnecessary files and then create a directory.
- An error occurs if the total number of characters in a directory name and its subordinate file name exceeds 64. Use the `show web-authentication html-files` command to check the file name.

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).

Operation when this parameter is omitted:

Information about files other than the HTML file, msg file, and ico file is displayed collectively as `the other files`.

Example

The following shows examples of displaying the size of the file (in bytes) registered by the `set web-authentication html-files` command and the date and time the file was registered.

- When the parameter is omitted:

```
# show web-authentication html-files


Date 2010/09/29 02:59:53 UTC
    Total Size :          50,356


    File Date               Size Name
    2010/09/29 02:12       1,507 login.html      <---1
    2010/09/29 02:12       1,307 loginProcess.html
    2010/09/29 02:12       1,260 loginOK.html
    2010/09/29 02:12         666 loginNG.html
    2010/09/29 02:12         937 logout.html
    2010/09/29 02:12         586 logoutOK.html
    2010/09/29 02:12         640 logoutNG.html
    2010/09/29 02:12         545 webauth.msg
    default now                0 favicon.ico     <---2
    2010/09/29 02:12      17,730 the other files
    < FILESETXYZ >                          <------3
    2010/09/29 02:14       1,507 login.html
    2010/09/29 02:14       1,307 loginProcess.html
    2010/09/29 02:14       1,260 loginOK.html
```

```
    2010/09/29 02:14         666 loginNG.html
    2010/09/29 02:14         937 logout.html
    2010/09/29 02:14         586 logoutOK.html
    2010/09/29 02:14         640 logoutNG.html
    2010/09/29 02:14         545 webauth.msg
    default now                0 favicon.ico
    2010/09/29 02:14      17,730 the other files

#
```

1. Displays the time required to register the basic Web authentication page custom file set.
2. For the default status, `default now` is displayed.
3. Displayed when the individual Web authentication page custom file set is registered.

- Specifying `detail` parameter (information about individual files that are not the HTML file, msg file, or ico file is displayed):

```
# show web-authentication html-files detail

Date 2010/09/29 02:59:56 UTC
    Total Size :          50,356

    File Date               Size Name
    2010/09/29 02:12       1,507 login.html
    2010/09/29 02:12       1,307 loginProcess.html
    2010/09/29 02:12       1,260 loginOK.html
    2010/09/29 02:12         666 loginNG.html
    2010/09/29 02:12         937 logout.html
    2010/09/29 02:12         586 logoutOK.html
    2010/09/29 02:12         640 logoutNG.html
    2010/09/29 02:12         545 webauth.msg
    default now                0 favicon.ico
    2010/09/29 02:12       8,441 IMAGE001.JPG
    2010/09/29 02:12       5,528 IMAGE002.JPG
    2010/09/29 02:12       3,761 IMAGE003.GIF
    < FILESETXYZ >
    2010/09/29 02:14       1,507 login.html
    2010/09/29 02:14       1,307 loginProcess.html
    2010/09/29 02:14       1,260 loginOK.html
    2010/09/29 02:14         666 loginNG.html
    2010/09/29 02:14         937 logout.html
    2010/09/29 02:14         586 logoutOK.html
    2010/09/29 02:14         640 logoutNG.html
```

```
2010/09/29 02:14         545 webauth.msg
default now                0 favicon.ico
2010/09/29 02:14       8,441 IMAGE001.JPG
2010/09/29 02:14       5,528 IMAGE002.JPG
2010/09/29 02:14       3,761 IMAGE003.GIF

#
```

Display items

None

Impact on communication

None

Response messages

Table 27-31 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 html-files

Deletes the Web authentication pages registered by the `set web-authentication html-files` command, messages, and icons, and reverts to the default file set.

Syntax

```
clear web-authentication html-files [{html-fileset <Name> | -all}][-f]
```

Input mode

Administrator mode

Parameters

{html-fileset <*Name*> | -all}

html-fileset <*Name*>

Deletes the custom file set for the specified individual Web authentication page.

-all

Deletes all custom file sets for individual Web authentication pages.

The basic Web authentication page reverts to the default file set.

Operation when this parameter is omitted:

The basic Web authentication page reverts to the default file set.

-f

Deletes the pages, messages, and icons without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

- When a confirmation message is displayed:

```
# clear web-authentication html-files
Do you wish to clear registered html-files and initialize? (y/n): y
executing...
Clear complete.

#
```

- When a confirmation message is not displayed:

```
# clear web-authentication html-file -f
executing...
Clear complete.

#
```

Display items

None

Impact on communication

None

Response messages

Table 27-32 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.
No such html-fileset 'xxx'.	The specified custom file set was not found. *xxx*: Custom file set name

Notes

This command can be executed regardless of whether or not the configuration command for Web authentication has been set.

show web-authentication redirect target

Displays the status when the redirect destination is changed to an external Web server in URL redirection.

Syntax

```
show web-authentication redirect target
```

Input mode

Administrator mode

Parameters

None

Example

The following shows an example displayed when the redirect destination is changed to an external Web server.

```
# show web-authentication redirect target

Date 2012/12/03 08:13:34 UTC
<Web-server information>
 target               : http://www.example.gaibuserver.co.jp
   status             : alive
   last change time   : 2012/12/03 08:12:39 UTC
   total change count : 2

#
```

Display items

Table 27-33 Information displayed when the redirect destination is changed to an external Web server

Item	Displayed information	Displayed detailed information
web-server information		
target	URL to which the external Web server is redirected	--
status	Status of the external Web server	`alive`: Normal (the external Web server is used.) `dead`: Failure (the Web server of the Switch is used.) If alive monitoring is not set, a hyphen (-) is displayed (the external Web server is used).
last change time	The last time the external Web server status changed	*year*`/`*month*`/`*day* *hour*`:`*minute*`:`*second* *time-zone* A hyphen (-) is displayed in the following cases: ● A port is in the `initialize` status. ● Alive monitoring is not set.
total change count	The number of times the external Web server status changed	A hyphen (-) is displayed if alive monitoring is not set.

Impact on communication

None

Response messages

Table 27-34 List of response messages for the show web-authentication redirect target command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Web-Authentication external redirection is not configured.	The redirect target has not been configured. Check the configuration.
Web-Authentication is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

None

28. MAC-based Authentication

show mac-authentication login
clear mac-authentication auth-state
show mac-authentication login select-option
show mac-authentication login summary
show mac-authentication logging
clear mac-authentication logging
show mac-authentication
show mac-authentication statistics
clear mac-authentication statistics
set mac-authentication mac-address
remove mac-authentication mac-address
show mac-authentication mac-address
commit mac-authentication
store mac-authentication
load mac-authentication

For details such as a description of the authentication modes, see the *Configuration Guide Vol. 2*.

show mac-authentication login

Displays information about the terminals (MAC address) that have been authenticated in ascending order by authenticated date and time.

Syntax

```
show mac-authentication login
```

Input mode

Administrator mode

Parameters

None

Example

```
# show mac-authentication login

Date 2012/11/30 20:10:47 UTC
 Dynamic VLAN mode total client counts(Login/Max):  1 / 1000
  Authenticating client counts :    0
  Hold down client counts      :    0
  Port roaming : Enable
   No F MAC address     Port  VLAN Class  Login time           Limit     Reauth
    1   009f.eafb.003d  0/33  1000    62  2012/11/30 20:10:46   23:59:58   86398

 Static VLAN mode total client counts(Login/Max):    1 / 1024
  Authenticating client counts :    0
  Hold down client counts      :    0
  Port roaming : Enable
   No F MAC address     Port  VLAN Class  Login time           Limit     Reauth
    1   0025.64c2.4725  0/4    200    24  2012/11/30 20:10:46   23:59:59   86399

#
```

Display items

Table 28-1 Items displayed for the authenticated terminal information

Item	Meaning	Displayed detailed information
Dynamic VLAN mode total client counts	The number of currently authenticated terminals	`(Login / Max)`: The number of currently authenticated terminals / the maximum number of registered terminals set for the device
Static VLAN mode total client counts		
Authenticating client counts	The number of terminals on which authentication is being processed	--
Hold down client counts	The number of terminals on which authentication has been suspended	--

Item	Meaning	Displayed detailed information
Port roaming	Roaming information	Changing of ports within the same VLAN. `Enable`: Enabled `Disable`: Disabled (default)
No	Entry number	The entry number for a currently authenticated terminal. This is just the displayed number, which changes depending on such factors as the filter conditions.
F	Forced authentication indication	*: A terminal authenticated by the forced authentication functionality. After the authentication state is canceled, the displayed asterisk (`*`) disappears if the RADIUS server accepts a request.
MAC address	MAC address	The MAC address of the currently authenticated terminal
Port	Port number	The port number or channel group number (CH: xx) when the currently authenticated terminal was authenticated
VLAN	VLAN	The VLAN in which the currently authenticated terminal is accommodated
Class	User class	The user class is displayed. `-` is displayed for the first step of multistep authentication.
Login time	Date and time authentication was successful	The first time the currently authenticated terminal was authenticated (*year*`/`*month*`/`*day* *hour*`:`*minute*`:`*second*)
Limit	Remaining time for authentication	The remaining time for the authenticated state of the currently authenticated terminal (*hour*`:`*minute*`:`*second*). When a terminal is authenticated, the remaining time might be displayed as `00:00:00` immediately before authentication for the terminal is canceled due to a timeout. When the maximum connection time is set to unlimited: infinity (If this has not been configured, the default value is displayed.)
Reauth	Remaining time for re-authentication	The remaining time until re-authentication is performed (in seconds). `-` is displayed if re-authentication is disabled. When a terminal is authenticated, the remaining time might be displayed as `0` immediately before authentication for the terminal is canceled due to a timeout.

Impact on communication

None

Response messages

Table 28-2 List of response messages for the show mac-authentication login command

Message	Description
There is no information. (mac-auth login)	There is no MAC address authenticated by MAC-based authentication.
MAC-Authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

Notes

None

clear mac-authentication auth-state

Forces cancellation of the authentication of a currently authenticated terminal.

Syntax

```
clear mac-authentication auth-state mac-address {<MAC> | -all} [-f]
```

Input mode

Administrator mode

Parameters

mac-address {<*MAC*> | -all}

<*MAC*>

Forces cancellation of the authentication of the currently authenticated terminal with the specified MAC address.

Specify the MAC address.

-all

Forces cancellation of the authentication for all currently authenticated terminals.

-f

Forces cancellation of the authentication for the specified MAC address without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

- Forcing cancellation of the authentication of the currently authenticated terminal with the specified MAC address:

```
# clear mac-authentication auth-state mac-address 0012.e212.3345
Do you wish to clear the authenticated MAC? (y/n): y
```

- Forcing cancellation of the authentication of all currently authenticated terminals:

```
# clear mac-authentication auth-state mac-address -all
Do you wish to clear the all authenticated MAC? (y/n): y
```

Display items

None

Impact on communication

Authentication for the specified terminal will be canceled.

Response messages

Table 28-3 List of response messages for the clear mac-authentication auth-state command

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

Message	Description
The specified MAC address does not exist.	The specified terminal (MAC address) does not exist (when a single MAC address is specified).
MAC address does not exist.	No terminals (MAC address) exist (when the `-all` parameter is specified).
MAC-Authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

Notes

None

show mac-authentication login select-option

Extracts specified items from the information about the currently authenticated terminals (MAC address) and displays them in ascending order by authentication date and time.

Note that if you execute the command with the `detail` option specified, entries in the process of authentication and entries for which authentication processing has been suspended are also displayed as extracted entries.

Syntax

```
show mac-authentication login select-option [mode {dynamic | static}]
[{port <Port# list> | channel-group-number <Channel group# list>}] [vlan <VLAN ID list>] [mac
<MAC>] [type force] [detail]
```

Input mode

Administrator mode

Parameters

When this command is executed, at least one parameter must be specified. Specify at least one of the parameters.

mode {dynamic | static}

dynamic

Displays information about terminals that have been authenticated in MAC-based authentication dynamic VLAN mode.

static

Displays information about terminals that have been authenticated in MAC-based authentication fixed VLAN mode.

Operation when this parameter is omitted:

Information about terminals authenticated in both dynamic VLAN mode and fixed VLAN mode is displayed.

{port *<Port# list>* | channel-group-number *<Channel group# list>*}

port *<Port# list>*

Displays information about authenticated terminals 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 the terminal information for the specified channel group. For details about how to specify *<Channel group# list>*, see *Specifiable values for parameters*.

vlan *<VLAN ID list>*

Displays information about authenticated terminals for the specified VLAN ID. For details about how to specify *<VLAN ID list>*, see *Specifiable values for parameters.*

mac *<MAC>*

Displays information about authenticated terminals for the specified MAC address.

type force

Displays information about terminals that have been authenticated by forced authentication.

detail

Displays detailed information, including information about terminals that have been authenticated, terminals in the process of being authenticated, and terminals for

which authentication processing has been suspended due to authentication failure.

Example 1

Figure 28-1 Displaying information about authenticated terminals for the specified port

```
# show mac-authentication login select-option port 0/4

Date 2012/11/30 20:23:21 UTC
 Static VLAN mode total client counts(Login/Max):    1 / 1024
  Authenticating client counts :    1
  Hold down client counts      :    1
  Port roaming : Enable
   No F MAC address     Port  VLAN Class  Login time           Limit     Reauth
    1   0025.64c2.4725  0/4    200    24  2012/11/30 20:10:46   23:59:59   86399

#
```

Display items 1

Table 28-4 Items displayed for the authenticated terminal information

Item	Meaning	Displayed detailed information
Dynamic VLAN mode total client counts	The number of currently authenticated terminals	`(Login / Max)`: The number of currently authenticated terminals / the maximum number of registered terminals set for the device
Static VLAN mode total client counts		
Authenticating client counts	The number of terminals on which authentication is being processed	--
Hold down client counts	The number of terminals on which authentication has been suspended	--
Port roaming	Roaming information	Changing of ports within the same VLAN. `Enable`: Enabled `Disable`: Disabled (default)
No	Entry number	The entry number for a currently authenticated terminal. This is just the displayed number, which changes depending on such factors as the filter conditions.
F	Forced authentication indication	*: A terminal authenticated by the forced authentication functionality. After the authentication state is canceled, the displayed asterisk (`*`) disappears if the RADIUS server accepts a request.
MAC address	MAC address	The MAC address of the currently authenticated terminal
Port	Port number	The port number or channel group number (CH: xx) when the currently authenticated terminal was authenticated

Item	Meaning	Displayed detailed information
VLAN	VLAN	The VLAN in which the currently authenticated terminal is accommodated
Class	User class	The user class is displayed. - is displayed for the first step of multistep authentication.
Login time	Date and time authentication was successful	The first time the currently authenticated terminal was authenticated (*year*/*month*/*day* *hour*:*minute*:*second*)
Limit	Remaining time for authentication	The remaining time for the authenticated state of the currently authenticated terminal (*hour*:*minute*:*second*). When a terminal is authenticated, the remaining time might be displayed as 00:00:00 immediately before authentication for the terminal is canceled due to a timeout. When the maximum connection time is set to unlimited: infinity (If this has not been configured, the default value is displayed.)
Reauth	Remaining time for re-authentication	The remaining time until re-authentication is performed (in seconds). - is displayed if re-authentication is disabled. When a terminal is authenticated, the remaining time might be displayed as 0 immediately before authentication for the terminal is canceled due to a timeout.

Example 2

Figure 28-2 Display of authentication status details for MAC-based authentication

```
# show mac-authentication login select-option detail

Date 2012/11/30 20:23:21 UTC
 Dynamic VLAN mode total client counts(Login/Max):   1 / 1000                  ┐
  Authenticating client counts :    1                                           │
  Hold down client counts      :    1                                          │(A)
  Port roaming : Enable                                                        │
   No F MAC address     Port  VLAN Class  Login time           Limit     Reauth │
    1   009f.eafb.003d  0/33  1000    62  2012/11/30 20:10:46   23:59:20   86398 ┘
  Authenticating client list
       MAC address     Port        Status
       009f.eafb.0048  0/13        Authenticating
  Hold down client list
       MAC address     Port        Status                Remaining
       0000.e28c.4add  0/5         Failed (RADIUS fail)  00:04:56

 Static VLAN mode total client counts(Login/Max):    1 / 1024                  ┐
  Authenticating client counts :    1                                          │
  Hold down client counts      :    1                                          │(A)
  Port roaming : Enable                                                       │
   No F MAC address     Port  VLAN Class  Login time           Limit     Reauth │
    1   0025.64c2.4725  0/4    200    24  2012/11/30 20:22:43   23:59:21   86361 ┘
  Authenticating client list
       MAC address     Port  VLAN  Status
       0000.e227.8bf6  0/8   4000  Authenticating
```

```
  Hold down client list
        MAC address     Port  VLAN  Status               Remaining
        0000.e227.8bf7  0/8   4000  Failed (refused)     00:00:59

#
```

Display items 2

Table 28-5 Items in the display of authentication status details for MAC-based authentication

Item	Meaning	Displayed detailed information
The explanation of (A) is the same as in *Display items 1*. See *Table 28-4 Items displayed for the authenticated terminal information*.		
Authenticating client list	List of terminals on which authentication is being processed	Information about terminals for which MAC-based authentication is being processed
MAC address	MAC address	MAC address of a terminal for which MAC-based authentication is being processed.
Port	Port number	Connection port number of a terminal for which MAC-based authentication is being processed, or channel group number (CH:*xx*)
VLAN	VLAN ID	The VLAN ID associated with a terminal for which MAC-based authentication is being processed. (This item is displayed for fixed VLAN mode only.)
Status	Authentication status	`Authenticating`: Authentication is in progress.
Hold down client list	List of terminals for which authentication has been suspended	Information about terminals for which MAC-based authentication has failed and authentication processing has been suspended
MAC address	MAC address	MAC address of a terminal for which MAC-based authentication has been suspended.
Port	Port number	Connection port number of a terminal for which MAC-based authentication has been suspended, or channel group number (CH:*xx*)
VLAN	VLAN ID	The VLAN ID associated with a terminal for which MAC-based authentication has been suspended. (This item is displayed for fixed VLAN mode only.)

Item	Meaning	Displayed detailed information
Status	Status of a terminal for which authentication is being suspended	The status of a terminal for which MAC-based authentication has been suspended is displayed. `Failed(reason*1)`: Authentication failed. `(*1)` The following are the reasons for an authentication failure: Information displayed in dynamic VLAN mode ● VLAN unmatch (An undefined VLAN was assigned.) ● refused (Authentication was rejected.) ● timeout (The RADIUS server did not respond.) ● RADIUS fail (An error on the RADIUS server connection occurred.) ● VLAN suspend (The VLAN was suspended.) Information displayed in fixed VLAN mode ● refused (Authentication was rejected.) ● timeout (The RADIUS server did not respond.) ● RADIUS fail (An error on the RADIUS server connection occurred.) ● VLAN suspend (The VLAN was suspended.)
Remaining	The remaining time until re-authentication will start again	*hours*`:`*minutes*`:`*seconds*

Impact on communication

None

Response messages

Table 28-6 List of response messages for the show mac-authentication login select-option command

Message	Description
There is no information. (mac-auth login)	There is no MAC address authenticated by MAC-based authentication.
MAC-Authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

Notes

None

show mac-authentication login summary

Displays the number of entries for currently authenticated terminals.

Syntax

```
show mac-authentication login summary {port [<Port# list>] | channel-group-number
[<Channel group# list>] | vlan [<VLAN ID list>]}
```

Input mode

Administrator mode

Parameters

{port [*<Port# list>*] | channel-group-number [*<Channel group# list>*] | vlan [*<VLAN ID list>*]}

<Port# list>

Displays the number of currently authenticated terminals for the specified port. For details about how to specify *<Port# list>*, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

The number of currently authenticated terminals for all ports is displayed.

channel-group-number [*<Channel group# list>*]

Displays the number of currently authenticated terminals for the specified channel group. For details about how to specify *<Channel group# list>*, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

The number of currently authenticated terminals for all channel groups is displayed.

<VLAN ID list>

Displays the number of currently authenticated terminals for the specified VLAN ID. For details about how to specify *<VLAN ID list>*, see *Specifiable values for parameters.*

Operation when this parameter is omitted:

The number of currently authenticated terminals for all VLANs is displayed.

Example 1

Figure 28-3 Displaying the number of authenticated terminals for the specified port

```
# show mac-authentication login summary port

Date 2012/11/30 20:28:21 UTC
 Dynamic VLAN mode total client counts(Login/Max):   1 / 1000
  Authenticating client counts :    1
  Hold down client counts      :    1
  Port roaming : Disable
   No  Port  Login /  Max
    1  0/33      1 / 1000

 Static VLAN mode total client counts(Login/Max):    1 / 1024
  Authenticating client counts :    1
  Hold down client counts      :    1
  Port roaming : Disable
```

```
  No  Port  Login /  Max
   1  0/4       1 / 1024

#
```

Display items 1

Table 28-7 Display items for each port

Item	Meaning	Displayed detailed information
Dynamic VLAN mode total client counts	The number of currently authenticated terminals	`(Login / Max)`: The number of currently authenticated terminals / the maximum number of registered terminals set for the device
Static VLAN mode total client counts		
Authenticating client counts	The number of terminals on which authentication is being processed	--
Hold down client counts	The number of terminals on which authentication has been suspended	--
Port roaming	Roaming information	Changing of ports within the same VLAN. `Enable`: Enabled `Disable`: Disabled (default)
No	Entry number	The entry number for a currently authenticated terminal. This is just the displayed number, which changes depending on such factors as the filter conditions.
Port	Port number	Port number on which the currently authenticated terminal exists, or channel group number
Login	The number of currently authenticated terminals	Number of currently authenticated terminals on the port
Max	The maximum registered terminals on the port	The maximum number of terminals set for the port

Example 2

Figure 28-4 Displaying the number of authenticated terminals for the specified VLAN

```
# show mac-authentication login summary vlan

Date 2012/11/30 20:30:53 UTC
 Dynamic VLAN mode total client counts(Login/Max):   1 / 1000
  Authenticating client counts :    1
  Hold down client counts      :    1
  Port roaming : Disable
   No  VLAN  Login
    1  1000      1
```

```
 Static VLAN mode total client counts(Login/Max):    1 / 1024
  Authenticating client counts :    1
  Hold down client counts      :    1
  Port roaming : Disable
   No  VLAN  Login
    1   200      1

#
```

Display items 2

Table 28-8 Items displayed for a VLAN

Item	Meaning	Displayed detailed information
Dynamic VLAN mode total client counts	The number of currently authenticated terminals	`(Login / Max)`: The number of currently authenticated terminals / the maximum number of registered terminals set for the device
Static VLAN mode total client counts		
Authenticating client counts	The number of terminals on which authentication is being processed	--
Hold down client counts	The number of terminals on which authentication has been suspended	--
Port roaming	Roaming information	Changing of ports within the same VLAN. `Enable`: Enabled `Disable`: Disabled (default)
No	Entry number	The entry number for a currently authenticated terminal. This is just the displayed number, which changes depending on such factors as the filter conditions.
VLAN	VLAN ID	The VLAN ID in which the currently authenticated terminal exists
Login	The number of currently authenticated terminals	Number of currently authenticated terminals on the port

Impact on communication

None

Response messages

Table 28-9 List of response messages for the show mac-authentication login summary command

Message	Description
There is no information. (mac-auth login)	There is no information about the terminals that have been authenticated by MAC-based authentication.
MAC-Authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

Notes

None

show mac-authentication logging

Displays the operation log messages collected by the MAC-based authentication functionality.

Syntax

```
show mac-authentication logging [search <Search string>]
```

Input mode

Administrator mode

Parameters

search *<Search string>*

Specifies the search string.

If you specify this parameter, only information that includes the search string will be displayed.

Specify the string with 1 to 64 characters. The characters are case sensitive.

Operation when this parameter is omitted:

All the operation log messages output by MAC-based authentication are displayed.

Example

- When the parameter is omitted:

```
# show mac-authentication logging


Date 2011/09/15 09:56:48 UTC
AUT 09/15 09:55:13 MAC No=1002:NOTICE:LOGIN: MAC=00a0.b014.ccd8
PORT=0/9 VLAN=4000 Login aborted ; Port link down.
AUT 09/15 09:54:57 MAC No=267:NORMAL:SYSTEM: MAC=00a0.b014.ccd8 Stop
authenticating for MAC address. [107]
AUT 09/15 09:54:57 MAC No=265:NORMAL:SYSTEM: MAC=00a0.b014.ccd8 Start
authenticating for MAC address.
AUT 09/15 09:54:42 MAC No=84:NORMAL:SYSTEM: Accepted commit command.
AUT 09/15 09:54:05 MAC No=4:NORMAL:LOGOUT: MAC=00a0.b014.ccd8
PORT=0/20 VLAN=200 Force logout ; Clear mac-authentication command
succeeded.
AUT 09/15 09:54:05 MAC No=82:NORMAL:SYSTEM: Accepted clear auth-state
command.
AUT 09/15 09:53:42 MAC No=1:NORMAL:LOGIN: MAC=00a0.b014.ccd8 PORT=0/20
VLAN=200 Login succeeded.
AUT 09/15 09:53:42 MAC No=265:NORMAL:SYSTEM: MAC=00a0.b014.ccd8 Start
authenticating for MAC address.


#
```

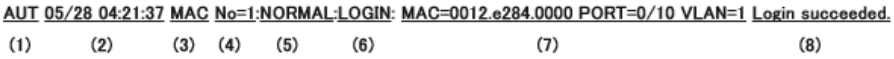
- Specifying `LOGOUT` for the parameter:

```
# show mac-authentication logging search "LOGOUT"
```

```
Date 2011/09/15 09:57:03 UTC

AUT 09/15 09:54:05 MAC No=4:NORMAL:LOGOUT: MAC=00a0.b014.ccd8
PORT=0/20 VLAN=200 Force logout ; Clear mac-authentication command
succeeded.


 1 event matched.


#
```

Display items

The following shows the display format of a message.



(1) Log functionality type: Indicates the type of authentication functionality. (Fixed at AUT.)

(2) Date and time: Indicates the date and time (*month*/*date* *hour*:*minute*:*second*) an event occurred.

(3) Authentication ID: Indicates MAC-based authentication.

(4) Message number: Indicates the number assigned to each message shown in *Table 28-12 List of operation log messages*.

(5) Log ID: Indicates the level of the operation log message.

(6) Log type: Indicates the type of operation that outputs the log message.

(7) Additional information: Indicates supplementary information provided in the message.

(8) Message body

Operation log messages show the following information:

- Log ID/Type: See *Table 28-10 Log ID and type in operation log messages*.
- Additional information: See *Table 28-11 Additional information*.
- Message list: See Table *Table 28-12 List of operation log messages*.

Table 28-10 Log ID and type in operation log messages

Log ID	**Log type**	Description
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 the attempt to cancel authentication failed.
	SYSTEM	Indicates an alternate operation when a communication failure occurs.
ERROR	SYSTEM	Indicates a communication failure or an

Log ID	Log type	Description
		operation failure in MAC-based authentication functionality.

Table 28-11 Additional information

Display format	Meaning
MAC=*xxxx.xxxx.xxxx*	Indicates the MAC address.
PORT=*xx/xx* CHGR=*x*	Indicates the port number or channel group number
VLAN=*xxxx*	Indicates the VLAN ID.

Table 28-12 List of operation log messages

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
1	NORMAL	LOGIN	Login succeeded.
	Dynamic VLAN Fixed VLAN		The terminal was successfully authenticated. [Action] None
			MAC, PORT or CHGR, VLAN[#2]
2	NORMAL	LOGOUT	Force logout ; Port link down.
	Dynamic VLAN Fixed VLAN		Authentication was canceled because the link for the relevant port went down. [Action] Make sure the status of relevant port is link-up.
			MAC, PORT or CHGR, VLAN[#2]

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
3	NORMAL	LOGOUT	Force logout ; Authentic method changed (RADIUS <-> Local).
	Dynamic VLAN Fixed VLAN		Authentication was canceled because the authentication methods were switched. This log data is collected when the setting of the following commands are changed: ● aaa authentication mac-authentication ● aaa authentication mac-authentication end-by-reject ● mac-authentication authentication [Action] None
			MAC, PORT or CHGR, VLAN[#2]
4	NORMAL	LOGOUT	Force logout ; Clear mac-authentication command succeeded.
	Dynamic VLAN Fixed VLAN		Authentication was canceled by an operation command. [Action] None
			MAC, PORT or CHGR, VLAN[#2]
5	NORMAL	LOGOUT	Force logout ; Connection time was beyond a limit.
	Dynamic VLAN Fixed VLAN		Authentication was canceled because the maximum connection time was exceeded. [Action] None (If the terminal is connected, authentication is attempted again.)
			MAC, PORT or CHGR, VLAN[#2]
6	NOTICE	LOGIN	Login failed ; Port link down.
	Fixed VLAN		Authentication error occurred because the port link was down. [Action] Make sure the status of relevant port is link-up.
			MAC, PORT or CHGR, VLAN

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
8	NOTICE	LOGIN	Login failed ; VLAN not specified.
	Dynamic VLAN		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, PORT or CHGR, VLAN[#2]
9	NORMAL	LOGOUT	Force logout ; Program stopped.
	Dynamic VLAN Fixed VLAN		The authentication of all terminals was canceled because the MAC-based authentication functionality stopped. [Action] To subsequently perform MAC-based authentication, set the configuration.
			MAC, PORT or CHGR, VLAN[#2]
10	NORMAL	LOGOUT	Force logout ; Other authentication program.
	Dynamic VLAN Fixed VLAN		Authentication was canceled because it was overwritten by another authentication operation. [Action] Make sure another authentication operation was not performed on the same terminal.
			MAC, PORT or CHGR, VLAN[#2]
11	NORMAL	LOGOUT	Force logout ; VLAN deleted.
	Dynamic VLAN Fixed VLAN		Authentication was canceled because the VLAN for the authentication port was changed. [Action] Check the configuration of the VLAN.
			MAC, PORT or CHGR, VLAN[#2]

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
12	NORMAL	LOGOUT	Force logout ; Client moved.
	Dynamic VLAN Fixed VLAN		The old authenticated state was canceled because the authenticated terminal was connected to another port. [Action] None Authentication is performed again.
			MAC, PORT or CHGR, VLAN[#2]
13	NOTICE	LOGIN	Login failed ; Double login. (L2MacManager)
	Dynamic VLAN Fixed VLAN		The VLAN functionality reported that authentication was not possible. ● 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 functionality that is currently authenticating the MAC address.
			MAC, PORT or CHGR, VLAN[#2]
15	NOTICE	LOGIN	Login failed ; Number of login was beyond limit.
	Dynamic VLAN Fixed VLAN		Authentication could not be performed because the number of logins exceeded the maximum allowable number. [Action] Attempt authentication again after the number of authentications decreases.
			MAC
18	NOTICE	LOGIN	Login failed ; MAC address could not register.
	Dynamic VLAN Fixed VLAN		Authentication could not be performed because registration of the MAC address failed. [Action] Attempt authentication again.
			MAC

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
20	NOTICE	LOGIN	Login failed ; RADIUS authentication failed.
	Dynamic VLAN Fixed VLAN		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, PORT or CHGR, VLAN[#2]
21	NOTICE	LOGIN	Login failed ; Failed to connection to RADIUS server.
	Dynamic VLAN Fixed VLAN		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, attempt authentication again.
			MAC, PORT or CHGR, VLAN[#2]
28	NORMAL	LOGOUT	Force logout ; Port not specified.
	Dynamic VLAN **Fixed VLAN**		Authentication was canceled because the setting was deleted from the port. [Action] Check the configuration.
			MAC, PORT or CHGR, VLAN[#2]
30	NORMAL	LOGOUT	Force logout ; mac-address-table aging.
	Dynamic VLAN Fixed VLAN		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, PORT or CHGR, VLAN[#2]

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
36	NOTICE	LOGIN	Login failed ; Number of login was beyond limit of port.
	Dynamic VLAN Fixed VLAN		Authentication cannot be performed because the maximum login limit for a port was exceeded. [Action] Reduce the number of terminals to be authenticated.
			MAC, PORT or CHGR, VLAN
37	NORMAL	LOGOUT	Force logout ; Number of login was beyond limit of port.
	Dynamic VLAN Fixed VLAN		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, PORT or CHGR, VLAN
82	NORMAL	SYSTEM	Accepted clear auth-state command.
	Dynamic VLAN Fixed VLAN		A notification issued by the `clear mac-authentication auth-state` command for forcibly canceling authentication was received. [Action] None
			--
83	NORMAL	SYSTEM	Accepted clear statistics command.
	Dynamic VLAN Fixed VLAN		A request issued by the `clear mac-authentication statistics` command to clear statistics was received. [Action] None
			--
84	NORMAL	SYSTEM	Accepted commit command.
	Dynamic VLAN Fixed VLAN		A commit notification issued by the `commit mac-authentication` command for re-configuring the authentication information was received. [Action] None

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
			--
99	ERROR	SYSTEM	Accounting failed ; RADIUS accounting.
	Dynamic VLAN Fixed VLAN		A response to an accounting request was not received from the RADIUS server. [Action] Check whether communication is available between the Switch and the RADIUS server. After the Switch can communicate with the RADIUS server, perform authentication again.
			MAC
105	NOTICE	LOGIN	Login failed ; VLAN suspended.
	Dynamic VLAN Fixed VLAN		An authentication error occurred because the status of the VLAN to be used for the terminal following a switch after authentication was suspended. [Action] After authentication, execute the `state` command to activate the VLAN, and then perform authentication again.
			MAC, PORT or CHGR, VLAN[#2]
106	NORMAL	LOGOUT	Force logout ; VLAN suspended.
	Dynamic VLAN Fixed VLAN		Authentication was canceled because the status of the VLAN for the authenticated terminal changed to suspend. [Action] After authentication, execute the `state` command to activate the VLAN, and then perform authentication again.
			MAC, PORT or CHGR, VLAN[#2]
107	NOTICE	LOGIN	Login failed ; MAC address not found to MAC authentication DB.
	Dynamic VLAN Fixed VLAN		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, VLAN[#1#2]

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
108	NOTICE	LOGIN	Login failed ; VLAN ID not found to MAC authentication DB.
	Fixed VLAN		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, VLAN
255	ERROR	SYSTEM	The other error.
	Dynamic VLAN Fixed VLAN		An internal MAC-based authentication error occurred. [Action] None
			--
256	NORMAL	LOGIN	Reauthentication succeeded.
	Dynamic VLAN Fixed VLAN		Re-authentication was successful. [Action] None
			MAC, PORT or CHGR, VLAN[#2]
258	NOTICE	LOGIN	Login failed ; Invalid attribute received from RADIUS server.
	Dynamic VLAN Fixed VLAN		Authentication failed because the attribute of an Accept packet received from the RADIUS server could not be analyzed. [Action] Check the RADIUS server settings.
			MAC, PORT or CHGR
261	NOTICE	LOGIN	Login failed ; Hardware restriction.
	Dynamic VLAN Fixed VLAN		Authentication could not be performed because the MAC address could not be registered due to hardware limitations. (There are no more available entries or hash entries) [Action] None
			MAC, PORT or CHGR

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
265	NORMAL	SYSTEM	Start authenticating for MAC address.
	Dynamic VLAN Fixed VLAN		Authentication processing has started. [Action] None
			MAC
266	NORMAL	SYSTEM	Restart authenticating for MAC address.
	Dynamic VLAN Fixed VLAN		Re-authentication processing has started. [Action] None
			MAC
267	NORMAL	SYSTEM	Stop authenticating for MAC address. [*error-code*]
	Dynamic VLAN Fixed VLAN		Authentication processing has stopped. [Action] See the action described in the log entry indicated by *error-code*.
			MAC, error code
268	NORMAL	SYSTEM	Received RADIUS server message. [*Message*]
	Dynamic VLAN Fixed VLAN		This is Reply-Message Attribute message sent from the RADIUS server (up to 80 characters are displayed). [Action] None
			Message
269	NORMAL	SYSTEM	Client port roaming.
	Dynamic VLAN Fixed VLAN		The terminal is roaming. [Action] None
			MAC, PORT or CHGR

No.	Log ID	Log type	Message text
	Authentication mode		**Description**
			Additional information
270	NOTICE	SYSTEM	MAC address was force-authorized.
	Dynamic VLAN Fixed VLAN		Forced authentication has started because an error occurred when a request was sent to the RADIUS server. [Action] None
			MAC, PORT or CHGR
280	NORMAL	LOGOUT	Force logout ; Multi-step finished.
	Dynamic VLAN Fixed VLAN		MAC-based authentication has been canceled because multistep authentication has completed. [Action] None
			MAC, PORT or CHGR, VLAN[#2]
282	NORMAL	LOGOUT	Force logout ; Authentic method changed (single <-> multi-step).
	Dynamic VLAN Fixed VLAN		Authentication for the port was canceled because of a switch between the single authentication and multistep authentication methods. [Action] None
			MAC, PORT or CHGR, VLAN[#2]
283	NORMAL	LOGIN	Login failed ; Number of table entry was beyond device limit.
	Dynamic VLAN Fixed VLAN		The authentication capacity limit of the switch was exceeded. [Action] Attempt authentication again after the number of authentications decreases.
			MAC
284	NOTICE	SYSTEM	Invalid user class. [*class*]
	Dynamic VLAN Fixed VLAN		The user class set for the RADIUS server is invalid. [Action] Review the RADIUS server setting.
			--

No.	Log ID	Log type	Message text
	Authentication mode		Description
			Additional information
1*xxx*	NOTICE	LOGIN	Login aborted ; *<cause of the stop>*
	See operation log message with the three digit number indicated.		Authentication processing has stopped. *xxx*: Operation log message number For details, see the descriptions of the indicated message number.

#1 Displayed when the mode is in fixed VLAN mode.

#2 For dynamic VLAN mode, the VLAN ID might not be displayed until the VLAN to be accommodated is decided.

Impact on communication

None

Response messages

Table 28-13 List of response messages for the show mac-authentication logging command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no logging data.	There is no log data.
There is no log data to match.	Log data matching the specified character string could not be found.
There is no memory.	There is not enough memory to collect data.

Notes

- MAC-based authentication operation log messages are displayed starting from the newer messages.
- If you execute this command with the `search` parameter set and if information that matches the specified character string exists, the number of matched operation log messages is displayed at the end.

  Example: 3 events matched.

clear mac-authentication logging

Clears the operation log information for MAC-based authentication.

Syntax

```
clear mac-authentication logging
```

Input mode

Administrator mode

Parameters

None

Example

The following shows an example of clearing the operation log information for MAC-based authentication:

```
# clear mac-authentication logging

#
```

Display items

None

Impact on communication

None

Response messages

Table 28-14 List of response messages for the clear mac-authentication logging command

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

Notes

None

show mac-authentication

Displays the configuration for MAC-based authentication.

Syntax

```
show mac-authentication
```

Input mode

Administrator mode

Parameters

None

Example

The following shows an example of displaying the configuration for MAC-based authentication:

```
# show mac-authentication

Date 2011/02/23 14:30:47 UTC
<<<MAC-Authentication mode status>>>
  Dynamic-VLAN     : Enable
  Static-VLAN      : Enable

<<<System configuration>>>
 * Authentication parameter
  Authentic-mode   : Dynamic-VLAN
  max-user         : 1024
  id-format type   : xx-xx-xx-xx-xx-xx
  password         : Disable
  vlan-check       : -
  roaming          : Disable

 * AAA methods
  Authentication Default       : RADIUS
  Authentication port-list-BBB : RADIUS ra-group-2
  Authentication End-by-reject : Disable
  Accounting Default           : RADIUS

 * Logout parameter
  max-timer        : infinity
  auto-logout      : 3600
  quiet-period     : 300
  reauth-period    : 3600

 * Logging status
  [Syslog send]    : Disable
  [Traps]          : Disable

<Port configuration>
  Port Count            : 2

  Port                  : 0/6
  VLAN ID               : 40
  Forceauth VLAN        : Disable
  Access-list-No        : L2-auth
  ARP relay             : Enable
  Max-user              : 1024
```

```
  Port                 : 0/22
  VLAN ID              : 40
  Forceauth VLAN       : Disable
  Access-list-No       : L2-auth
  ARP relay            : Enable
  Max-user             : 1024
  Authentication method : port-list-BBB

<<<System configuration>>>
 * Authentication parameter
  Authentic-mode   : Static-VLAN
  max-user         : 1024
  id-format type   : xx-xx-xx-xx-xx-xx
  password         : Disable
  vlan-check       : Disable
  roaming          : Disable

 * AAA methods
  Authentication Default       : RADIUS
  Authentication port-list-BBB : RADIUS ra-group-2
  Authentication End-by-reject : Disable
  Accounting Default           : RADIUS

 * Logout parameter
  max-timer        : infinity
  auto-logout      : 3600
  quiet-period     : 300
  reauth-period    : 3600

 * Logging status
  [Syslog send]    : Disable
  [Traps]          : Disable

<Port configuration>
  Port Count           : 3

  Port                 : 0/5
  VLAN ID              : 4
  Forceauth VLAN       : Disable
  Access-list-No       : L2-auth
  ARP relay            : Enable
  Max-user             : 1024
  Authentication method : port-list-BBB

  Port                 : 0/6
  VLAN ID              : 4
  Forceauth VLAN       : Disable
  Access-list-No       : L2-auth
  ARP relay            : Enable
  Max-user             : 1024

  Port                 : 0/22
  VLAN ID              : 4
  Forceauth VLAN       : Disable
  Access-list-No       : L2-auth
  ARP relay            : Enable
  Max-user             : 1024
  Authentication method : port-list-BBB

#
```

Display items

Table 28-15 Items displayed for the configuration of MAC-based authentication

Item	Meaning	Displayed detailed information	Mode	
			D	F
Dynamic-VLAN	Dynamic VLAN mode	Operating status of dynamic VLAN mode `Enable`: Enabled `Disable`: Disabled (If this item is `Disable`, the information that follows `<<<System configuration>>>` is not displayed.)	Y	N
Static-VLAN	Fixed VLAN mode	Operating status of fixed VLAN mode[#1] `Enable`: Enabled `Disable`: Disabled (If this item is `Disable`, the information that follows `<<<System configuration>>>` is not displayed.)	N	Y
* Authentication parameter				
Authentic-mode	Authentication mode	Authentication mode for the MAC-based authentication functionality. `Dynamic-VLAN`: Indicates dynamic VLAN mode `Static-VLAN`: Indicates fixed VLAN mode	Y	Y
max-user	Maximum number of authenticated terminals	The maximum number of authenticated terminals per device	Y	Y
id-format type	MAC address format	The MAC address format used when an authentication request is issued to the RADIUS server	Y	Y
password	Password	The password used when an authentication request is issued to the RADIUS server `Disable` is displayed when this item is disabled.	Y	Y
vlan-check	VLAN ID matching	VLAN ID matching in authentication `Enable`: Enabled `Disable`: Disabled	N	Y
key	Character string added to the user ID	A character string that is added to the user ID when an authentication request is issued to the RADIUS server. `%VLAN` is displayed if this item is not set.	N	Y
roaming	Roaming	Setting status for roaming `Enable`: Enabled `Disable`: Disabled	Y	Y
* AAA methods				
Authentication Default	Default authentication method on the Switch	`Local`: Indicates local authentication `RADIUS`: Indicates RADIUS authentication `Local, RADIUS`: RADIUS authentication after local authentication `RADIUS, Local`: Local authentication after RADIUS authentication	Y	Y

Item	Meaning	Displayed detailed information	Mode	
			D	F
		`Local` is displayed when this item is not set.		
Authentication *<List name>*	The list name and authentication method for the authentication method list	Displays the RADIUS server group name for the authentication method list. RADIUS *<Group name>* `RADIUS`: Indicates RADIUS authentication *<Group name>*: RADIUS server group name `(Not defined)` is displayed after the group name if the RADIUS server group name that has been set is invalid. This item is not displayed if it is not set.	Y	Y
Authenticaion End-by-reject	Operation of rejected authentication	`Enable`: Terminates authentication as error. The second method specified by the `aaa authentication mac-authentication` configuration command is used for authentication. `Disable` is displayed when this item is not set.	Y	Y
Accounting Default	Whether the accounting server is available	`RADIUS`: A general-use RADIUS server or RADIUS server dedicated to MAC-based authentication `Disable` is displayed when this item is not set.	Y	Y
* Logout parameter				
max-timer	Maximum connection time	The maximum connection time for an authenticated terminal (in minutes)	Y	Y
auto-logout	Whether forcible cancellation of authentication is enabled	Use of the functionality that forcibly cancels authentication by MAC address aging in MAC-based authentication dynamic VLAN mode `Disable` is displayed when this item is disabled.	Y	Y
quiet-period	Time waiting for an authentication retry	The time waiting after a MAC-based authentication failure for the start of the next authentication processing for the same terminal (MAC address) (in seconds)	Y	Y
reauth-period	Re-authentication time	The interval between re-authentication operations for the terminal after MAC-based authentication has been successful in dynamic VLAN mode (in seconds)	Y	Y
* Logging status				
[Syslog send]	syslog	Setting status of syslog information output `Enable`: Enabled `Disable`: Disabled	Y	Y
[Traps]	Traps	SNMP trap setting status `Disable` is displayed when this item is disabled.	Y	Y
Port Count	Total number of	Number of ports for which MAC-based authentication is	Y	Y

Item	Meaning	Displayed detailed information	Mode	
			D	F
	ports	enabled		
Port	Port information	Port number or channel group number (CH:*xx*)	Y	Y
VLAN ID	VLAN information	VLAN ID#2 registered in MAC-based authentication. `-` is displayed if this item has not been set.	Y	Y
Forceauth VLAN	Forced authentication	Setting status of forced authentication in dynamic VLAN mode#3 *xxxx*: Enabled. *xxxx* indicates the VLAN ID set in configuration. `VLAN unmatch`: Invalid due to an insufficient setting `Disable`: Disabled (default)	Y	N
		Setting status of forced authentication in fixed VLAN mode `Enable`: Enabled `Disable`: Disabled	N	Y
Access-list-No	Access Lists	Setting status of authentication IP access-group `Disable` is displayed if this item is not set.	Y	Y
Arp relay	ARP relay	Setting status of authentication arp-relay `Enable`: Enabled `Disable`: Disabled	Y	Y
Max-user	Maximum number of authenticated terminals	The maximum number of authentication terminals for each port	Y	Y
Authentication method	Authentication list name for the port-based authentication method	Displays the name of the authentication method list registered for each port. ● `(Not defined)` is displayed after the authentication method list name if the set authentication method list name is invalid. ● This item is not displayed if it is not set.	Y	Y

Legend:

D: Dynamic VLAN mode

F: Fixed VLAN mode

Y: Applicable

N: Not applicable (`-` is also displayed on the screen)

#1 For details about the conditions for enabling the operating status, see *11.1.2 Configuration procedure for MAC-based authentication* in the *Configuration Guide Vol. 2*.

#2 VLAN IDs registered by automatic VLAN assignment are not displayed.

However, VLAN IDs are displayed if they are accommodated in the native VLAN (fixed) as the result of automatic VLAN assignment.

#3 `native vlan` is displayed if the `authentication force-authorized enable` command is enabled and the `authentication force-authorized vlan` command is not set.

Impact on communication

None

Response messages

Table 28-16 List of response messages for the show mac-authentication command

Message	Description
MAC-Authentication is not configured.	The MAC-based authentication functionality 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

Example

The following shows an example of displaying MAC-based authentication statistics:

```
# show mac-authentication statistics

Date 2010/08/05 13:23:41 UTC
MAC-Authentication Information:
  Authentication Request Total :         56
  Authentication Success Total :         32
  Authentication Fail Total    :         24
  Authentication Refuse Total  :         21
  Authentication Current Count :          1
  Authentication Current Fail  :          1

RADIUS MAC-Authentication Information:
[RADIUS frames]
  TxTotal   :        52  TxAccReq  :        52  TxError   :         0
  RxTotal   :        38  RxAccAccpt:        16  RxAccRejct:        22
                         RxAccChllg:         0  RxInvalid :         0
Account MAC-Authentication Information:
[Account frames]
  TxTotal   :        22  TxAccReq  :        22  TxError   :         0
  RxTotal   :        20  RxAccResp :        20  RxInvalid :         0

#
```

Display items

Table 28-17 Items displayed for MAC-based authentication statistics

Item	Meaning
Authentication Request Total	The total number of authentication requests
Authentication Success Total	The total number of authenticated MAC addresses
Authentication Fail Total	The total number of MAC addresses for which authentication failed
Authentication Refuse Total	The total number of MAC addresses for which authentication was rejected
Authentication Current Count	The number of currently authenticated MAC addresses

Item	Meaning
Authentication Current Fail	The number of MAC addresses for which authentication has failed (waiting for re-authentication)
RADIUS frames	RADIUS server information
TxTotal	The total number of transmissions 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 receptions 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 transmitted 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

None

Impact on communication

None

Response messages

Table 28-18 List of response messages for the show mac-authentication statistics command

Message	Description
MAC-Authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

Notes

None

clear mac-authentication statistics

Clears the MAC-based authentication statistics.

Syntax

```
clear mac-authentication statistics
```

Input mode

Administrator mode

Parameters

None

Example

The following shows an example of clearing MAC-based authentication statistics:

```
# clear mac-authentication statistics

#
```

Display items

None

Impact on communication

None

Response messages

Table 28-19 List of response messages for the clear mac-authentication statistics command

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

Notes

None

set mac-authentication mac-address

Adds a MAC address for MAC-based authentication to the internal MAC-based authentication DB. A MAC mask and a VLAN ID to which the MAC address belongs can also be specified. You can add a MAC address that has already been registered if its MAC mask or VLAN ID is different from the registered MAC address.

To check the editing or registration status, execute the `show mac-authentication mac-address` command.

To apply the setting to the internal MAC-based authentication DB, execute the `commit mac-authentication` command.

Syntax

```
set mac-authentication mac-address <MAC> [<MAC mask>] [<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).

<MAC mask>

Specify in MAC address format a MAC address mask in which you set the bits that you want to allow any value set to 1.

Specify the MAC address mask in the range from `0000.0000.0000` to `ffff.ffff.ffff`.

Operation when this parameter is omitted:

The MAC mask becomes `0000.0000.0000`.

Specification of `ffff.ffff.ffff` as the MAC mask:

All MAC addresses are applied.

Specify `0000.0000.0000` for the MAC address and `ffff.ffff.ffff` for the MAC mask.

Only one entry can be registered for this condition. If an entry in this condition has already been registered, registering a new entry overwrites the old one.

<VLAN ID>

Specify the VLAN ID of the VLAN to which the terminal will communicate after authentication. For details about the specifiable range of values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

The VLAN ID is not checked at authentication time.

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
```

- Adding `0012.e2` as the vender ID and `0000.00ff.ffff` as the MAC mask:

```
# set mac-authentication mac-address 0012.e200.0000 0000.00ff.ffff 10
```

- Adding `ffff.ffff.ffff` as the MAC mask:

```
# set mac-authentication mac-address 0000.0000.0000 ffff.ffff.ffff 1
```

Display items

None

Impact on communication

None

Response messages

Table 28-20 List of response messages for the set mac-authentication mac-address command

Message	Description
Already mac address xxxx.xxxx.xxxx,dddd exists.	The specified MAC address has already been registered. *xxxx.xxxx.xxxx*: MAC address *dddd*: VLAN ID (If `0` is displayed, no VLAN ID is set.)
Already mac address xxxx.xxxx.xxxx(nnnn.nnnn.nnnn),dddd exists.	The specified MAC address has already been registered. *xxxx.xxxx.xxxx*: MAC address *nnnn.nnnn.nnnn*: MAC mask *dddd*: VLAN ID (If `0` is displayed, no VLAN ID is set.)
The number of client exceeds limits.	A MAC address could not be added because the number of entries exceeded the maximum number of entries allowed for the internal MAC-based authentication DB.
MAC-Authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

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.
- You can register a MAC address that has already been registered if its MAC mask or VLAN ID is different from the registered MAC address.

remove mac-authentication mac-address

Deletes MAC addresses, for MAC-based authentication, from the internal MAC-based authentication DB.

All entries specified by the MAC address and MAC mask (if registered) are deleted, (including when there are different VLAN IDs).

To check the editing or registration status, execute the `show mac-authentication mac-address` command.

To apply the setting to the authentication information, execute the `commit mac-authentication` command.

Syntax

```
remove mac-authentication mac-address {<MAC> [<MAC mask>] | -all} [-f]
```

Input mode

Administrator mode

Parameters

{*<mac>* [*<MAC mask>*] | -all}

<MAC>

Specify the MAC address to be deleted.

<MAC mask>

Specify the MAC mask for the MAC address to be deleted.

Operation when this parameter is omitted:

The specified MAC address (no MAC mask) is deleted.

To delete the MAC mask entry `ffff.ffff.ffff`:

Specify `0000.0000.0000` for the MAC address and `ffff.ffff.ffff` for the MAC mask.

-all

Deletes all MAC addresses.

-f

Deletes MAC addresses without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

- When deleting 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
```

- Deleting all MAC addresses registered in the internal MAC-based authentication DB:

```
# remove mac-authentication mac-address -all
Remove all mac-authentication mac-address.  Are you sure? (y/n): y
```

- Deleting the MAC mask `ffff.ffff.ffff`:

```
# remove mac-authentication mac-address 0000.0000.0000 ffff.ffff.ffff
Remove mac-authentication mac-address.  Are you sure? (y/n): y
```

Display items

None

Impact on communication

None

Response messages

Table 28-21 List of response messages for the remove mac-authentication mac-address command

Message	Description
Unknown MAC address 'xxxx.xxxx.xxxx'.	The MAC address has not been registered. (when a single MAC address is specified) *xxxx.xxxx.xxxx*: MAC address
Unknown MAC address 'xxxx.xxxx.xxxx(nnnn.nnnn.nnnn)'.	The MAC address has not been registered. (when a single MAC address is specified) *xxxx.xxxx.xxxx*: MAC address *nnnn.nnnn.nnnn*: MAC mask
MAC address does not exist.	The MAC address has not been registered. (when the `-all` parameter is specified)
MAC-Authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

Notes

- The setting is applied to the internal MAC-based authentication DB only when the `commit mac-authentication` command is executed.
- MAC addresses that are not the same as registered addresses cannot be deleted.

show mac-authentication mac-address

Displays information about the MAC addresses for MAC-based authentication that are registered in a Switch. 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 by MAC address. Entries with no MAC mask information are displayed first, followed by the entries with MAC mask information.

Syntax

```
show mac-authentication mac-address {edit | commit}
```

Input mode

Administrator mode

Parameters

{edit | commit}

edit

Displays information that is being edited.

commit

Displays information about the current internal MAC-based authentication DB.

Example

- When displaying information that is being edited:

```
# show mac-authentication mac-address edit

Date 2010/09/13 18:02:43 UTC
 Total mac-address counts: 5
 mac-address     mac-mask          VLAN
 0012.e200.1234  -                 4094
 0012.e200.abcd  -                    4
 0012.e200.1234  0000.0000.ffff      10
 0012.e200.abcd  0000.0000.ffff       8
 (any)           ffff.ffff.ffff       1 *

#
```

*: If an entry has been registered as `(any)`, it always appears at the end.

- When displaying information about the current internal MAC-based authentication DB:

```
# show mac-authentication mac-address commit

Date 2010/09/13 18:02:48 UTC
 Total mac-address counts: 3
```

```
mac-address     mac-mask          VLAN
0012.e200.1234  -                 4094
0012.e200.abcd  -                    4
0012.e200.1234  0000.0000.ffff      10

#
```

Display items

Table 28-22 Items displayed for the MAC address information for MAC-based authentication

Item	Meaning	Displayed detailed information
Total mac-address counts	The total number of registered MAC addresses	The number of registered MAC addresses
mac-address	MAC address	Registered MAC address `(any)`: An entry registered with `0000.0000.0000` specified for the MAC address and `ffff.ffff.ffff` specified for the MAC mask
mac-mask	MAC mask	The registered MAC mask `-`: Indicates that a MAC mask has not been specified, in which case `0000.0000.0000` is used.
VLAN	VLAN	The VLAN set for a registered MAC address. `-`: Indicates that a VLAN has not been specified.

Impact on communication

None

Response messages

Table 28-23 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.
There is no information. (edit)	There was no information in the edit area of the internal MAC-based authentication DB.
There is no information. (commit)	There was no information in the commit area of the internal MAC-based authentication DB.
MAC-Authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

Notes

None

commit mac-authentication

Stores the internal MAC-based authentication DB in internal flash memory and reflects its contents for operation.

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 in internal flash memory and reflects its contents for operation. No confirmation message is displayed.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

The following shows an example of storing the internal MAC-based authentication DB:

```
# 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 28-24 List of response messages for the commit mac-authentication command

Message	Description
Commit complete.	Storing the DB in internal flash memory and reflecting its contents for MAC-based authentication finished normally.
Flash memory write failed.	Writing of the information to internal flash memory failed.

Message	Description
MAC-Authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

Notes

The information in the internal MAC-based authentication DB which is being used is modified only when this command is executed.

store mac-authentication

Backs up the internal MAC-based authentication DB to files.

Syntax

```
store mac-authentication ramdisk <File name> [-f]
```

Input mode

Administrator mode

Parameters

ramdisk

Backs up the internal MAC-based authentication DB to files on the RAMDISK.

<File name>

Specify the name of a file to which the internal MAC-based authentication DB is to be backed up.

Two backup files, one which contains MAC mask information and the other which does not, are created on the RAMDISK.

The file names are as follows:

File that does not contain MAC mask information: *<File name>*

File that contains MAC mask information: *<File name>*`.msk`

Specify the file name with 60 or fewer characters.

For the characters that can be specified, see *Specifiable values for parameters.*

-f

Backs up the internal MAC-based authentication DB to files without displaying confirmation messages.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

Backing up the internal MAC-based authentication DB to the `mac-db.txt` file:

```
# store mac-authentication ramdisk mac-db.txt
Backup mac-authentication MAC address data.  Are You sure? (y/n): y

Backup complete.
#
```

Display items

None

Impact on communication

None

Response messages

Table 28-25 List of response messages for the store mac-authentication command

Message	Description
Backup complete.	A backup file has been created successfully.
Store operation failed.	The command could not be executed because of insufficient RAMDISK capacity.
Command information was damaged.	A backup file could not be generated because the authentication information was corrupted.
Data doesn't exist.	A backup file could not be generated. A commit operation might not have been executed. Execute a commit operation, and then check the result. If the commit operation fails again, the internal flash memory might be corrupted.
MAC-Authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

Notes

- If the internal MAC-based authentication DB is backed up when the RAMDISK capacity is insufficient, incomplete backup files might be created.

  When creating backup files, use the `show ramdisk` command to make sure there is enough free capacity on the RAMDISK.

  The following is an example of executing the `show ramdisk` command:

```
> show ramdisk

Date 2010/08/06 17:38:36 UTC
       used       152,576 byte
       free    31,304,704 byte
       total   31,457,280 byte

>
```

  Note: The underlined part (the value for `free` indicating the free capacity of the user area) must be at least 200kB.

- If the free capacity on the RAMDISK is insufficient, use the `del` 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 ramdisk <File name> [-f]
```

Input mode

Administrator mode

Parameters

ramdisk

Restores the internal MAC-based authentication DB from a backup file on the RAMDISK.

<File name>

Specify the name of the backup file from which the internal MAC-based authentication DB is to be restored.

Specify the file name with 64 or fewer characters.

For the characters that can be specified, see *Specifiable values for parameters.*

-f

Restores the internal MAC-based authentication DB without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

Restoring the internal MAC-based authentication DB from the `mac-db.txt` file:

```
# load mac-authentication ramdisk mac-db.txt
Restore mac-authentication MAC address data.  Are you sure? (y/n): y

Restore complete.
#
```

Display items

None

Impact on communication

None

Response messages

Table 28-26 List of response messages for the load mac-authentication command

Message	Description
Restore complete.	Restoration from the backup file was successful.
Load operation failed.	Restoration from the backup file failed.
File format error.	The format of the specified backup file is different from the internal MAC-based authentication DB.
Flash memory write failed.	Writing of the information to internal flash memory failed.
MAC-Authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

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

29. Multistep Authentication

show authentication multi-step

show authentication multi-step

Displays the information for authenticated terminals on a multistep authentication port for an interface.

Syntax

```
show authentication multi-step [{port <IF#> | channel-group-number <Channel group#>}]
[mac <MAC>]
```

Input mode

Administrator mode

Parameters

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

port *<IF#>*

Specify the number of the interface for which you want to display the multistep authentication progress.

channel-group-number *<Channel group#>*

Specify the number of the channel group for which you want to display the multistep authentication progress.

Operation when this parameter is omitted:

The progress of multistep authentication is displayed for all MAC addresses.

mac *<MAC>*

Specify the MAC address for which you want to display multistep authentication progress.

Operation when this parameter is omitted:

The progress of multistep authentication is displayed for all MAC addresses.

Example

Figure 29-1 Displaying the progress of multistep authentication

```
# show authentication multi-step

Date 2012/11/29 11:36:36 UTC
Port 0/8  : multi-step permissive
     <     Supplicant information     >  <Authentic method>
  No MAC address    State VLAN F Type   class  Last  (first step)
   1 0025.64c2.4725 pass   200   multi     60  web   (mac)

Port 0/48 : multi-step permissive
     <     Supplicant information     >  <Authentic method>
  No MAC address    State VLAN F Type   class  Last  (first step)
   1 000a.e460.af52 pass   200   single    24  mac   (-)

#
```

Display items

Table 29-1 Information displayed for authenticated terminals on a multistep authentication port

Item	Meaning	Displayed detailed information
Port	Port number or channel group number	Displayed only when an authentication entry exists on the multistep authentication port.
<port status>	multi-step	User authentication is not permitted if MAC-based authentication fails.
	multi-step permissive	The `permissive` option has been set and user authentication is permitted even if MAC-based authentication fails.
	multi-step dot1x	The `dot1x` option has been set and Web authentication is not permitted if MAC-base or IEEE 802.1x authentication fails.
No	Terminal display number	Terminal display number for each port
<Supplicant information>	Authentication terminal information	--
MAC address	MAC address	The MAC address of the terminal on which authentication is being processed.
State	Authentication status	`wait`: A new terminal is being authenticated. `pass`: Single authentication or multistep authentication has been completed. This status is displayed when re-authentication is in progress or when the authentication time is being updated.
VLAN	VLAN ID of the VLAN that accommodates a terminal	`1` to `4094`: Indicates a VLAN ID. For multistep authentication, the result of user authentication has priority for determining the VLAN ID of the VLAN that will actually accommodate the terminal. `-` is displayed if the VLAN accommodating the terminal has not been identified because authentication has not been completed.
F	Forced authentication indication	*: The terminal that was logged in by using the forced authentication functionality. If a request is sent to the RADIUS server for processing such as re-authentication and the RADIUS server accepts the request, the displayed asterisk (`*`) disappears.

Item	Meaning	Displayed detailed information
Type	Step authentication type	`single`: The terminal has been authenticated in single authentication mode. `multi`: The terminal has been authenticated in multistep authentication mode. `-` is displayed if the authentication type has not been identified because the authentication processing has not been completed.
Class	User class	The user class is displayed. However, `-` is displayed in the following cases: ● No user class is specified. ● The user class is unknown because the authentication is not yet complete. ● It is the first step of authentication
<Authentic method>	Authentication functionality information	--
Last	Final authentication functionality	Displays the authentication functionality used for final authentication of the terminal. `mac`: MAC-based authentication `web`: Web authentication `dot1x`: IEEE 802.1X `-` is displayed if the final authentication processing has not been completed.
(first step)	First step authentication functionality	For the multistep authentication terminal, this item displays the authentication functionality used for the first step. `(mac)`: MAC-based authentication `(dot1x)`: IEEE 802.1X `-` is displayed if there is no awareness of authentication.

Impact on communication

None

Response messages

Table 29-2 List of response messages for the show authentication multi-step command

Message	Description
There is no information. (authentication multi-step)	There is no authenticated terminal information on the multistep authentication port.
Authentication multi-step is not configured.	The multistep authentication functionality has not been configured. Check the configuration.

Notes

None

30. Secure Wake-on-LAN [OS-L2A]

set wol-device name [OS-L2A]
set wol-device mac [OS-L2A]
set wol-device vlan [OS-L2A]
set wol-device ip [OS-L2A]
set wol-device alive [OS-L2A]
set wol-device description [OS-L2A]
remove wol-device name [OS-L2A]
show wol-device name [OS-L2A]
commit wol-device [OS-L2A]
store wol-device [OS-L2A]
load wol-device [OS-L2A]
set wol-authentication user [OS-L2A]
set wol-authentication password [OS-L2A]
set wol-authentication permit [OS-L2A]
remove wol-authentication user [OS-L2A]
show wol-authentication user [OS-L2A]
commit wol-authentication [OS-L2A]
store wol-authentication [OS-L2A]
load wol-authentication [OS-L2A]
wol [OS-L2A]
show wol [OS-L2A]

set wol-device name [OS-L2A]

Registers information about a new terminal that sends the startup command for Secure Wake-on-LAN. The information is registered in the internal DB used to register the terminal that sends the startup command.

To apply the setting to the terminal information, execute the `commit wol-device` command.

Syntax

```
set wol-device name <Name> <MAC> <VLAN ID>[ip <IP address> ][ alive {check [timeout
<Seconds>] | nocheck} ][ description <Description> ]
```

Input mode

Administrator mode

Parameters

< Name>

Specify a terminal name.

Specify 1 to 128 characters. You can use alphanumeric characters (case sensitive), at marks (`@`), hyphens (`-`), underscores (`_`), and periods (`.`).

<MAC>

Specify the 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).

<VLAN ID>

Specify the VLAN ID of the VLAN to which the terminal will belong. For details about the specifiable range of values, see *Specifiable values for parameters*.

ip *<IP address>*

Directly specify the IP address of the terminal in a static IP address environment.

Specify the IP address in the range from `1.0.0.0` to `126.255.255.255` or from `128.0.0.0` to `223.255.255.255`.

Operation when this parameter is omitted:

DHCP is used. In a DHCP environment, an IP address is set in conjunction with DHCP snooping.

alive

Sets verification that the terminal is still activated.

check [timeout *<Seconds>*]

Verifies that the terminal is still activated.

timeout *<Seconds>*

Sets the interval for verifying terminal activation. Specify an interval from 60 to 600 seconds.

Operation when this parameter is omitted:

The verification interval is set to 120 seconds.

nocheck

Sets that verification of terminal activation is not performed.

description *<Description>*

Sets supplementary information about the terminal.

Specify 1 to 128 characters. You can use alphanumeric characters (case sensitive), at marks (@), hyphens (-), underscores (_), and periods (.).

Operation when this parameter is omitted:

No supplementary information is provided.

Example

Registering a new terminal PC01:

```
# set wol-device name PC01 1234.5678.9abc 1000 ip 192.168.100.100 alive check
timeout 600 description Commom-NotePC@example.com
```

Display items

None

Impact on communication

None

Response messages

Table 30-1 List of response messages for the set wol-device name command

Message	Description
Already device '*<Name>*' exists.	The specified terminal has already been registered.
The number of devices exceeds 300.	The number of terminals to be registered exceeds 300.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- To check the registered terminal information, execute the `show wol-device name` command.
- The maximum number of terminals that can be registered is 300.
- If the `alive nocheck` parameter is specified, the address information specified for the `ip` parameter is invalid.
- This command can be applied to a new terminal. To change the setting, use another `set wol-device` command.

set wol-device mac [OS-L2A]

Changes the MAC address of the terminal information that has been registered.

To apply the setting to the terminal information, execute the `commit wol-device` command.

Syntax

```
set wol-device mac <Name> <MAC>
```

Input mode

Administrator mode

Parameters

< Name>

Specify the name of the terminal whose MAC address is to be changed.

<MAC>

Specify a new 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).

Example

Changing the MAC address for terminal `PC01`:

```
# set wol-device mac PC01 0012.ee86.6fd4
```

Display items

None

Impact on communication

None

Response messages

Table 30-2 List of response messages for the set wol-device mac command

Message	Description
Unknown device '*<Name>*'.	The specified terminal name has not been registered.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- Before execution of this command, terminal information must be registered by the `set wol-device name` command.

set wol-device vlan [OS-L2A]

Changes the VLAN ID in the terminal information that has been registered.

To apply the setting to the terminal information, execute the `commit wol-device` command.

Syntax

```
set wol-device vlan <Name> <VLAN ID>
```

Input mode

Administrator mode

Parameters

< Name>

Specify the name of the terminal whose VLAN ID is to be changed.

<VLAN ID>

Changes the VLAN ID of the VLAN to which the terminal will belong. For details about the specifiable range of values, see *Specifiable values for parameters*.

Example

Changing the VLAN ID for terminal `PC01`:

```
# set wol-device vlan PC01 4094
```

Display items

None

Impact on communication

None

Response messages

Table 30-3 List of response messages for the set wol-device vlan command

Message	Description
Unknown device '*<Name>*'.	The specified terminal name has not been registered.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- Before execution of this command, terminal information must be registered by the `set wol-device name` command.

set wol-device ip [OS-L2A]

Changes the IP address and method used to identify the IP address in the terminal information that has been registered.

To apply the setting to the terminal information, execute the `commit wol-device` command.

Syntax

```
set wol-device ip <Name> {<IP address> | dhcp}
```

Input mode

Administrator mode

Parameters

< Name>

Specify the name of the terminal whose IP address information is to be changed.

{*<IP address>* | dhcp}

<IP address>

Directly specify the IP address of the terminal in a static IP address environment.

Specify the IP address in the range from `1.0.0.0` to `126.255.255.255` or from `128.0.0.0` to `223.255.255.255`.

dhcp

In a DHCP environment, an IP address is set in conjunction with DHCP snooping.

Example

Changing the IP address for terminal `PC01`:

```
# set wol-device ip PC01 202.68.133.72
```

Display items

None

Impact on communication

None

Response messages

Table 30-4 List of response messages for the set wol-device ip command

Message	Description
Unknown device '*<Name>*'.	The specified terminal name has not been registered.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.

- Before execution of this command, terminal information must be registered by the `set wol-device name` command.
- If the `alive nocheck` parameter is specified, the address information specified for the `ip` parameter is invalid.

set wol-device alive [OS-L2A]

Changes the method for verifying terminal activation in the information that has been registered.

To apply the setting to the terminal information, execute the `commit wol-device` command.

Syntax

```
set wol-device alive <Name> {check [timeout <Seconds>] | nocheck}
```

Input mode

Administrator mode

Parameters

< Name>

Specify the name of the terminal whose setting for activation verification method is to be changed.

check [timeout *<Seconds>*]

Verifies that the terminal is still activated.

timeout *<Seconds>*

Sets the interval for verifying terminal activation. Specify an interval from 60 to 600 seconds.

Operation when this parameter is omitted:

The verification interval is set to 120 seconds.

nocheck

Sets that verification of terminal activation is not performed.

Example

Changing the interval for verifying activation of terminal `PC01`:

```
# set wol-device alive PC01 check timeout 300
```

Display items

None

Impact on communication

None

Response messages

Table 30-5 List of response messages for the set wol-device alive command

Message	Description
Unknown device '*<Name>*'.	The specified terminal name has not been registered.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- Before execution of this command, terminal information must be registered by the `set wol-device name` command.
- If the `alive nocheck` parameter is specified, the address information specified for the `ip` parameter is invalid.

set wol-device description [OS-L2A]

Changes the supplementary information in the terminal information that has been registered.

To apply the setting to the terminal information, execute the `commit wol-device` command.

Syntax

```
set wol-device description <Name> [<Description>]
```

Input mode

Administrator mode

Parameters

< Name>

Specify the name of the terminal whose supplementary information is to be changed.

<Description>

Enter the new supplementary information.

Specify 1 to 128 characters. You can use alphanumeric characters (case sensitive), at marks (`@`), hyphens (`-`), underscores (`_`), and periods (`.`).

Operation when this parameter is omitted:

The supplementary information is deleted.

Example

Changing the supplementary information for terminal `PC01`:

```
# set wol-device description PC01 change-user
```

Display items

None

Impact on communication

None

Response messages

Table 30-6 List of response messages for the set wol-device description command

Message	Description
Unknown device '*<Name>*'.	The specified terminal name has not been registered.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- Before execution of this command, terminal information must be registered by the `set wol-device name` command.

remove wol-device name [OS-L2A]

Deletes the terminal information that has been registered.

To apply the setting to the terminal information, execute the `commit wol-device` command.

Syntax

```
remove wol-device name {<Name> | -all} [-f]
```

Input mode

Administrator mode

Parameters

{*<Name>* | -all}

< Name>

Specify the name of the terminal to be deleted.

-all

Deletes all terminal information.

-f

Deletes the terminal information without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

- Deleting terminal `DEVICE01`:

```
# remove wol-device name PC01
Remove wol-device name.  Are you sure? (y/n): y
```

- Deleting all terminal information that has been registered in the internal DB used to register the terminal that sends the startup command:

```
# remove wol-device name -all
Remove all wol-device name.  Are you sure? (y/n): y
```

Display items

None

Impact on communication

None

Response messages

Table 30-7 List of response messages for the remove wol-device name command

Message	Description
Unknown device '*<Name>*'.	The specified terminal name has not been registered. (when a single MAC address is specified)

Message	Description
Device does not exist.	The terminal information does not exist. (when `-all` is specified)
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.

show wol-device name [OS-L2A]

Displays the terminal information that has been registered in the internal DB used to register the terminal that sends the startup command. This command can also display user information that is being entered or edited by using the following commands:

- `set wol-device name` command
- `set wol-device mac` command
- `set wol-device vlan` command
- `set wol-device ip` command
- `set wol-device alive` command
- `set wol-device description` command
- `remove wol-device name` command

Syntax

```
show wol-device name {edit | commit} [device-name <Name>] [detail]
```

Input mode

Administrator mode

Parameters

{ edit | commit }

edit

Displays the terminal information being edited.

commit

Displays information about the terminals being operated.

device-name <*Name*>

Specify a terminal name.

If the specified character string partly matches a terminal name that has been registered, the relevant terminal information is displayed.

Specify 1 to 128 characters. You can use alphanumeric characters (case sensitive), at marks (`@`), hyphens (`-`), underscores (`_`), and periods (`.`).

Operation when this parameter is omitted:

All terminal information is displayed.

detail

Displays detailed information about the terminals that are being edited or operated.

Operation when this parameter is omitted:

Detailed information is not displayed.

Example 1

- Displaying the terminal information being edited:

```
# show wol-device name edit

Date 2010/09/06 14:48:49 UTC
 Total device counts:   5
  No Device name  MAC         VLAN IP address     Alive   Description
```

```
 1 PC01       0012.ee86.6fd4 4094 202.68.133.72  300    change-user
 2 PC02       00ee.16fd.a142  100 10.1.10.10    600    all-user-...
 3 PC03_High...  0022.fa12.34dd   10 dhcp         60     High_price
 4 PC04          04ff.d423.f145    5 dhcp           120
 5 PC05         0612.7faf.1fdd 2000 202.68.133.70   no-check notePC

#
```

Display items in Example 1

Table 30-8 Items displayed for the terminal information

Item	Meaning	Displayed detailed information
Total device counts	Number of registered terminals	Maximum of 300 terminals
No	Entry number	Maximum of 300 entries
Device name	Terminal name	Up to 12 characters are displayed. (If the name exceeds 12 characters, part of the name is omitted and replaced with three periods (`...`). The full name can be checked in detailed information.)
MAC	MAC address	--
VLAN	VLAN ID	--
IP address	IP addresses	`dhcp` is displayed if the IP address has been set via DHCP.
Alive	Time for verifying activation (seconds)	Displays the interval used to verify activation. `no-check` is displayed if activation verification is not performed.
Description	Supplementary explanation	Up to 12 characters are displayed. (If the name exceeds 12 characters, part of the name is omitted and replaced with three periods (`...`). The full name can be checked in detailed information.) This item is not displayed if it has not been set.

Example 2

Figure 30-1 Example of displaying detailed terminal information:

```
# show wol-device name edit detail

Date 2010/09/06 14:58:27 UTC
 No    1 : PC01
  MAC: 0012.ee86.6fd4,  VLAN: 4094
  IP address: 202.68.133.72,  Alive: check  Timeout: 300(s)
  Description: change-user

 No    2 : PC02
  MAC: 00ee.16fd.a142,  VLAN: 100
  IP address: 10.1.10.10,  Alive: check  Timeout: 600(s)
```

```
 Description: all-user-backup

No    3 : PC03_High-Speed_machine
 MAC: 0022.fa12.34dd,  VLAN: 10
 IP address: dhcp,  Alive: check  Timeout: 60(s)
 Description: High_price

No    4 : PC04
 MAC: 04ff.d423.f145,  VLAN: 5
 IP address: dhcp,  Alive: check  Timeout: 120(s)
 Description:

No    5 : PC05
 MAC: 0612.7faf.1fdd,  VLAN: 2000
 IP address: 202.68.133.70,  Alive: no-check
 Description: notePC

#
```

Display items in Example 2

Table 30-9 Items displayed for the detailed terminal information

Item	Meaning	Displayed detailed information
No	Entry number	Maximum of 300 entries
	Terminal name	--
MAC	MAC address	--
VLAN	VLAN ID	--
IP address	IP addresses	`dhcp` is displayed if the IP address has been set via DHCP.
Alive	Time for verifying activation (seconds)	Displays the interval used to verify activation. `no-check` is displayed if activation verification is not performed.
Description	Supplementary explanation	Displays supplementary information about the terminal. This item is not displayed if it has not been set.

Impact on communication

None

Response messages

Table 30-10 List of response messages for the show wol-device name command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no information. (edit)	There was no information in the edit area of the internal DB.

Message	Description
There is no information. (commit)	There was no information in the commit area of the internal DB.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.

commit wol-device [OS-L2A]

Stores the edited terminal information in internal flash memory and reflects its contents for operation.

Syntax

```
commit wol-device [-f]
```

Input mode

Administrator mode

Parameters

-f

Stores the edited terminal information in internal flash memory and reflects its contents for operation. A confirmation message is not displayed.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

Example of storing the internal DB used to register the terminal that sends the startup command:

```
# commit wol-device
Commitment wol-device name data.  Are you sure? (y/n): y

Commit complete.
#
```

Display items

None

Impact on communication

None

Response messages

Table 30-11 List of response messages for the commit wol-device command

Message	Description
Commit complete.	Storing the information to internal flash memory and reflecting its contents for Secure Wake-on-LAN finished normally.
Flash memory write failed.	Writing of the information to internal flash memory failed.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- For current users of the terminal, the execution results are applied from the next login. (Even if the information for the terminal being used has been deleted, the user

can continue to use the terminal.)

store wol-device [OS-L2A]

Creates a backup file of the internal DB used to register the terminal that sends the startup command.

Syntax

```
store wol-device ramdisk <File name> [-f]
```

Input mode

Administrator mode

Parameters

ramdisk

Creates on the RAMDISK a backup file of the internal DB used to register the terminal that sends the startup command.

<File name>

Specify the name of the file to which the internal DB used to register the terminal that sends the startup command is to be backed up.

Specify the file name with 64 or fewer characters. For the characters that can be specified, see *Specifiable values for parameters.*

-f

Creates a backup file of the internal DB used to register the terminal that sends the startup command without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

Create the backup file `wol_dev.txt` for the internal DB used to register the terminal that sends the startup command:

```
# store wol-device ramdisk wol_dev.txt
Backup wol-device name data.  Are You sure? (y/n): y

Backup complete.
#
```

Display items

None

Impact on communication

None

Response messages

Table 30-12 List of response messages for the store wol-device command

Message	Description
Backup complete.	A backup file has been created successfully.

Message	Description
Store operation failed.	The command could not be executed because of insufficient RAMDISK capacity.
Command information was damaged.	A backup file could not be generated because the DB information is corrupted.
Data doesn't exist.	A backup file could not be generated. A commit operation might not have been executed. Execute a commit operation, and then check the result. If the commit operation fails again, the internal flash memory might be corrupted.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- If the free capacity on the RAMDISK is insufficient, use the `del` command to delete unnecessary files before creating the backup files.

load wol-device [OS-L2A]

Restores from a backup file the internal DB used to register the terminal that sends the startup command.

Note that information registered or changed by using the following commands will be replaced by the information that is being restored:

- `set wol-device name` command
- `set wol-device mac` command
- `set wol-device vlan` command
- `set wol-device ip` command
- `set wol-device alive` command
- `set wol-device description` command
- `remove wol-device name` command
- `commit wol-device` command

Syntax

```
load wol-device ramdisk <File name> [-f]
```

Input mode

Administrator mode

Parameters

ramdisk

Restores to the RAMDISK from a backup file the internal DB used to register the terminal that sends the startup command.

<File name>

Specify the name of the file from which the internal DB for registering the terminal that sends the startup command is to be restored.

Specify the file name with 64 or fewer characters. For the characters that can be specified, see *Specifiable values for parameters.*

-f

Restores the internal DB used to register the terminal that sends the startup command without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

Restore the internal DB used to register the terminal that sends the startup command from the backup file:

```
# load wol-device ramdisk wol_dev.txt
Restore wol-device name data.  Are you sure? (y/n): y

Restore complete.
#
```

Display items

None

Impact on communication

None

Response messages

Table 30-13 List of response messages for the load wol-device command

Message	Description
Restore complete.	Restoration from the backup file was successful.
File format error.	The format of the specified backup file is different from the internal DB used to register the terminal that sends the startup command.
Load operation failed.	Restoration from the backup file failed.
Flash memory write failed.	Writing of the information to internal flash memory failed.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- For current users of the terminal, the execution results are applied from the next login. (Even if the information for the terminal being used has been deleted, the user can continue to use the terminal.)

set wol-authentication user [OS-L2A]

Registers new user information in the internal DB for user authentication. Specify the name of an accessible terminal and access permissions.

To apply the setting to user information, execute the `commit wol-authentication` command.

Syntax

```
set wol-authentication user <User name> <Password> permit [any] [manual] [device-name <Name>]
```

Input mode

Administrator mode

Parameters

<User name>

The user name.

Specify 1 to 128 characters. You can use alphanumeric characters (case sensitive), at marks (@), hyphens (-), underscores (_), and periods (.).

<Password>

Specify the user password.

Specify 1 to 32 characters. You can use alphanumeric characters (case sensitive), at marks (@), hyphens (-), underscores (_), and periods (.).

permit [any] [manual] [device-name *<Name>*]

any

Sets access permissions for all terminals that have been registered in the internal DB used to register the terminal that sends the startup command.

manual

Sets access permissions that directly specify the MAC address and VLAN ID.

device-name *<Name>*

Sets the terminal name that has been registered in the internal DB used to register the terminal that sends the startup command.

Specify 1 to 128 characters. You can use alphanumeric characters (case sensitive), at marks (@), hyphens (-), underscores (_), and periods (.).

Note on setting this parameter

You cannot omit all of the parameters. Specify at least one of the parameters.

Example

Registering the new user name `USER01`:

```
# set wol-authentication user USER01 pass permit any manual device-name PC01
```

Display items

None

Impact on communication

None

Response messages

Table 30-14 List of response messages for the set wol-authentication user command

Message	Description
Already user '*<User name>*' exists.	The specified user has already been registered.
The number of users exceeds 300.	The number of users to be registered exceeds 300.
The sum of the device of each user exceeds 300.	The number of combinations of users and terminals set for each user has exceeded 300.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- To check user information, execute the `show wol-authentication user` command.
- The maximum number of users that can be registered is 300.
- The upper limit on the number of combinations of users and terminals is 300. For example, if you allowed one user to access 300 terminals, then no more access permissions for other terminals can be set for the user. The `any` and `manual` settings are excluded from this limit.
- You can allow one user to access multiple terminals, but one execution of the command only registers access permissions for one terminal. To allow access to more terminals, use the `set wol-authentication permit` command.
- This command applies only to the registration of a new user. To change the setting, use another `set wol-authentication` command.

set wol-authentication password [OS-L2A]

Changes a user password that has been registered.

To apply the setting to user information, execute the `commit wol-authentication` command.

Syntax

```
set wol-authentication password <User name> <Old password> <New password>
```

Input mode

Administrator mode

Parameters

<User name>

Specify the name of the user whose password is to be changed.

<Old Password>

Specify the current password.

<New Password>

Specify the new password.

Specify 1 to 32 characters. You can use alphanumeric characters (case sensitive), at marks (`@`), hyphens (`-`), underscores (`_`), and periods (`.`).

Example

Changing the password for user `USER01`:

```
# set wol-authentication password USER01 pass user0101
```

Display items

None

Impact on communication

None

Response messages

Table 30-15 List of response messages for the set wol-authentication password command

Message	Description
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.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- Before execution of the command, user information must be registered by the `set wol-authentication user` command.

set wol-authentication permit [OS-L2A]

Changes (adds or deletes) information about the terminals that can be accessed by registered users.

To apply the setting to user information, execute the `commit wol-authentication` command.

Syntax

```
set wol-authentication permit <User name> { add [any][manual][device-name <Name>] |del
[any][manual][device-name <Name>] }
```

Input mode

Administrator mode

Parameters

<User name>

Specify the name of the user whose access permissions for the terminal are to be changed.

add [any][manual][device-name *<Name>*]

any

Adds access permissions for all terminals that have been registered in the internal DB used to register the terminal that sends the startup command.

manual

Adds access permission for a terminal for which a MAC address and VLAN ID are directly specified.

device-name *<Name>*

Adds the terminal name that has been registered in the internal DB used to register the terminal that sends the startup command.

Specify 1 to 128 characters. You can use alphanumeric characters (case sensitive), at marks (`@`), hyphens (`-`), underscores (_), and periods (`.`).

Note on setting this parameter

You cannot omit all of the parameters. Specify at least one of the parameters.

del [any][manual][device-name *<Name>*]

any

Deletes the access permissions for all terminals that have been registered in the internal DB used to register the terminal that sends the startup command.

manual

Deletes the access permissions for the terminal for which a MAC address and VLAN ID are directly specified.

device-name *<Name>*

Deletes the terminal name that has been registered in the internal DB used to register the terminal that sends the startup command.

Note on setting this parameter

You cannot omit all of the parameters. Specify at least one of the parameters.

Example

- Adding user access permissions for a terminal:

  ```
  # set wol-authentication permit USER01 add device-name PC02
  ```

- Deleting user access permissions for a terminal:

  ```
  # set wol-authentication permit USER01 del any manual device-name PC02@example.com
  ```

Display items

None

Impact on communication

None

Response messages

Table 30-16 List of response messages for the set wol-authentication permit command

Message	Description
Unknown user '<*User name*>'.	The specified user has not been registered.
The sum of the device of each user exceeds 300.	The number of combinations of users and terminals set for each user has exceeded 300.
The parameter cannot be adjusted to 0.	The parameter cannot be set to 0.
Unknown parameter.	The specified parameter could not be found.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- Before execution of the command, user information must be registered by the `set wol-authentication user` command.
- You can allow one user to access multiple terminals, but one execution of the command only registers access permissions for one terminal.
- An access permission that has already been registered cannot be added even if specified for the `add` parameter.
- The `del` parameter cannot be used to reduce the number of terminals that can be accessed to 0.

remove wol-authentication user [OS-L2A]

Deletes the user information that has been registered.

To apply the setting to user information, execute the `commit wol-authentication` command.

Syntax

```
remove wol-authentication user {<User name> | -all} [-f]
```

Input mode

Administrator mode

Parameters

{ *<User name>* | -all }

<User name>

Specify the name of the user to be deleted.

-all

Deletes all users.

-f

Deletes the user without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

- When deleting the user `USER01`:

```
# remove wol-authentication user USER01
Remove wol-authentication user.  Are you sure? (y/n): y
```

- Deleting all users who have been registered in the internal DB for user authentication:

```
# remove wol-authentication user -all
Remove all wol-authentication user.  Are you sure? (y/n): y
```

Display items

None

Impact on communication

None

Response messages

Table 30-17 List of response messages for the remove wol-authentication user command

Message	Description
Unknown user '*<User name>*'.	The specified user has not been registered. (when a single MAC address is specified)

Message	Description
User does not exist.	The user was not found (when the `-all` parameter is specified).
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.

show wol-authentication user [OS-L2A]

Displays user information that has been registered in the internal DB for user authentication. This command can also display user information that is being entered or edited by using the following commands:

- `set wol-authentication user` command
- `set wol-authentication password` command
- `set wol-authentication permit` command
- `remove wol-authentication user` command

User information is displayed in ascending order of user name.

Syntax

```
show wol-authentication user { edit | commit } [username <User name>] [detail]
```

Input mode

Administrator mode

Parameters

{ edit | commit }

edit

Displays user information being edited.

commit

Displays operating user information.

username *<User name>*

The user name.

If the specified character string partly matches the user name that has been registered, the relevant user information is displayed.

Specify 1 to 128 characters. You can use alphanumeric characters (case sensitive), at marks (@), hyphens (-), underscores (_), and periods (.).

Operation when this parameter is omitted:

All user information is displayed.

detail

Displays detailed information about the users who are being edited or operated.

Operation when this parameter is omitted:

Detailed information is not displayed.

Example 1

When displaying the user information being edited:

```
# show wol-authentication user edit

Date 2010/09/06 20:48:57 UTC
  Total user counts:   5
  Total device link:   7
   No any     manual  device  Username
    1 deny    deny         2  Mail-Address_of_USER04_of_The_Company...
    2 permit  permit       1  USER01
*   3 deny    permit       3  USER02
    4 permit  deny         0  USER03
```

```
*   5 permit  deny         1  USER05

#
```

* indicates that the relevant terminal name has not been registered in the internal DB used to register the terminal that sends the startup command.

Display items in Example 1

Table 30-18 Items displayed for the user information

Item	Meaning	Displayed detailed information
Total user counts	Number of registered users	Maximum of 300 terminals
Total device link	Number of combinations of users and terminals	Maximum of 300 sets
No	Entry number	Maximum of 300 entries
any	Setting status of access permissions for all terminals	permit: Access permissions have been set. deny: Access permissions have not been set.
manual	Setting status of access permissions that have been entered manually	permit: Access permissions have been set. deny: Access permissions have not been set.
device	Number of combinations of users and terminals	The number of terminals that have been set for one user
Username	user name	Up to 40 characters are displayed. (If the name exceeds 40 characters, part of the name is replaced with three periods (...). The full name can be checked in the detailed information.)

Example 2

Figure 30-2 Example of displaying detailed user information:

```
# show wol-authentication user edit detail

Date 2010/09/06 20:49:10 UTC
 No    1 : Mail-Address_of_USER04_of_The_Company@example.com
  permit : any=deny, manual=deny
   device-name
        1  : PC01
        2  : PC03_High-Speed_machine

 No    2 : USER01
  permit : any=permit, manual=permit
   device-name
        1  : PC01

 No    3 : USER02
  permit : any=deny, manual=permit
   device-name
    *   1  : PC02@
        2  : PC01
```

```
          3  : PC03_High-Speed_machine

 No    4 : USER03
  permit : any=permit, manual=deny

 No    5 : USER05
  permit : any=permit, manual=deny
   device-name
     *   1  : PC04@

#
```

* indicates that the relevant terminal name has not been registered in the internal DB used to register the terminal that sends the startup command.

Display items in Example 2

Table 30-19 Items displayed for detailed user information

Item		Meaning	Displayed detailed information
No		Entry number	Maximum of 300 entries
		user name	--
permit	any=	Setting status of access permissions for all terminals	`permit`: Access permissions have been set. `deny`: Access permissions have not been set.
	manual=	Setting status of access permissions that have been entered manually	`permit`: Access permissions have been set. `deny`: Access permissions have not been set.
	device-name	Entry number	Maximum of 300 entries
		Terminal name	This item is not displayed if it has not been set.

Impact on communication

None

Response messages

Table 30-20 List of response messages for the show wol-authentication user command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no information. (edit)	There was no information in the edit area of the internal DB.
There is no information. (commit)	There was no information in the commit area of the internal DB.

Message	Description
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- (*) indicates that the relevant terminal name has not been registered in the internal DB used to register the terminal that sends the startup command. Use the `show wol-device-name` command to check the information that has been registered.

commit wol-authentication [OS-L2A]

Stores the edited user information in internal flash memory and reflects its contents for operation.

Syntax

```
commit wol-authentication [-f]
```

Input mode

Administrator mode

Parameters

-f

Stores the internal DB for user authentication in internal flash memory and reflects its contents for operation. A confirmation message is not displayed.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

Example of storing the internal DB for user authentication:

```
# commit wol-authentication
Commitment wol-authentication user data.  Are you sure? (y/n): y

Commit complete.
#
```

Display items

None

Impact on communication

None

Response messages

Table 30-21 List of response messages for the commit wol-authentication command

Message	Description
Commit complete.	Storing the information to internal flash memory and reflecting its contents for Secure Wake-on-LAN finished normally.
Flash memory write failed.	Writing of the information to internal flash memory failed.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- For current users of the terminal, the execution results are applied from the next login. (Even if the information of the user being used has been deleted, the user can continue to use the terminal.)

store wol-authentication [OS-L2A]

Creates a backup file of the internal DB for user authentication.

Syntax

```
store wol-authentication ramdisk <File name> [-f]
```

Input mode

Administrator mode

Parameters

ramdisk

Creates a backup file of the internal DB for user authentication on the RAMDISK.

<File name>

Specify the name of the file to which the internal DB for user authentication is to be backed up.

Specify the file name with 64 or fewer characters. For the characters that can be specified, see *Specifiable values for parameters.*

-f

Creates a backup file of the internal DB for user authentication without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

Creating the backup file `wol_auth.txt` for the internal DB for user authentication:

```
# store wol-authentication ramdisk wol_auth.txt
Backup wol-authentication user data.  Are You sure? (y/n): y

Backup complete.
#
```

Display items

None

Impact on communication

None

Response messages

Table 30-22 List of response messages for the store wol-authentication command

Message	Description
Backup complete.	A backup file has been created successfully.
Store operation failed.	The command could not be executed because of insufficient RAMDISK capacity.

Message	Description
Command information was damaged.	A backup file could not be generated because the DB information is corrupted.
Data doesn't exist.	A backup file could not be generated. A commit operation might not have been executed. Execute a commit operation, and then check the result. If the commit operation fails again, the internal flash memory might be corrupted.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- If the free capacity on the RAMDISK is insufficient, use the `del` command to delete unnecessary files before creating the backup files.

load wol-authentication [OS-L2A]

Restores the internal DB for user authentication from a backup file.

Note that information registered or changed by using the following commands will be replaced by the information that is being restored:

- `set wol-authentication user` command
- `set wol-authentication password` command
- `set wol-authentication permit` command
- `remove wol-authentication user` command
- `commit wol-authentication` command

Syntax

```
load wol-authentication ramdisk <File name> [-f]
```

Input mode

Administrator mode

Parameters

ramdisk

Restores the internal DB for user authentication from a backup file to the RAMDISK.

<File name>

Specify the name of the backup file from which the internal DB for user authentication is to be restored.

Specify the file name with 64 or fewer characters. For the characters that can be specified, see *Specifiable values for parameters*.

-f

Restores the internal DB for user authentication without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

Restoring the internal DB for user authentication from the backup file `wol_auth.txt`:

```
# load wol-authentication ramdisk wol_auth.txt
Restore wol-authentication user data.  Are you sure? (y/n): y

Restore complete.
#
```

Display items

None

Impact on communication

None

Response messages

Table 30-23 List of response messages for the load wol-authentication command

Message	Description
Restore complete.	Restoration from the backup file was successful.
File format error.	The format of the specified backup file is different from the internal DB for authentication.
Load operation failed.	Restoration from the backup file failed.
Flash memory write failed.	Writing of the information to internal flash memory failed.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- For current users of the terminal, the execution results are applied from the next login. (Even if the information of the user being used has been deleted, the user can continue to use the terminal.)

wol [OS-L2A]

Directly sends the startup command to the specified terminal to turn it on.

Syntax

```
wol <MAC> <VLAN ID>
```

Input mode

Administrator mode

Parameters

<MAC>

Specify the MAC address of the terminal to which the startup command is to be sent.

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 to which the terminal to which the startup command is to be sent belongs. For details about the specifiable range of values, see *Specifiable values for parameters*.

Example

Sending the startup command to the terminal whose MAC address is `0012.e256.7890` and VLAN ID is `200`:

```
# wol 0012.e256.7890 200
```

Display items

None

Impact on communication

None

Response messages

Table 30-24 List of response messages for the wol command

Message	Description
The magic packet is sent.	The startup command has been sent.
The magic packet is not sent.	An attempt to send the startup command failed.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- One execution of this command will send the startup command only once.

show wol [OS-L2A]

Displays information about the users currently using the Secure Wake-on-LAN functionality from Web browsers.

Syntax

```
show wol
```

Input mode

Administrator mode

Parameters

None

Example

Example of displaying information about current users:

```
# show wol

Date 2010/09/06 17:32:25 UTC
  No User name                          Phase   Magic  Device IP       Target
   1 User-A                             IDLE    -      -               Timeout
   2 User-B                             CHECK   Sent   192.168.1.102   Waiting
   3 User-C                             IDLE    Sent   192.168.10.100  Alive
   4 User-D                             RESOLVE Failed Waiting         -
   5 User-E                             RESOLVE Sent   Waiting         -
   6 Mail-Address_of_USER04_of_The_Co... IDLE    Sent   202.68.133.72   Alive

#
```

Display items

Table 30-25 Information displayed for current users

Item	Meaning	Displayed detailed information
No	Entry number	Maximum of 32 entries
User name	user name	The name of a user for which authentication is currently being processed Up to 35 characters are displayed. (If the name exceeds 35 characters, part of the name is replaced with three periods (`...`).)
Phase	The status of the user	`REGIST`: The initial user authentication status `MAGIC`: The startup command can be issued after the terminal information has been selected and entered. `RESOLVE`: IP resolution on the DHCP terminal is being monitored. `CHECK`: The terminal is being monitored. `IDLE`: A processing series either has been completed or has suspended due to timing out of a request or similar reason. `FIN`: The response to the final update

Item	Meaning	Displayed detailed information
		request has been completed, or completion processing continues due to timing out of the request or a similar reason.
Magic	The status of sending the startup command	`Sent`: The startup command has been sent. `Failed`: An attempt to send the startup command failed. `-`: Not executed.
Device IP	Terminal IP address	`-`: Unknown IP address `Waiting`: The IP address for the DHCP terminal is being checked. `IPv4`: The terminal IP address has been resolved.
Target	The status of the applicable terminal	`-`: Not executed. `Waiting`: The terminal is being monitored. `Alive`: A verification response has been received. `Timeout`: Monitoring or a request has timed out. #: The monitoring status continues no more than 1 minute.

Impact on communication

None

Response messages

Table 30-26 List of response messages for the show wol command

Message	Description
There is no information.	There is no information about users using Secure Wake-on-LAN.
License key is not installed.	The license key has not been set.

Notes

- This command can be executed only after the license key has been installed.
- The execution results of the `wol` command are not applied.

31. DHCP Snooping

show ip dhcp snooping
show ip dhcp snooping binding
clear ip dhcp snooping binding
show ip dhcp snooping statistics
clear ip dhcp snooping statistics
show ip arp inspection statistics
clear ip arp inspection statistics

show ip dhcp snooping

Displays information about DHCP snooping.

Syntax

```
show ip dhcp snooping
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 31-1 Displaying DHCP snooping information

```
> show ip dhcp snooping

Date 2010/12/20 20:45:04 UTC
Switch DHCP snooping is Enable
Option allow untrusted: off,  Verify mac-address: on
DHCP snooping is configured on the following VLANs:
  1-8,2048,4090-4094
Port      Trusted Verify source Rate limit(pps)
0/1       no      off           unlimited
0/2       no      off           unlimited
0/3       no      off           unlimited
     :                  :
ChGr:32   no      off           unlimited
ChGr:64   yes     off           unlimited

>
```

Display items

Table 31-1 Information displayed by executing the show ip dhcp snooping command

Item	Meaning	Displayed detailed information
Switch DHCP snooping is	The status of DHCP snooping	`Enable`: Enabled `Disable`: Disabled
Option allow untrusted	Permission to receive option 82	`on`: Receiving the option is permitted. `off`: Receiving the option is not permitted.
Verify mac-address	Verification of the MAC address from which DHCP packets are sent	`on`: The source MAC address is checked. `off`: The source MAC address is not checked.
VLANs	List of VLANs on which DHCP snooping is operating	`nothing` is displayed if there is no VLANs.

Item	Meaning	Displayed detailed information
Port	Port	If the interface is gigabitethernet or tengigabitethernet, the interface number is displayed. For port-channel, the following value is displayed: `ChGr:1` to `ChGr:64`
Trusted	--	`yes`: Trusted port `no`: Untrusted port
Verify source	Terminal filter setting	`off`: No filtering `on`: Filtering by IP address `mac-only`: Filtering by MAC address `port-security`: Filtering by IP address and MAC address
Rate limit(pps)	Limit on the reception rate for each port	Displays the limit value set for the reception rate of DHCP packets. `1` to `300`: (pps) `unlimited`: There is no limit.

Impact on communication

None

Response messages

None

Notes

None

show ip dhcp snooping binding

Displays information about the DHCP snooping binding database.

Syntax

```
show ip dhcp snooping binding[ip <IP address>][mac <MAC>][vlan <VLAN ID>]  [port <Port# list>][channel-group-number <Channel group# list>] [{static|dynamic}]
```

Input mode

User mode and administrator mode

Parameters

ip *<IP address>*

Displays the entries for the specified IP address.

mac *<MAC>*

Displays the entries for the specified MAC address.

vlan *<VLAN ID>*

Displays the entries for the specified VLAN interface.

For *<VLAN ID>*, specify the VLAN ID set by the `ip dhcp snooping vlan` command.

port *<Port# list>*

Displays information about the DHCP snooping binding database for the ports specified in list format.

For details about how to specify *<Port# list>* and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number *<Channel group# list>*

Displays information about the DHCP snooping binding database 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*.

{static|dynamic}

static

Displays the static entries.

dynamic

Displays the dynamic entries.

Note on setting parameters

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, the information that meets all the specified conditions is displayed (if the `port` or `channel-group-number` parameter is specified, information that meets any of the conditions is displayed).

Example

Figure 31-2 Displaying the DHCP snooping binding database information

```
> show ip dhcp snooping binding

Date 2010/12/20 20:45:08 UTC

Agent URL: -
Last succeeded time: -
```

```
Total Bindings: 10
MAC Address     IP Address       Expire(min)  Type      VLAN  Port
0012.e294.86b2  192.168.254.201  1437         dynamic   4094  0/1
0012.e294.88b2  192.168.254.202  1438         dynamic   4094  0/1
0012.e294.8ab2  192.168.254.203  1439         dynamic   4094  0/1
     :                  :
0012.e2a5.4241  192.168.254.154  -            static    4094  0/3
0012.e2a5.4251  192.168.254.155  -            static    4094  0/3

>
```

Display items

Table 31-2 Information displayed by executing the show ip dhcp snooping binding command

Item	Meaning	Displayed detailed information
Agent URL	Save location for the binding database	Displays the configuration information. `flash`: Indicates internal flash memory. `mc`: Indicates a memory card. `-`: Not specified
Last succeeded time	Date and time the device last saved information [#1]	*year*`/`*month*`/`*day* *hour*`:`*minute*`:`*second* *time-zone* Date and time information was saved to the save location. `-` is displayed for the following cases:[#2] ● The agent URL is not specified. ● The database has never been saved. ● The number of the binding entries for database restoration is zero.
Total Bindings	Total number	--
MAC Address	Terminal MAC address.	--
IP Address	Terminal IP address	--
Expire(min)	Aging time (in minutes)	If `Type` is `static` or there is no aging time limit, `-` is displayed.
Type	Entry type	`static`: Indicates a static entry. `dynamic`: Indicates a dynamic entry.
VLAN	The number of the VLAN connected to the terminal	--

Item	Meaning	Displayed detailed information
Port	Port to which a terminal is connected	If the interface is gigabitethernet or tengigabitethernet, the interface number is displayed. For port-channel, the following value is displayed: `ChGr:1` to `ChGr:64`

#1 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.

#2 If this command is executed when either of the following conditions exists, `Last succeeded time` is displayed, and the `No binding entry.` message might be displayed.

- There are no static entries.
- An aging timeout occurred for all dynamic entries.

  (Or the `clear ip dhcp snooping binding` command is executed)

Impact on communication

None

Response messages

Table 31-3 List of response messages for the show ip dhcp snooping binding command

Message	Description
DHCP Snooping is not configured.	The command could not be executed because DHCP snooping had not been configured.
No binding entry.	There is no information to be displayed.

Notes

None

clear ip dhcp snooping binding

Clears information in 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>][vlan <VLAN ID>]
[port <Port# list>][channel-group-number <Channel group# list>]
```

Input mode

User mode and administrator mode

Parameters

ip *<IP address>*

Clears the entries for the specified IP address.

mac *<MAC>*

Clears the entries for the specified MAC address.

vlan *<VLAN ID>*

Clears the entries for the specified VLAN interface.

For *<VLAN ID>*, specify the VLAN ID set by the `ip dhcp snooping vlan` command.

port *<Port# list>*

Clears information about the DHCP snooping binding database for the ports specified in list format.

For details about how to specify *<Port# list>* and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number *<Channel group# list>*

Clears information about the DHCP snooping binding database 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*.

Note on setting parameters

This command can clear only the information that meets the conditions specified by the parameter. If no parameter is specified, information is cleared without being limited by any conditions. If multiple parameters are specified, information that meets all conditions will be cleared. (If the port or channel-group-number parameter is specified, information that meets any of the conditions is cleared.)

Example

Figure 31-3 Clearing information by executing the clear ip dhcp snooping binding command

```
> clear ip dhcp snooping binding

>
```

Display items

None

Impact on communication

Terminal filters remain enabled until the address is redistributed.

Response messages

Table 31-4 List of response messages for the clear ip dhcp snooping binding command

Message	Description
DHCP Snooping is not configured.	The command could not be executed because DHCP snooping had not been configured.
No binding entry.	There is no information to be cleared.

Notes

None

show ip dhcp snooping statistics

Displays statistics about DHCP snooping.

Syntax

```
show ip dhcp snooping statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 31-4 Displaying statistics about DHCP snooping

```
> show ip dhcp snooping statistics

Date 2010/12/20 20:45:14 UTC
Database Exceeded: 0
Total DHCP Packets: 78
Port            Recv      Filter   Rate over
0/1               35           0           0
0/2                0           0           0
0/3               23           3           0
     :               :
ChGr:16            0           0           0
ChGr:32            0           0           0

>
```

Display items

Table 31-5 Information displayed by executing the show ip dhcp snooping statistics command

Item	Meaning	Displayed detailed information
Database Exceeded	Number of times 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	If the interface is gigabitethernet or tengigabitethernet, the interface number is displayed. For port-channel, the following value is displayed: `ChGr:1` to `ChGr:64`
Recv	Number of DHCP packets received on untrusted ports for DHCP snooping	The number of discarded packets displayed in `Filter` and `Rate over` are included.

Item	Meaning	Displayed detailed information
Filter	Of the DHCP packets received (Recv) on the untrusted port for DHCP snooping, the number of DHCP packets discarded as invalid packets	The number of discarded packets displayed in `Rate over` is not included.
Rate over	Of the DHCP packets received (Recv) on the untrusted port for DHCP snooping, the number of DHCP packets discarded when an exceeded rate limit was detected	The number of discarded packets displayed in `Filter` is not included. * A rate check precedes an invalid packet check.

Impact on communication

None

Response messages

Table 31-6 List of response messages for the show ip dhcp snooping statistics command

Message	Description
DHCP Snooping is not configured.	The command could not be executed because DHCP snooping had not been configured.

Notes

None

clear ip dhcp snooping statistics

Clears the DHCP snooping statistics.

Syntax

```
clear ip dhcp snooping statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 31-5 Clearing information by executing the clear ip dhcp snooping statistics command

```
> clear ip dhcp snooping statistics

>
```

Display items

None

Impact on communication

None

Response messages

Table 31-7 List of response messages for the clear ip dhcp snooping statistics command

Message	Description
DHCP Snooping is not configured.	The command could not be executed because DHCP snooping had not been configured.

Notes

None

show ip arp inspection statistics

Displays statistics about dynamic ARP inspection.

Syntax

```
show ip arp inspection statistics
```

Input mode

Administrator mode

Parameters

None

Example

Figure 31-6 Displaying statistics about ARP inspection

```
> show ip arp inspection statistics

Date 2010/09/14 13:09:52 UTC
 Port   VLAN   Forwarded      Dropped (  Rate over  DB unmatch     Invalid )
 0/1      11           0           15 (          0          15           0 )
 0/2      11         584          883 (          0         883           0 )
 0/3      11           0            0 (          0           0           0 )

   :                  :

 ChGr2    11         170           53 (          0          53           0 )

>
```

Display items

Table 31-8 Information displayed by executing the show ip arp inspection statistics command

Item	Meaning	Displayed detailed information
Port	Port number or channel group number	If the interface is gigabitethernet or tengigabitethernet, the interface number is displayed. For port-channel, the following value is displayed: `ChGr1` to `ChGr64`
VLAN	VLAN ID	--
Forwarded	Number of forwarded ARP packets	--
Dropped	Total number of discarded ARP packets	Total of the numbers displayed in `Rate over`, `DB unmatch`, and `Invalid`
Rate over	Number of ARP packets discarded because of exceeded reception rate limits	--

Item	Meaning	Displayed detailed information
DB unmatch	Number of ARP packets discarded because they did not match the information in the binding database	--
Invalid	Number of ARP packets discarded because of invalid binding information	--

Impact on communication

None

Response messages

Table 31-9 List of response messages for the show ip arp inspection statistics command

Message	Description
ARP Inspection is not configured.	The command could not be executed because dynamic ARP inspection had not been configured.
There is no information. (ip arp inspection statistics)	There is no statistics on dynamic ARP inspection.

Notes

None

clear ip arp inspection statistics

Clears dynamic ARP inspection statistics.

Syntax

```
clear ip arp inspection statistics
```

Input mode

Administrator mode

Parameters

None

Example

Figure 31-7 Clearing statistics by executing the clear ip arp inspection statistics command

```
# clear ip arp inspection statistics

#
```

Display items

None

Impact on communication

None

Response messages

None

Notes

None

Part 11: High Reliability Based on Redundant Configurations

32. GSRP

show gsrp aware

show gsrp aware

Displays GSRP aware information.

Syntax

```
show gsrp aware
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 32-1 Example of executing the command show gsrp aware

```
> show gsrp aware

Date 2010/09/14 14:34:40 UTC
Last mac_address_table Flush Time : 2010/09/14 14:34:35
GSRP Flush Request Parameters :
 GSRP ID : 10      VLAN Group ID : 6   Port : 0/16
 Source MAC Address : 0012.e208.2096

>
```

Display items

Item	Meaning	Displayed detailed information
Last mac_address_table Flush Time	Time `mac_address_table Flush` was last performed	*yyyy/mm/dd hh:mm:ss* year/month/day hour:minute:second
GSRP Flush Request Parameters	Information about the GSRP Flush request frame when `mac_address_table Flush` was last performed	--
GSRP ID	GSRP group number	1 to 65535
VLAN Group ID	The VLAN group number for the received GSRP Flush request frame	1 to 64 (This ID indicates the number of the VLAN group in which the master and backup are switched.)
Port	Port on which a GSRP Flush request frame was received	`Peer-link` is displayed if the port received while SML is used is a peer link.
Source MAC Address	MAC address from which the received GSRP Flush request frame was sent	--

Impact on communication

None

Response messages

Table 32-1 List of response messages for the show gsrp aware command

Message	Description
No received flush request frame.	No GSRP Flush request frames were received.

Notes

Receiving a GSRP Flush request frame clears all MAC address tables for every VLAN group IDs.

33. Uplink Redundancy

set switchport-backup active
show switchport-backup
show switchport-backup statistics
clear switchport-backup statistics
show switchport-backup mac-address-table update
show switchport-backup mac-address-table update statistics
clear switchport-backup mac-address-table update statistics

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 status due to a failure.

Syntax

```
set switchport-backup active { port <IF#> | channel-group-number <Channel group#> } [-f]
```

Input mode

User mode and administrator mode

Parameters

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

port *<Port#>*

Specifies the interface port number which becomes the active port.

channel-group-number *<Channel group#>*

Specifies the channel group number which becomes the active port.

-f

Switches to the active port without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

The following is an example of switching the standby port to the active port.

Figure 33-1 Example of executing the command that switches the active port

```
> set switchport-backup active port 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 33-1 List of response messages for the set switchport-backup active command

Message	Description
Uplink redundant is not configured.	Uplink redundancy has not been set. Check the configuration.
Ethernet *<IF#>* is already selected.	The specified interface is already running. *<IF#>*: Interface port number

Message	Description
Port-channel <*Channel group#*> is already selected.	The specified interface is already running. <*Channel group#*>: Channel group number
Ethernet < *IF#* > is down.	The specified interface is not running. <*IF#*>: Interface port number
Port-channel <*Channel group#*> is down.	The specified interface is not running. <*Channel group#*>: Channel group number
Not ready. Please wait a minute.	Uplink redundancy is being initialized. Wait a while.

Notes

Make sure that the port that you want to activate is in linkup status before you execute the command.

show switchport-backup

Displays information about the uplink redundancy.

Syntax

```
show switchport-backup
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 33-2 Exaple of displaying the information of uplink redundancy

```
> show switchport-backup

Date 2010/09/08 16:48:07 UTC
Startup active port selection: primary only
Switchport backup pairs                          Preemption    Flush
 Primary    Status      Secondary  Status       Delay Limit   VLAN
 Port 0/1   Blocking    Port 0/25  Forwarding       -     -   4094
*Port 0/10  Blocking    ChGr 4     Forwarding     100    98     10
 Port 0/11  Down        Port 0/15  Down             -     -      -
 Port 0/26  Blocking    ChGr 1     Forwarding      30    25   untag
 ChGr 8     Blocking    Port 0/24  Forwarding     300   297    100

>
```

Display items

Table 33-2 Items displayed for uplink redundancy information

Item		Meaning	Displayed detailed information
Startup active port selection		Setting of the functionality to fix the active port at Switch startup	`primary only`: The functionality to fix the active port at Switch startup is enabled. This item is displayed only when this functionality is enabled.
Switchport backup pairs	Primary	The number of the primary port or the channel group	If an asterisk (`*`) is displayed, the port is an uplink port and the secondary port cannot be used for communication because the functionality to fix the active port at Switch startup is enabled.
	Status	Status of the primary port	`Forwarding`: Forwarding `Blocking`: Blocking `Down`: Link down
	Secondary	The number of the secondary port or the channel group	--

Item		Meaning	Displayed detailed information
	Status	Status of the secondary port	`Forwarding`: Forwarding `Blocking`: Blocking `Down`: Link down
Preemption	Delay	The time value (in seconds) for automatic or timer switch-back	`-` is displayed when this item is not set.
	Limit	The time remaining until a timer switch-back (in seconds)	`-` is displayed when this item is not set.
Flush	VLAN	VLAN to which flush control frames are sent	`1` to `4094`: Indicates a VLAN ID. `untag`: No VLAN is specified. `-`: Send setting is not set.

Impact on communication

None

Response messages

Table 33-3 List of response messages for the show switchport-backup command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Uplink redundant is not configured.	Uplink redundancy has not been set. Check the configuration.
Not ready. Please wait a minute.	Uplink redundancy is being initialized. Wait a while.

Notes

If there is no configuration for the port channel interface specified as the secondary port, no information about a primary or secondary pair is displayed.

show switchport-backup statistics

Displays statistics related to flush control frames.

Syntax

```
show switchport-backup statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 33-3 Example of displaying statistics about the flush control frames

```
> show switchport-backup statistics

Date 2010/09/04 17:34:51 UTC
System ID : 00ed.f009.0001
Port 0/1  Transmit : on
          Transmit Total packets      :          3
          Receive  Total packets      :          0
                   Valid packets      :          0
                   Unknown version    :          0
                   Self-transmitted   :          0
                   Duplicate sequence :          0
  Last change time   : 2010/09/04 16:52:21 UTC (00:42:30 ago)
  Last transmit time : 2010/09/04 16:52:22 UTC (00:42:29 ago)
  Last receive time  : -
   Sender system ID  : 00ed.f001.0001

Port 0/2  Transmit : off
          Transmit Total packets      :          0
          Receive  Total packets      :          3
                   Valid packets      :          1
                   Unknown version    :          0
                   Self-transmitted   :          0
                   Duplicate sequence :          2
  Last change time   : -
  Last transmit time : -
  Last receive time  : 2010/09/04 17:18:26 UTC (00:16:25 ago)
   Sender system ID  : 00ed.f004.0001

          :

ChGr 8    Transmit : on
          Transmit Total packets      :          0
          Receive  Total packets      :          0
                   Valid packets      :          0
                   Unknown version    :          0
                   Self-transmitted   :          0
                   Duplicate sequence :          0
  Last change time   : -
  Last transmit time : -
  Last receive time  : -
   Sender system ID  : 00ed.f010.0001
```

>

Display items

Table 33-4 Items displayed for statistics about the flush control frames

Item	Meaning	Displayed detailed information
System ID	MAC address of the Switch	--
Port:<*IF#*>	Interface port number	--
ChGr<*Channel group#*>	Channel group number	--
Peer-link	Peer link	This item is displayed only when SML is used.
Transmit	Whether the transmission of flush control frames has been set	`on`: Flush control frames are sent. `off`: Flush control frames are not sent.
Transmit Total packets	Number of times a flush control frame was sent	--
Receive Total packets	Number of times a flush control frame was received	--
Valid packets	Number of received frames for which the MAC address table was cleared	--
Unknown version	Number of received frames for which the MAC address table was not cleared	The version in the frames was unknown.
Self-transmitted	Number of received frames for which the MAC address table was not cleared	Frames originated by the device
Duplicate sequence	Number of received frames for which the MAC address table was not cleared	Sequence duplication in the frames
Last change time	Date and time the primary and secondary were last switched and the time that has elapsed since then	*year*`/`*month*`/`*day* *hour*`:`*minute*`:`*second* *time-zone* `(`*d* `days` *hh*`:`*mm*`:`*ss* `ago)`[#1] `-` is displayed if the primary and secondary has never been switched.
Last transmit time	Date and time a flush control frame was last sent and the time that has elapsed since then	*year*`/`*month*`/`*day* *hour*`:`*minute*`:`*second* *time-zone* `(`*d* `days` *hh*`:`*mm*`:`*ss* `ago)`[#1] `-` is displayed if the frame has never been sent.

Item	Meaning	Displayed detailed information
Last receive time	Date and time a flush control frame was last received and the time that has elapsed since then	*year*/*month*/*day* *hour*:*minute*:*second* *time-zone* (*d* days *hh*:*mm*:*ss* ago)#1 - is displayed if the frame has never been received.
Sender system ID	MAC address from which the last received flush control frame was sent	- is displayed if the frame has never been received.

#1 Display of the elapsed time:

If the elapsed time is 24 hours or less: *hh*:*mm*:*ss* ago (*hh*=hours, *mm*=minutes, *ss*=seconds)

If the elapsed time is more than 10000 days: Over 10000 days

Impact on communication

None

Response messages

Table 33-5 List of response messages for the show switchport-backup statistics command

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

Notes

None

clear switchport-backup statistics

Clears statistics related to flush control frames.

Syntax

```
clear switchport-backup statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

```
> clear switchport-backup statistics

>
```

Display items

None

Impact on communication

None

Response messages

Table 33-6 List of response messages for the clear switchport-backup statistics command

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

Notes

None

show switchport-backup mac-address-table update

Displays information about MAC address update frames.

Syntax

```
show switchport-backup mac-address-table update
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 33-4 Example of displaying statistics about the MAC address update frames

```
> show switchport-backup mac-address-table update

Date 2010/09/09 18:02:40 UTC
Startup active port selection: primary only
Switchport backup pairs                       Preemption    Retransmit
 Primary    Status      Secondary  Status      Delay Limit
 Port 0/1   Down        Port 0/2   Forwarding      0     -            -
  VLAN            : 1,101-149,151-200,2001-2049,2051-2100,4040-4049,4051-4094
  Exclude-VLAN    : 50,150,1050,2050,3050,4050

Switchport backup pairs                       Preemption    Retransmit
 Primary    Status      Secondary  Status      Delay Limit
 Port 0/25  Down        Port 0/26  Forwarding      0     -            3
  VLAN            : 1,101-149,151-200,2001-2049,2051-2100,4040-4049,4051-4094
  Exclude-VLAN    : 50,150,1050,2050,3050,4050

Switchport backup pairs                       Preemption    Retransmit
 Primary    Status      Secondary  Status      Delay Limit
 ChGr 1     Down        ChGr 2     Forwarding      0     -            3
  VLAN            : 1,101-149,151-200,2001-2049,2051-2100,4040-4049,4051-4094
  Exclude-VLAN    : 50,150,1050,2050,3050,4050

>
```

Display items

Table 33-7 Information displayed for MAC address update frames

Item		Meaning	Displayed detailed information
Startup active port selection		Setting of the functionality to fix the active port at Switch startup	`primary only`: The functionality to fix the active port at Switch startup is enabled. This item is displayed only when this functionality is enabled.
Switchport backup pairs	Primary	The number of the primary port or the channel group	If an asterisk (`*`) is displayed, the port is an uplink port and the secondary port cannot be used for communication because the functionality to fix the active port at

Item		Meaning	Displayed detailed information
			Switch startup is enabled.
	Status	Status of the primary port	`Forwarding`: Forwarding `Blocking`: Blocking `Down`: Link down
	Secondary	The number of the secondary port or the channel group	--
	Status	Status of the secondary port	`Forwarding`: Forwarding `Blocking`: Blocking `Down`: Link down
Preemption	Delay	The time value (in seconds) for automatic or timer switch-back	`-` is displayed when this item is not set.
	Limit	The time remaining until a timer switch-back (in seconds)	`-` is displayed when this item is not set.
Retransmit		Number of retransmissions of MAC address update frames	`-` is displayed when this item is not set.
VLAN		VLANs that are subject to the MAC address update functionality	`-` is displayed when this item is not set. Up to 256 parameters are displayed. If the parameters exceed more than 256, parameters are included in the target VLAN, however, those are not displayed.
Exclude-VLAN		VLANs that are not subject to the MAC address update functionality	`-` is displayed when this item is not set.

Impact on communication

None

Response messages

Table 33-8 List of response messages for the show switchport-backup mac-address-table update command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Uplink redundant is not configured.	Uplink redundancy has not been set. Check the configuration.
Mac-address-table update is not configured.	The functionality for sending MAC address update frames has not been set or enabled.

Message	Description
Not ready. Please wait a minute.	Uplink redundancy is being initialized. Wait a while.

Notes

If there is no configuration for the port channel interface specified as the secondary port, no information about a primary or secondary pair is displayed.

show switchport-backup mac-address-table update statistics

Displays statistics related to MAC address update frames.

Syntax

```
show switchport-backup mac-address-table update statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 33-5 Example of displaying statistics about the MAC address update frames

```
> show switchport-backup mac-address-table update statistics

Date 2010/09/20 18:04:33 UTC
System ID : 0012.e244.0000
Port 0/1  Transition count                 :      20094
          Update transmit total packets    :          0
          Transmission over flows          :          0
  Last change time   : 2010/09/20 16:25:55 UTC (01:38:38 ago)
  Last transmit time : -

Port 0/2  Transition count                 :      20094
          Update transmit total packets    :        294
          Transmission over flows          :          0
  Last change time   : 2010/09/20 16:25:59 UTC (01:38:34 ago)
  Last transmit time : 2010/09/20 16:26:07 UTC (01:38:26 ago)

Port 0/25 Transition count                 :      18743
          Update transmit total packets    :     325020
          Transmission over flows          :       9224
  Last change time   : 2010/09/20 18:01:31 UTC (00:03:02 ago)
  Last transmit time : 2010/09/20 18:01:36 UTC (00:02:57 ago)

Port 0/26 Transition count                 :      18743
          Update transmit total packets    :    4098830
          Transmission over flows          :      10569
  Last change time   : 2010/09/20 18:01:37 UTC (00:02:56 ago)
  Last transmit time : 2010/09/20 18:04:22 UTC (00:00:11 ago)

ChGr 1    Transition count                 :        511
          Update transmit total packets    :      30553
          Transmission over flows          :        480
  Last change time   : 2010/09/20 18:01:29 UTC (00:03:04 ago)
  Last transmit time : 2010/09/20 18:01:19 UTC (00:03:14 ago)

ChGr 2    Transition count                 :        512
          Update transmit total packets    :     128844
          Transmission over flows          :        480
  Last change time   : 2010/09/20 18:01:33 UTC (00:03:00 ago)
  Last transmit time : 2010/09/20 18:04:32 UTC (00:00:01 ago)

>
```

Display items

Table 33-9 Display items for statistics about MAC address update frames

Item	Meaning	Displayed detailed information
System ID	MAC address of the Switch	--
Port<*IF#*>	Interface port number	--
ChGr<*Channel group#*>	Channel group number	--
Transition count	Number of primary and secondary switchovers	--
Update transmit total packets	Number of MAC address update frames that have been sent	--
Transmission over flows	Number of overflows when MAC address update frames were sent	# This counter counts up when the MAC addresses subject to sending exceeds 1024 in one switchover.
Last change time	Date and time the primary and secondary were last switched and the time that has elapsed since then	*year*`/`*month*`/`*day* *hour*`:`*minute*`:`*second* *time-zone* `(`*d* `days` *hh*`:`*mm*`:`*ss* `ago)`#1 `-` is displayed if the primary and secondary has never been switched.
Last transmit time	Date and time a MAC address update frame was last sent and the time that has elapsed since then	*year*`/`*month*`/`*day* *hour*`:`*minute*`:`*second* *time-zone* `(`*d* `days` *hh*`:`*mm*`:`*ss* `ago)`#1 `-` is displayed if the frame has never been sent.

#1 Display of the elapsed time:

If the elapsed time is 24 hours or less: *hh*`:`*mm*`:`*ss* `ago` (*hh*=hours, *mm*=minutes, *ss*=seconds)

If the elapsed time is more than 10000 days: `Over 10000 days`

Impact on communication

None

Response messages

Table 33-10 List of response messages for the show switchport-backup mac-address-table update statistics command

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

Message	Description
Uplink redundant is not configured.	Uplink redundancy has not been set. Check the configuration.
Mac-address-table update is not configured.	The functionality for sending MAC address update frames has not been set or enabled.
Not ready. Please wait a minute.	Uplink redundancy is being initialized. Wait a while.

Notes

If there is no configuration for the port channel interface specified as the secondary port, no information about a primary or secondary pair is displayed.

clear switchport-backup mac-address-table update statistics

Clears the statistics related to MAC address update frames.

Syntax

```
clear switchport-backup mac-address-table update statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

```
> clear switchport-backup mac-address-table update statistics

>
```

Display items

None

Impact on communication

None

Response messages

Table 33-11 List of response messages for the clear switchport-backup mac-address-table update statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Uplink redundant is not configured.	Uplink redundancy has not been set. Check the configuration.
Mac-address-table update is not configured.	The functionality for sending MAC address update frames has not been set or enabled.
Not ready. Please wait a minute.	Uplink redundancy is being initialized. Wait a while.

Notes

None

34. SML (Split Multi Link) [OS-L2A]

show sml [OS-L2A]
show sml channel-group [OS-L2A]

show sml [OS-L2A]

Displays the information about the SML status and settings.

Syntax

```
show sml
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 34-1 Example of executing the command show sml

```
> show sml

Date 2010/07/04 11:23:45 UTC
SML Status : Full
  sml id        : 1
  sml domain    : 100
  sml peer-link : 0/49-50
Peer
  sml id        : 2
  sml domain    : 100

>
```

Display items

Table 34-1 Items displayed for the information about the SML status and settings

Item	Meaning	Displayed detailed information
SML Status	SML status	`Conflict`: Detects the SML ID conflict `Standalone`: Not connecting to the neighboring devices `Full`: Connecting to the neighboring devices
sml id	SML ID for the Switch	The setting value of the `system sml id` command#
sml domain	SML domain ID for the Switch	The setting value of the `system sml domain` command
peer-link	Peer-link	The peer-link interface for the Switch The setting value of the `system sml peer-link` command#
Peer	Information about neighboring devices	--
sml id	SML ID for the neighboring device	`-` is displayed except for `SML Status=Full`.

Item	Meaning	Displayed detailed information
sml domain	SML domain ID for the neighboring device	- is displayed except for SML Status=Full.

It shows the value when the Switch startup.

Impact on communication

None

Response messages

Table 34-2 List of response messages for the show sml command

Message	Description
License key is not installed.	The license key has not been set.
SML is not configured.	SML has not been configured. Check the configuration.

Notes

None

show sml channel-group [OS-L2A]

Displays SML channel group information.

Syntax

```
show sml channel-group [summary]
```

Input mode

User mode and administrator mode

Parameters

summary

Displays summary information about SML channel groups.

Operation when this parameter is omitted:

Displays SML channel group information.

Example 1

Figure 34-2 Example of executing the command show sml channel-group

```
> show sml channel-group

Date 2012/12/06 18:20:21 UTC
ChGr:31   Mode: LACP
  CH Status      : Down  Elapsed Time: 00:15:33
  Actor System   : Priority: 128    MAC: 0012.e2a4.fe51  Key: 31
  Partner System : -
  Port Information
    1/0/25  Down  State: Detached
    2/0/23  Down  State: Detached
    2/0/25  Down  State: Detached

ChGr:32   Mode: LACP
  CH Status      : Up    Elapsed Time: 00:14:50
  Actor System   : Priority: 128    MAC: 0012.e2a4.fe51  Key: 32
  Partner System : Priority: 128    MAC: 0012.e2a8.85a2  Key: 32
  Port Information
    1/0/26  Up    State: Distributing
    2/0/26  Up    State: Distributing

ChGr:33   Mode: LACP
  CH Status      : Down  Elapsed Time: 00:15:35
  Actor System   : Priority: 128    MAC: 0012.e2a4.fe51  Key: 33
  Partner System : -
  Port Information
    2/0/22  Up    State: Detached

ChGr:64   Mode: Static
  CH Status      : Up    Elapsed Time: 00:14:56
  Port Information
    2/0/24  Up    State: Distributing

>
```

Display items in Example 1

Table 34-3 Items displayed for SML channel group information

Item	Meaning	Displayed detailed information
ChGr	Channel group number	--
Mode#1	Link aggregation mode	`LACP`: LACP link aggregation mode `Static`: Static link aggregation mode `-`: Link aggregation mode is not set.
CH Status#1	Channel group status	`Up`: Indicates that the channel group status is Up. `Down`: Indicates that the channel group status is Down.
Elapsed Time#1	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.
Actor System#1	Information about the actor system	This item is displayed only when LACP mode is enabled.
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	This value is the same as the channel group number. 0 to 65535
Partner System#1	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.
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	--
Key	Group key	0 to 65535
Port Information	Information about the ports managed by the channel group is	--

Item	Meaning	Displayed detailed information
	displayed.	
<SML ID>/*<IF#>*	SML ID and port number	--
Up	Link status of the port (up)	--
Down	Link status of the port (down)	--
State	Aggregation status of the port	`Detached`[#2]: The port is reserved, a port speed mismatch occurred, or half-duplex mode is set. `Attached`[#2]: The port is in a transition state or is negotiating. `Collecting`: The port is in a transition state or is negotiating (data can be received). `Distributing`: Data can be sent and received. If the status of the port is `Down`, `Detached` is displayed.

#1: Information about the device whose channel group status is Up is displayed.

If the channel group status is Up at both this device and the neighboring device, information about this device is displayed.

#2: If static link aggregation mode is enabled, data can be received while the port is in linkup status.

Example 2

Figure 34-3 Example of executing the command show sml channel-group with summary specified

```
> show sml channel-group summary

Date 2012/12/06 18:20:34 UTC
<ChGr> <          channel-group status          >
< No > <ChGr> <   SML ID:2   >   <   SML ID:1   >
  31    Down   Down              Down
  32    Up     Up                Up
  33    Down   Down              Not configured
  64    Up     Up                Up

>
```

Display items in Example 2

Table 34-4 Items displayed for SML channel group summary information

Item	Meaning	Displayed detailed information
<ChGr> <No>	Channel group number	--
<channel-group status><ChGr>	Channel group status	`Up`: Indicates that the channel group status is Up. `Down`: Indicates that the channel group status is Down.

Item	Meaning	Displayed detailed information
<SML ID:*n*> (left side)	Information for the device (*n*: SML ID for the device)	Channel group status of the device. `Up`: Indicates that the channel status is Up. `Down`: Indicates that the channel status is Down. `Not configured`: Interface port-channel has not been set.
<SML ID:*n*> (right side)	Information for the neighboring device (*n*: SML ID for the neighboring device) `-` is displayed in `Isolated` status.	Channel group status of the neighboring device. `Up`: Indicates that the channel status is Up. `Down`: Indicates that the channel status is Down. `Not configured`: Interface port-channel has not been set. `Isolated`: The status is unknown.

Impact on communication

None

Response messages

Table 34-5 List of response messages for the show sml channel-group command

Message	Description
License key is not installed.	The license key has not been set.
SML is not configured.	SML has not been configured. Check the configuration.
There is no information. (channel-group)	There is no channel group information.

Notes

None

Part 12: High Reliability Based on Network Failure Detection

35. IEEE 802.3ah/UDLD

show efmoam
show efmoam statistics
clear efmoam statistics

show efmoam

Displays the IEEE 802.3ah/OAM configuration information and the status of ports.

Syntax

```
show efmoam [port <Port# list>]
```

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*.

Operation when this parameter is omitted:

The IEEE 802.3ah/OAM configuration information for all ports is displayed.

Operation when all parameters are omitted:

The IEEE 802.3ah/OAM configuration information for all ports is displayed.

Example

The following is an example of displaying brief information related to the IEEE 802.3ah/OAM configuration.

Figure 35-1 Displaying IEEE 802.3ah/OAM configuration information

```
> show efmoam

Date 2010/09/13 17:36:11 UTC
Port    Status              Dest MAC
0/1     Forced Down (UDLD)  0012.e214.ffae
0/2     Mutually Seen       0012.e214.ffaf
0/3     Partner Seen        0012.e214.ffb0
0/4     Down                unknown
0/5     Down                unknown

>
```

Display items

Table 35-1 Items displayed for the IEEE 802.3ah/OAM configuration

Item	Meaning	Displayed detailed information
Port	Port number	Number of the interface port whose information is to be displayed
Status	Port status in the IEEE 802.3ah/UDLD functionality	`Forced Down (UDLD)`: Forced link-down in the UDLD functionality `Down`: Link-down due to some other reason `Passive Wait`: Wait status because the partner switch has not been recognized `Active Wait`: Wait status because the partner switch has not been recognized (OAM is being sent) `Partner Seen`: The partner switch has been

Item	Meaning	Displayed detailed information
		recognized. (Whether the partner switch has recognized the Switch is not clear.) `Mutually Seen`: The partner switch has been recognized. (The partner switch has also recognized the Switch.)
Dest MAC	MAC address of the port on the partner device	`unknown`: No information has been received from the partner switch since the device started up. MAC address: The MAC address for the partner switch from which information was last received

Impact on communication

None

Response messages

Table 35-2 List of response messages for the show efmoam command

Message	Description
There is no information. (efmoam)	`efmoam disable` has been set. There is no log information to be displayed.

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*.

Operation when this parameter is omitted:

Statistics for all IEEE 802.3ah/OAM frames (OAMPDU) are displayed by port.

Example

The following is an example of displaying the statistics for all configured IEEE 802.3ah/OAM.

Figure 35-2 Displaying the IEEE 802.3ah/OAM statistics for the specified port

```
> show efmoam statistics port 0/1-3,0/15

Date 2010/09/13 17:35:25 UTC
Port 0/1 [Forced Down (UDLD)]
  OAMPDUs:Tx     :        133  Rx        :         57
          Invalid:          0  Unrecogn. :          0
  Expirings      :          1  Thrashings:          0  Blockings:          1
Port 0/2 [Mutually Seen]
  OAMPDUs:Tx     :        771  Rx        :        750
          Invalid:          0  Unrecogn. :          0
  Expirings      :          0  Thrashings:          0  Blockings:          0
Port 0/3 [Partner Seen]
  OAMPDUs:Tx     :        631  Rx        :        593
          Invalid:          0  Unrecogn. :          0
  Expirings      :          0  Thrashings:          0  Blockings:          0
Port 0/15 [Down]
  OAMPDUs:Tx     :          0  Rx        :          0
          Invalid:          0  Unrecogn. :          0
  Expirings      :          0  Thrashings:          0  Blockings:          0

>
```

Display items

Table 35-3 Display items for the IEEE 802.3ah/OAM statistics for the specified port

Item	Meaning	Displayed detailed information
Port	Port number	Number of the interface port whose information is to be displayed

Item	Meaning	Displayed detailed information
[Status]	Port status in the IEEE 802.3ah/UDLD functionality	`Forced Down (UDLD)`: Forced link-down in the UDLD functionality `Down`: Link-down due to some other reason `Passive Wait`: Wait status because the partner switch has not been recognized `Active Wait`: Wait status because the partner switch has not been recognized (OAM is being sent) `Partner Seen`: The partner switch has been recognized.(Whether the partner switch has recognized the Switch is not clear.) `Mutually Seen`: The partner switch has been recognized.(The partner switch has also recognized the Switch.)
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
Expirings	Number of timeouts that occurred after the partner switch was detected	0 to 4294967295
Thrashings	Number of times other partner switches were detected before a timeout after a partner switch was initially detected	0 to 4294967295
Blockings	Number of shutdowns in UDLD	0 to 4294967295

Impact on communication

None

Response messages

Table 35-4 List of response messages for the show efmoam statistics command

Message	Description
There is no information. (efmoam)	`efmoam disable` has been set. There is no log information to be displayed.

Notes

The ports on which no OAMPDUs have been sent or received in passive mode are not displayed.

clear efmoam statistics

Clears the IEEE 802.3ah/OAM statistics.

Syntax

```
clear efmoam statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 35-3 Example of clearing IEEE 802.3ah/OAM statistics

```
> clear efmoam statistics

>
```

Display items

None

Impact on communication

None

Response messages

None

Notes

None

36. Storm Control

show storm-control
clear storm-control

show storm-control

Displays storm control information.

Syntax

```
show storm-control [port <Port# list>][broadcast][multicast][unicast][detail]
```

Input mode

User mode and administrator mode

Parameters

port *<Port# list>*

Displays the storm control information for the specified port.

For details about how to specify *<Port# list>* and the specifiable range of values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Storm control information for all ports is displayed.

broadcast

Displays broadcast storm control information.

multicast

Displays multicast storm control information.

unicast

Displays unicast storm control information.

Note on setting parameters

This command can display only the information relevant to the condition applied by a parameter that has been set. If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information that meets the conditions will be displayed.

detail

Displays detailed information about storm control.

Operation when this parameter is omitted:

Storm control information for all ports is displayed.

Example 1

Figure 36-1 Displaying storm control information

```
> show storm-control

Date 2010/09/24 10:46:35 UTC
<Broadcast>
 Port    Detect Recovery   Filter  State            Count Last detect
 0/1        200      100      100  Filtering            1 2010/09/24 10:46:25
 0/2        200      100        -  Forwarding           0 ----/--/-- --:--:--

<Unicast>
 Port    Detect Recovery   Filter  State            Count Last detect
 0/1      10000     5000     5000  Filtering            1 2010/09/24 10:45:52
 0/2      10000     5000        -  Forwarding           0 ----/--/-- --:--:--

>
```

Display items in Example 1

Table 36-1 Display items for storm control information

Item	Meaning	Displayed detailed information
Port	Port number	--
Detect	Storm detection threshold	Displays the upper threshold.
Recovery	Recovery-from-storm threshold	--
Filter	Flow rate limit value	Displays the lower threshold. `-` is displayed if a storm-control action filter has not been set.
State	Storm detection status	`Forwarding`: Forwarding normally `Filtering`: The flow rate limit is on. `Inactivate`: A port has been blocked by storm detection. `Detecting`: A storm has been detected (this status is displayed when a port is being blocked or when a flow limit has not been set).
Count	Number of storms that have been detected	--
Last detect	Date and time a storm was last detected	*year*`/`*month*`/`*day* *hour*`:`*minute*`:`*second* `-` is displayed when no storms have been detected.

Example 2

Figure 36-2 Displaying detailed information about storm control

```
> show storm-control port 0/1 broadcast detail

Date 2010/09/24 10:48:20 UTC
<Broadcast>
 Port 0/1
  Detect rate : 200         Recover rate : 100         Filter rate : 100
  Action : Filter,Trap,Log
  Filter recovery time : 30
  <Status>
  State : Filtering          Filter recovery remaining time : 30
  Current rate :        189  Current filter rate     :        100
  Detect count :          1  Last detect             : 2010/09/24 10:46:25

>
```

Display items in Example 2

Table 36-2 Items displayed for detailed storm control information

Item	Meaning	Displayed detailed information
Port	Port number	--
Detect rate	Storm detection threshold	Displays the upper threshold.

Item	Meaning	Displayed detailed information
Recover rate	Recovery-from-storm threshold	`-` is displayed if this item has not been set.
Filter rate	Flow rate limit value	Displays the lower threshold. `-` is displayed if a storm-control action filter has not been set.
Action	Operations when a storm is detected	`Inactivate`: The applicable port is blocked. `Filter`: The flow rate of the received frames has a limit. `Trap`: An SNMP trap is issued. `Log`: A log message is output.
Filter recovery time	Monitoring time for canceling the flow rate limit	`-` is displayed if a storm-control action filter has not been set.
State	Storm detection status	`Forwarding`: Forwarding normally `Filtering`: The flow rate limit is on. `Inactivate`: A port has been blocked by storm detection. `Detecting`: A storm has been detected (this status is displayed when a port is being blocked or when a flow limit has not been set).
Filter recovery remaining time	Remaining monitoring time for canceling the flow rate limit (in seconds)	`-` is displayed if `State` is not `Filtering`.
Current rate	Current flow rate	--
Current filter rate	Current status of the flow rate limit	When `State` is `Filtering`: The flow limit value When `State` is not `Filtering`: The storm detection threshold
Detect count	Number of storms that have been detected	--
Last detect	Date and time a storm was last detected	*year*`/`*month*`/`*day* *hour*`:`*minute*`:`*second* `-` is displayed when no storms have been detected.

Impact on communication

None

Response messages

Table 36-3 List of response messages for the show storm-control command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
storm-control is not configured.	The storm control functionality has not been configured. Check the configuration.

Notes

None

clear storm-control

Clears the storm control statistics counters.

Syntax

```
clear storm-control
```

Input mode

User mode and administrator mode

Parameters

None

Example 1

Figure 36-3 Clearing the storm control statistics counters

```
> clear storm-control

>
```

Impact on communication

None

Response messages

Table 36-4 List of response messages for the clear storm-control command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
storm-control is not configured.	The storm control functionality has not been configured. Check the configuration.

Notes

None

37. L2 Loop Detection

show loop-detection
show loop-detection statistics
clear loop-detection statistics
show loop-detection logging
clear loop-detection logging

show loop-detection

Displays 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>*

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 specified channel group link aggregation (in a list).

For details about how to specify *<Channel group# list>*, see *Specifiable values for parameters*.

Note on setting parameters

This command can display only the information relevant to the condition applied by a parameter that has been set.

If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information that meets the conditions will be displayed.

Operation when all parameters are omitted:

All L2 loop detection information is displayed.

Example

Displays L2 loop detection information.

Figure 37-1 Example of displaying L2 loop detection information

```
> show loop-detection

Date 2012/11/30 17:02:48 UTC
Interval Time           :10
Output Rate             :20pps
Threshold               :1
Hold Time               :infinity
Auto Restore Time       :-
VLAN Port Counts
    Configuration       :15         Capacity       :200
Port Information
  Port      Status     Type        DetectCnt RestoringTimer  SourcePort   Vlan
  0/1       Up         uplink              -              -  -
  0/2       Down       trap                0              -  -
  0/3       Down       send                3              -  Peer-link(U) 4093
  0/4       Down(loop) send-inact          1              -  Peer-link(U) 4093
  0/5       Up         exception           0              -  0/3          4093
  0/6       Up         exception           0              -  0/3          4093
  0/7       Down       trap                0              -  -
  0/8       Down       send                0              -  -
```

```
0/9       Up         send              0             -  -
0/10      Down       send              0             -  -
0/11      Down       send              0             -  -
0/12      Down       send              0             -  -
0/13      Down       send              0             -  -
0/14      Down       send              0             -  -
0/15      Down       send              0             -  -
0/16      Down       send              0             -  -
0/17      Down       send              0             -  -
0/18      Down       send              0             -  -
0/19      Down       send              0             -  -
0/20      Down       send              0             -  -
0/21      Down       trap              0             -  -
0/22      Down       trap              0             -  -
0/23      Down       trap              0             -  -
ChGr:31   Up         trap              0             -  -
ChGr:32   Up         trap              0             -  -
ChGr:64   Up         trap              0             -  -
Peer-link Up         uplink            -             -  0/3          4093

>
```

Display items

Table 37-1 Items displayed for 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 a port is blocked	Displays the setting value for the number of L2 loop detections before a port is blocked.
Hold Time	Time the number of detections is retained (in seconds)	Displays the setting time that the number of L2 loop detections is retained before a port is blocked. `infinity` is displayed if this item has not been set.#1
Auto Restore Time	Automatic restoration time (in seconds)	Displays the setting time before a blocked port is activated automatically. `-` is displayed if a port is not automatically restored.#2
Configuration	Number of ports set to send L2 loop detection frames	Displays the number of VLAN ports#3 that are set to send L2 loop detection frames If this value is larger than the value displayed for `Capacity` (the number of ports allowed for sending L2 loop detection frames), some L2 loop detection frames could not be sent.
Capacity	Number of ports allowed to send L2 loop detection frames	Number of VLAN ports#3 that are able to send L2 loop detection frames at the defined transmission rate

Item	Meaning	Displayed detailed information
Port	Port number, channel group number, or peer link	<*IF#*>: Port number `ChGr:`<*Channel group#*>: Channel group number `Peer-link`: Peer link (displayed during SML operation only)
Status	Port state	`Up`: Indicates that the port status is Up. Down: The port is in Down status. Down(loop): The port status is Down due to the L2 loop detection functionality.
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	Number of current detections	Displays the number of L2 loop detections. For an uplink port, `-` is displayed. The number of detections on the uplink port is counted on the sending port. The number of detections is updated until it reaches 10000.
RestoringTimer	Time remaining until automatic recovery (in seconds)	The time before the port is activated automatically is displayed. `-` is displayed if a port is not automatically restored.#2
SourcePort	Port for sending L2 loop detection frames	The sending port used when an L2 loop detection frame was last received. <*IF#*>: Port number `ChGr:`<*Channel group#*>: Channel group number `Peer-link`: Peer link (displayed during SML operation only) For the receive uplink port, `(U)` is displayed. `-` is displayed if no L2 loop detection frame has 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.

#1 When the `loop-detection hold-time` configuration command is omitted.

#2 When the `loop-detection auto-restore-time` configuration command is omitted.

#3 Total number in the VLANs set for the applicable physical ports or channel groups

Impact on communication

None

Response messages

Table 37-2 List of response messages for the show loop-detection command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
No corresponding port information.	No port and channel group information for L2 loop detection was found.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the functionality has not been enabled. Check the configuration.

Notes

Changing or disabling the L2 loop detection functionality clears the L2 loop detection information.

show loop-detection statistics

Displays 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>*

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*.

Note on setting parameters

This command can display only the information relevant to the condition applied by a parameter that has been set.

If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information that meets the conditions will be displayed.

Operation when all parameters are omitted:

All L2 loop detection statistics are displayed.

Example

Displays L2 loop detection statistics.

Figure 37-2 Example of displaying L2 loop detection statistics

```
> show loop-detection statistics

Date 2012/11/30 17:02:56 UTC
Port:0/1   Up          Type :uplink
 TxFrame       :                  0 RxFrame       :                  0
 Inactive Count:                  0 RxDiscard     :                  0
 Last Inactive :                  - Last RxFrame  :                  -
Port:0/2   Down        Type :trap
 TxFrame       :                  0 RxFrame       :                  0
 Inactive Count:                  0 RxDiscard     :                  0
 Last Inactive :                  - Last RxFrame  :                  -
Port:0/3   Down        Type :send
 TxFrame       :                 18 RxFrame       :                  0
 Inactive Count:                  0 RxDiscard     :                  0
 Last Inactive :                  - Last RxFrame  :                  -
Port:0/4   Down(loop)  Type :send-inact
 TxFrame       :                  1 RxFrame       :                  0
 Inactive Count:                  1 RxDiscard     :                  0
 Last Inactive : 2012/11/30 16:52:26 Last RxFrame  :                  -
```

```
Port:0/5   Up          Type :exception
 TxFrame       :                0 RxFrame       :                  14
 Inactive Count:                0 RxDiscard     :                   0
 Last Inactive :                - Last RxFrame  : 2012/11/30 17:02:37
Port:0/6   Up          Type :exception
 TxFrame       :                0 RxFrame       :                  12
 Inactive Count:                0 RxDiscard     :                   0
 Last Inactive :                - Last RxFrame  : 2012/11/30 17:02:37

                          :                           :

ChGr:64    Up          Type :trap
 TxFrame       :                0 RxFrame       :                   0
 Inactive Count:                0 RxDiscard     :                   0
 Last Inactive :                - Last RxFrame  :                   -
Peer-link  Up          Type :uplink
 TxFrame       :                0 RxFrame       :                  16
 Inactive Count:                0 RxDiscard     :                   0
 Last Inactive :                - Last RxFrame  : 2012/11/30 17:02:37

>
```

Display items

Table 37-3 Items displayed for L2 loop detection statistics

Item	Meaning	Displayed detailed information
Port	Port number	*<IF#>*: Port number
ChGr	Channel group number	*<Channel group#>*: Channel group number
Peer-link	Peer link	This item is displayed only when SML is used.
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 functionality.	--
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 the port has been blocked	--

Item	Meaning	Displayed detailed information
RxDiscard	Number of L2 loop detection frames that have been received and discarded	Displays the number of abnormal L2 detection frames that have been received and discarded.
Last Inactive	Time the port was last blocked	*year*/*month*/*day* *hour*:*minute*:*second* - is displayed if the port is an uplink port or if the port has never been blocked.
Last RxFrame	Time when the L2 loop detection frame was last received	*year*/*month*/*day* *hour*:*minute*:*second* - is displayed if no L2 loop detection frame has been received. The time an L2 loop detection frame was received and discarded is not displayed.

Impact on communication

None

Response messages

Table 37-4 List of response messages for the show loop-detection statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
No corresponding port information.	No port and channel group information for L2 loop detection was found.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the functionality has not been enabled. Check the configuration.

Notes

Changing or disabling the L2 loop detection functionality clears the statistics.

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>*

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*.

Note on setting parameters

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, information that meets the conditions will be displayed.

Operation when all parameters are omitted:

All L2 loop detection statistics are cleared.

Example

Clears L2 loop detection statistics.

Figure 37-3 Example of clearing L2 loop detection statistics

```
> clear loop-detection statistics

>
```

Display items

None

Impact on communication

None

Response messages

Table 37-5 List of response messages for the clear loop-detection statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the functionality has not been enabled. Check the configuration.

Notes

- Disabling the L2 loop detection functionality clears the statistics.
- Using this command to clear statistics also clears the MIB information obtained by SNMP.

show loop-detection logging

The following figure is an example of displaying log information about the received L2 loop detection frames.

With this command, you can check the port from which an L2 loop detection frame was sent and the port on which it was received. Log entries for the latest 1000 received frames are displayed in reverse chronological order. Note that the discarded frames are not displayed.

Syntax

```
show loop-detection logging
```

Input mode

User mode and administrator mode

Parameters

None

Example

Display the log information for received L2 loop detection frames.

Figure 37-4 Example of displaying log information for received L2 loop detection frames

```
> show loop-detection logging

Date 2010/09/12 16:23:10 UTC
2010/09/12 16:22:16  0/5     Source: 0/7     Vlan: 1
2010/09/12 16:22:06  0/5     Source: 0/7     Vlan: 1
2010/09/12 16:21:56  ChGr:8  Source: 0/8     Vlan: 1     Uplink Inactive
2010/09/12 16:21:56  0/5     Source: 0/7     Vlan: 1
2010/09/12 16:21:56  0/4     Source: 0/6     Vlan: 1     Inactive
2010/09/12 16:21:56  0/6     Source: 0/4     Vlan: 1
2010/09/12 16:21:56  ChGr:1  Source: ChGr:2  Vlan: 1     Inactive
2010/09/12 16:21:56  ChGr:2  Source: ChGr:1  Vlan: 1     Inactive
2010/09/12 16:21:46  ChGr:8  Source: 0/8     Vlan: 1     Uplink

>
```

Display items

Table 37-6 Items displayed for the log information about received L2 loop detection frames

Item	Meaning	Displayed detailed information
Data Time	Date and time the L2 loop detection frame was received	*yy*/*mm*/*dd hh*:*mm*:*ss* year/month/day hour:minute:second
<IF#>	Port number	Displays the number of the port on which the L2 loop detection frame was received.
ChGr:<*Channel group#*>	Channel group number	Displays the number of the channel group on which the L2 loop detection frame was received.
Peer-link	Peer link	This item is displayed only when SML is used.

Item	Meaning	Displayed detailed information
Source	The number of the port from which the L2 loop detection frame was sent	Displays the number of the port from which the L2 loop detection frame was sent. *<IF#>*: Port number `ChGr:`*<Channel group#>*: Channel group number
Vlan	VLAN ID	Displays the VLAN ID when an L2 loop detection frame was sent.
Uplink	Uplink port	Indicates that the L2 loop detection frame was received at the uplink port.
Inactive	Port blocked	Indicates that a port has been blocked.

Impact on communication

None

Response messages

Table 37-7 List of response messages for the show loop-detection logging command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
There is no logging data.	There is no log data.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the functionality has not been enabled. Check the configuration.

Notes

Disabling the L2 loop detection functionality clears log information about the received detection frames.

clear loop-detection logging

Cears the log information for received L2 loop detection frames.

Syntax

```
clear loop-detection logging
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure is an example of clearing the log information for received L2 loop detection frames.

Figure 37-5 Example of clearing the log information for received L2 loop detection frames

```
> clear loop-detection logging

>
```

Display items

None

Impact on communication

None

Response messages

Table 37-8 List of response messages for the clear loop-detection logging command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the functionality has not been enabled. Check the configuration.

Notes

None

38. CFM

l2ping
l2traceroute
show cfm
show cfm remote-mep
clear cfm remote-mep
show cfm fault
clear cfm fault
show cfm l2traceroute-db
clear cfm l2traceroute-db
show cfm statistics
clear cfm statistics

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 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 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.

Operation 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.

Operation 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.

Operation when this parameter is omitted:

40 bytes are added, and the CFM PDU that is sent is 64 bytes.

Example

The following figure is an example of executing the `l2ping` command.

Figure 38-1 Example of executing the l2ping command

```
> l2ping remote-mep 1010 domain-level 7 ma 1000 mep 1020 count 3
L2ping to MP:1010(0012.e254.dc01) on Level:7  MA:1000  MEP:1020  VLAN:20
Time:2010/09/28 06:59:50
1: L2ping Reply from 0012.e254.dc01  64bytes  Time=   20 ms
2: L2ping Reply from 0012.e254.dc01  64bytes  Time=   10 ms
3: L2ping Reply from 0012.e254.dc01  64bytes  Time=   10 ms

--- L2ping Statistics ---
  Tx L2ping Request :    3  Rx L2ping Reply :    3  Lost Frame  :   0%
  Round-trip Min/Avg/Max : 10/13/20 ms
>
```

Display items

Table 38-1 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 a remote MEP or MIP is specified. *<Remote MEP ID>*(*<Remote MAC address>*): When a remote MEP ID is specified.
Level	Domain level	0 to 7
MA	MA ID number	Configured MA ID number
MEP	MEP ID	MEP ID for the Switch
VLAN	VLAN ID	Source VLAN ID
Time	Send time	*yyyy*/*mm*/*dd hh*:*mm*:*ss* year/month/day hour:minute:second
<Count>	Test number	Test number
L2ping Reply from *<MAC address>*	MAC address of the replying MP	The MAC address of the remote MEP or MIP that replied.
bytes	Number of received bytes	Number of bytes starting from the common CFM header and ending with End TLV of the CFM PDU
Time	Response time	The time from the transmission of a loopback message until a loopback reply is received
Request Timed Out.	Reply wait timeout	Indicates that no reply was received within the reply wait time.
Transmission failure.	Transmission failure	Indicates that a message could not be sent from the source VLAN.
Tx L2ping Request	Number of loopback messages that were sent	--

Item	Meaning	Displayed detailed information
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 time	--

Impact on communication

None

Response messages

Table 38-2 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.
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 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. (This command also cannot be used concurrently with the `l2traceroute` command.)
- If you want to specify 1476 bytes or more for the `framesize` parameter, use the `mtu` or `system mtu` configuration command to set the MTU value for the jumbo frame to 1500 byte 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 whose route you want to verify. 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 whose route 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 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.

Operation 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.

Operation when this parameter is omitted:

The maximum number of hops is 64.

Example

The following figure is an example of executing the `l2traceroute` command.

Figure 38-2 Example of executing the l2traceroute command

```
> l2traceroute remote-mep 1010 domain-level 7 ma 1000 mep 1020 ttl 64
L2traceroute to MP:1010(0012.e254.dc01) on Level:7  MA:1000  MEP:1020  VLAN:20
Time:2010/09/28 08:27:44
 63  00ed.f205.0115  Forwarded
 62  0012.e2a8.f8d0  Forwarded
 61  0012.e254.dc01  NotForwarded  Hit
>
```

Display items

Table 38-3 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 a remote MEP or MIP is specified. *<Remote MEP ID>*(*<Remote MAC address>*): When a remote MEP ID is specified.
Level	Domain level	0 to 7
MA	MA ID number	Configured MA ID number
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 38-4 List of response messages for the l2traceroute 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.

Message	Description
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 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. (This command also cannot be used concurrently with the `l2ping` command.)
- 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.
- We recommend that you specify 64 or less for the TTL value to maintain the reception performance of the Switch.

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.

Operation 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.

Operation when this parameter is omitted:

All CFM information is displayed.

Example 1

The following figure is an example of displaying the CFM configuration information.

Figure 38-3 Example of displaying the CFM configuration information

```
> show cfm

Date 2010/09/28 09:31:33 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:00ed.f205.0101  Status:-
  MA 400   Name(str) : Tokyo_to_Nagoya
    Primary VLAN:400   VLAN:30-40,400
    CC:Enable   Interval:10min
    Alarm Priority:0  Start Time: 7500ms  Reset Time: 5000ms
    MEP Information
      ID:8014  DownMEP  0/21(Up)    Disable  MAC:00ed.f205.0115  Status:-
  MIP Information
      0/12(Up)    Enable   MAC:00ed.f205.010c
      0/22(Down)  Enable   MAC:-
```

```
Domain Level 4 Name(str): ProviderDomain_4
  MIP Information
      CH8 (Up)    Enable   MAC:00ed.f205.0108

>
```

Display items in Example 1

Table 38-5 Items displayed for the CFM configuration information

Item	Meaning	Displayed detailed information
Domain Level *<Level>*	Domain level and domain name	*<Level>*: Domain level `Name:-`: Indicates that the domain name is not used. `Name(str):`*<Name>*: A character string is used for the domain name. `Name(dns):`*<Name>*: A domain name server name is used for the domain name. `Name(mac):`*<MAC>*`(`*ID*`)`: A MAC address and ID are used for the domain name.
MA *<No.>*	MA ID number and MA name	*<No.>*: Configured MA ID number `Name(str):`*<Name>*: A character string is used for the MA name. `Name(id):`*<ID>*: A numeric value is used for the MA name. `Name(vlan):`*<VLAN ID>*: A 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 belonging to the MA. `-` is displayed if no VLANs have been configured.
CC	Operating status of the CC	`Enable`: CC is enabled. `Disable`: CC is disabled.
Interval	CCM transmission interval	`1s`: The interval for sending CCMs is 1 second. `10s`: The interval for sending CCMs is 10 seconds. `1min`: The interval for sending CCMs is 1 minute. `10min`: The interval for sending CCMs is 10 minutes. `-` is displayed if CC is disabled.

Item	Meaning	Displayed detailed information
Alarm Priority	Failure detection level	The value of the failure detection level at which alarms are issued If a failure whose level is equal to or higher than the failure detection level that has been set occurs, an alarm is reported. ● 0: Indicates that no alarms are reported. ● 1: Indicates that a failure was detected on the remote MEP. ● 2: Indicates a port failure on the remote MEP. ● 3: Indicates 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 issued	2500 to 10000 ms: The time lapsing from the detection of a failure until an alarm is issued - is displayed if CC is not operating.
Reset Time	Time from the detection of a failure until an alarm is canceled	2500 to 10000 ms: The time lapsing 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
<IF#>	Port number	MEP port number
CH*<Channel group#>*	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.	--

Item	Meaning	Displayed detailed information
MAC	MEP MAC address	- is displayed if the status of the port to which the MEP belongs is Down.
Status	The 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 transmission interval, was received. ● Timeout: Indicates 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 any failure has not been detected.
MIP Information	MIP information	--
<IF#>	Port number	MIP port number
CH*<Channel group#>*	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 is an example of displaying the number of entities accommodated in the CFM configuration.

Figure 38-4 Example of displaying the number of entities accommodated in the CFM configuration

```
> show cfm summary

Date 2010/09/28 09:31:36 UTC
DownMEP Counts    :       1
```

```
UpMEP Counts      :       1
MIP Counts        :       3
CFM Port Counts   :       4

>
```

Display items in Example 2

Table 38-6 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 ports from which CFM PDUs are sent in the primary VLAN that has been set for the MA in the configuration

Impact on communication

None

Response messages

Table 38-7 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.
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 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 functionality of CFM, and the status of connection monitoring between the Switch 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.

Operation 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

The following figure is an example of displaying detailed remote MEP information.

Operation when this parameter is omitted:

Summary information about the remote MEP is displayed.

Operation when all parameters are omitted:

Summary information about all remote MEPs is displayed.

Example 1

The following figure is an example of displaying remote MEP information.

Figure 38-5 Example of displaying remote MEP information

```
> show cfm remote-mep

Date 2010/09/29 06:05:00 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.e254.dbf1  Time:2010/09/29 05:54:17
      ID:15    Status:RDI         MAC:00ed.f006.0118  Time:2010/09/29 06:04:15
  MA 200   Name(str) : Tokyo_to_Nagoya
    MEP ID:8012  CH1 (Up)    Enable   Status:-
      RMEP Information  Counts:  2
      ID:8003  Status:-           MAC:0012.e254.dc20  Time:2010/09/29 06:04:17
```

```
                ID:8004  Status:-          MAC:00ed.f006.0108  Time:2010/09/29 06:04:35

>
```

Display items in Example 1

Table 38-8 Items displayed for 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>*: Domain level `Name:-`: Indicates that the domain name is not used. `Name(str):`*<Name>*: A character string is used for the domain name. `Name(dns):`*<Name>*: A domain name server name is used for the domain name. `Name(mac):`*<MAC>*`(`*ID*`)`: A MAC address and ID are used for the domain name.
MA *<No.>*	MA ID number and MA name	*<No.>*: Configured MA ID number `Name(str):`*<Name>*: A character string is used for the MA name. `Name(id):`*<ID>*: A numeric value is used for the MA name. `Name(vlan):`*<VLAN ID>*: A VLAN ID is used for the MA name.
MEP ID	MEP ID for the Switch	--
<IF#>	Port number	MEP port number
CH*<Channel group#>*	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	The highest-level failure of the failures detected by the Switch's 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 transmission interval, was received. ● `Timeout`: Indicates 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 any failure has not 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	The highest-level failure of the failures detected by the remote 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 transmission interval, was received. ● Timeout: Indicates 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 any failure has not 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 is an example of displaying detailed remote MEP information.

Figure 38-6 Example of displaying detailed remote MEP information

```
> show cfm remote-mep detail

Date 2010/09/29 06:05:03 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.e254.dbf1  Time:2010/09/29 05:54:17
        Interface:Down             Port:Blocked       RDI:-
        Chassis ID Type:MAC        Info: 0012.e254.dbf0
      ID:15    Status:RDI         MAC:00ed.f006.0118  Time:2010/09/29 06:04:15
        Interface:Up               Port:Forwarding    RDI:On
        Chassis ID Type:MAC        Info: 00ed.f006.0001
```

```
MA 200   Name(str) : Tokyo_to_Nagoya
  MEP ID:8012  CH1 (Up)    Enable   Status:-
    RMEP Information  Counts:  2
    ID:8003  Status:-          MAC:0012.e254.dc20  Time:2010/09/29 06:04:17
      Interface:Up              Port:Forwarding    RDI:-
      Chassis ID Type:MAC       Info: 0012.e254.dbf0
    ID:8004  Status:-          MAC:00ed.f006.0108  Time:2010/09/29 06:04:35
      Interface:Up              Port:Forwarding    RDI:-
      Chassis ID Type:MAC       Info: 00ed.f006.0001

>
```

Display items in Example 2

Table 38-9 Items displayed for detailed remote MEP information

Item	Meaning	Displayed detailed information
Total RMEP Counts	Total number of remote MEPs	--
Domain Level *<Level>*	Domain level and domain name	*<Level>*: Domain level `Name:-`: Indicates that the domain name is not used. `Name(str):`*<Name>*: A character string is used for the domain name. `Name(dns):`*<Name>*: A domain name server name is used for the domain name. `Name(mac):`*<MAC>*`(`*ID*`)`: A MAC address and ID are used for the domain name.
MA *<No.>*	MA ID number and MA name	*<No.>*: Configured MA ID number `Name(str):`*<Name>*: A character string is used for the MA name. `Name(id):`*<ID>*: A numeric value is used for the MA name. `Name(vlan):`*<VLAN ID>*: A VLAN ID is used for the MA name.
MEP ID	MEP ID for the Switch	--
<IF#>	Port number	MEP port number
CH*<Channel group#>*	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.	--

Item	Meaning	Displayed detailed information
Status	The status of failure detection on the Switch's MEP	The highest-level failure of the failures detected by the Switch's 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 transmission interval, was received. ● `Timeout`: Indicates 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 any failure has not 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	The highest-level failure of the failures detected by the remote 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 transmission interval, was received. ● `Timeout`: Indicates 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 any failure has not 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 Up status. ● `Down`: Indicates 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 for the following cases:

Item	Meaning	Displayed detailed information
		● This information is not in the received CCM. ● The failure information has been cleared by the `clear cfm fault` command.
Port	The status of the remote MEP port	The status of PortStatus in the CCM that was last received. ● `Forwarding`: Indicates Forwarding status. ● `Blocked`: Indicates blocking status. `-` is displayed for the following cases: ● This information is not in the received CCM. ● The failure information has been cleared by the `clear cfm fault` command.
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`: A failure is being detected. `-` is displayed for the following cases: ● No failure has been detected. ● The failure information has been cleared by the `clear cfm fault` command.
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`. ● `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 in the received CCM. For this information sent from the Switch, MAC is displayed for `Type` and the MAC address of the Switch is displayed for `Info`.

Item	Meaning	Displayed detailed information
Info	Information about the chassis ID	Information displayed for `Type`. `-` is displayed if this information is not in the received CCM.

Impact on communication

None

Response messages

Table 38-10 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.
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 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 the 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.

Operation 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.

Operation when all parameters are omitted:

All remote MEP information is cleared.

Example

The following figure is an example of clearing remote MEP information.

Figure 38-7 Example of clearing remote MEP information

```
> clear cfm remote-mep
>
```

Display items

None

Impact on communication

None

Response messages

Table 38-11 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.

Message	Description
CFM is not configured.	CFM has not been configured. Check the configuration.

Notes

None

show cfm fault

Displays the type of failure that has been detected by the CC functionality 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.

Operation 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.

Operation when this parameter is omitted:

Summary information about a failure is displayed.

Operation when all parameters are omitted:

Summary information about all failures is displayed.

Example 1

Display summary information about a CFM failure.

Figure 38-8 Example of displaying failure information

```
> show cfm fault

Date 2010/09/29 07:28:29 UTC
MD:6  MA:100   MEP:600   Cleared  Time:-
MD:7  MA:1000  MEP:1000  Fault    Time:2010/09/29 07:27:20
MD:7  MA:1010  MEP:1011  Cleared  Time:-

>
```

Display items in Example 1

Table 38-12 Items displayed for failure information

Item	Meaning	Displayed detailed information
MD	Domain level	0 to 7
MA	MA ID number	Configured MA ID number
MEP	MEP ID	MEP ID for the Switch
Fault	A failure is being detected.	--
Cleared	A failure has been cleared.	--
Time	Time a failure was detected	The time 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 is an example of displaying detailed information about a CFM failure.

Figure 38-9 Example of displaying detailed failure information

```
> show cfm fault domain-level 7 detail

Date 2010/09/29 07:28:32 UTC
MD:7  MA:1000  MEP:1000  Fault
  OtherCCM : -  RMEP:1001 MAC:0012.e254.dbff VLAN:1000 Time:2010/09/29 07:18:44
  ErrorCCM : On RMEP:1001 MAC:0012.e254.dbff VLAN:1000 Time:2010/09/29 07:27:45
  Timeout  : On RMEP:1001 MAC:0012.e254.dbff VLAN:1000 Time:2010/09/29 07:27:20
  PortState: -
  RDI      : -  RMEP:1001 MAC:0012.e254.dbff VLAN:1000 Time:2010/09/29 07:23:45
MD:7  MA:1010  MEP:1011  Cleared
  OtherCCM : -
  ErrorCCM : -  RMEP:1010 MAC:0012.e254.dc01 VLAN:1011 Time:2010/09/29 07:19:01
  Timeout  : -  RMEP:1010 MAC:0012.e254.dc01 VLAN:1011 Time:2010/09/29 07:18:44
  PortState: -
  RDI      : -  RMEP:1010 MAC:0012.e254.dc01 VLAN:1011 Time:2010/09/29 07:21:01

>
```

Display items in Example 2

Table 38-13 Items displayed for detailed failure information

Item	Meaning	Displayed detailed information
MD	Domain level	0 to 7
MA	MA ID number	Configured MA ID number
MEP	MEP ID	MEP ID for the Switch

Item	Meaning	Displayed detailed information
Fault	A failure is being detected.	--
Cleared	A failure has been cleared.	--
OtherCCM	Failure level 5 A CCM was received from another MA.	Indicates that a CCM was received from the remote MEP belonging to another MA. On: A failure was found. -: 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 transmission 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 is being 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	Displays the ID of the remote MEP that sent the CCM when the last failure was detected.
MAC	MAC address of the remote MEP	--
VLAN	VLAN that received a CCM	--
Time	Time a failure was detected	The time a failure was detected *yyyy/mm/dd hh:mm:ss* year/month/day hour:minute:second

Impact on communication

None

Response messages

Table 38-14 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.

Message	Description
CFM is not configured.	CFM has not been configured. Check the configuration.
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 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 fault

Clears the 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.

Operation 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.

Operation when all parameters are omitted:

All failure information is cleared.

Example

The following figure is an example of clearing CFM failure information.

Figure 38-10 Example of clearing CFM failure information

```
> clear cfm fault
>
```

Display items

None

Impact on communication

None

Response messages

Table 38-15 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.

Notes

None

show cfm l2traceroute-db

Displays routing 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 on the route that will be displayed.

domain-level *<Level>*

Specify the domain level to which the destination remote MEP or MIP belongs.

ma *<No.>*

Specify the MA ID number to which the destination remote MEP or MIP belongs.

detail

Displays detailed information about the route and the MP on the route.

Operation when this parameter is omitted:

Only the routing information is displayed.

Operation when all parameters are omitted:

All routing information in the linktrace database is displayed.

Example 1

The following figure is an example of displaying routing information in the linktrace database.

Figure 38-11 Example of displaying linktrace database information

```
> show cfm l2traceroute-db

Date 2010/09/29 08:28:28 UTC
L2traceroute to MP:0012.e254.dc09 on Level:3  MA:300   MEP:300  VLAN:300
Time:2010/09/29 08:21:05
63   00ed.f205.0111  Forwarded
62   0012.e254.dc09  NotForwarded  Hit

>
```

Display items in Example 1

Table 38-16 Items displayed for 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 a remote MEP or MIP is specified. *<Remote MEP ID>*(*<Remote MAC address>*): When a remote MEP ID is specified.
Level	Domain level	0 to 7
MA	MA ID number	Configured MA ID number
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 is an example of displaying detailed linktrace database information.

Figure 38-12 Example of displaying detailed linktrace database information

```
> show cfm l2traceroute-db detail

Date 2010/09/29 08:45:32 UTC
L2traceroute to MP:302(0012.e254.dc09) on Level:3  MA:300   MEP:300  VLAN:300
Time:2010/09/29 08:35:02
63   00ed.f205.0111  Forwarded
  Last Egress : 00ed.f205.0001  Next Egress : 00ed.f205.0001
  Relay Action: MacAdrTbl
  Chassis ID    Type: MAC       Info: 00ed.f205.0001
  Ingress Port  Type: LOCAL      Info: Port 0/1
    MP Address: 00ed.f205.0101  Action: OK
  Egress Port   Type: LOCAL      Info: Port 0/17
    MP Address: 00ed.f205.0111  Action: OK
62   0012.e254.dc09  NotForwarded  Hit
  Last Egress : 00ed.f205.0001  Next Egress : 0012.e254.dbf0
```

```
    Relay Action: RlyHit
    Chassis ID    Type: MAC       Info: 0012.e254.dbf0
    Ingress Port  Type: LOCAL      Info: Port 0/17
      MP Address: 0012.e254.dc01  Action: OK
    Egress Port   Type: LOCAL      Info: Port 0/25
      MP Address: 0012.e254.dc09  Action: OK

>
```

Display items in Example 2

Table 38-17 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 a remote MEP or MIP is specified. *<Remote MEP ID>*(*<Remote MAC address>*): When a remote MEP ID is specified.
Level	Domain level	0 to 7
MA	MA ID number	Configured MA ID number
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 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 in the received linktrace reply. The device MAC address is used for sending this information from the Switch to another device.

Item	Meaning	Displayed detailed information
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.
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 in the received linktrace reply. For this information sent from the Switch, MAC is displayed for `Type` and the MAC address of the Switch is displayed for `Info`.
Info	Information about the chassis ID	Information displayed for `Type`. `-` is displayed if this information is not in the received linktrace reply.
Ingress Port	Information about MP ports that received a linktrace message	--

Item	Meaning	Displayed detailed information
Type	Subtype of the ingress port	Type of the information displayed for `Info`. ● `PORT`: Indicates that `ifAlias` of the interface MIB is displayed for `Info`. ● `COMP`: Indicates that `entPhysicalAlias` 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`. ● `AGENT`: Indicates that `Agent Circuit ID` defined in IETF RFC 3046 is displayed for `Info`. ● `LOCAL`: Indicates that local of the CFM MIB is displayed for `Info`. `-` is displayed if this information is not in the received linktrace reply. For this information sent from the Switch, `LOCAL` is displayed for `Type` and the following character string is displayed for `Info`: `Port`*<IF#>*: Port number `CH` *<Channel group#>*: Channel group number
Info	Ingress port information	Information displayed for `Type`. `-` is displayed if this information is not in the received linktrace reply.
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 in the received linktrace reply.
Action	Status of the port that received a linktrace message	Displays the status of the MP port that received the linktrace message of each device. ● `OK`: Indicates normal status. ● `Down`: Indicates Down status. ● `Blocked`: Indicates Blocked status. ● `NoVLAN`: Indicates that there is no VLAN setting for linktrace messages. `-` is displayed if this information is not in the received linktrace reply.
Egress Port	Port information for the MP that forwarded a linktrace message	--

Item	Meaning	Displayed detailed information
Type	Subtype of the egress port	Type of the information displayed for `Info`. ● `PORT`: Indicates that `ifAlias` of the interface MIB is displayed for `Info`. ● `COMP`: Indicates that `entPhysicalAlias` 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`. ● `AGENT`: Indicates that `Agent Circuit ID` defined in IETF RFC 3046 is displayed for `Info`. ● `LOCAL`: Indicates that local of the CFM MIB is displayed for `Info`. `-` is displayed if this information is not in the received linktrace reply. For this information sent from the Switch, `LOCAL` is displayed for `Type` and the following character string is displayed for `Info`: `Port`*<IF#>*: Port number `CH`*<Channel group#>*: Channel group number
Info	Egress port information	Information displayed for `Type`. `-` is displayed if this information is not in the received linktrace reply.
MP Address	MAC address of the MP that forwarded the linktrace message	MAC address of the MP of those configured on the egress ports that sent the linktrace message `-` is displayed if this information is not 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 normal status. ● `Down`: Indicates Down status. ● `Blocked`: Indicates Blocked status. ● `NoVLAN`: Indicates that there is no VLAN setting for linktrace messages. `-` is displayed if this information is not in the received linktrace reply.

Impact on communication

None

Response messages

Table 38-18 List of response messages for the show cfm l2traceroute-db command

Message	Description
CFM is not configured.	CFM has not been configured. Check the configuration.

Message	Description
No such destination MAC address.	The specified destination MAC address is unknown. Make sure the specified parameter is correct, and then try again.
No such Domain Level.	The specified domain level is unknown. Make sure the specified parameter is correct, and then try again.
No such MA.	The specified MA ID is unknown. Make sure the specified parameter is correct, and then try again.
No such Remote MEP.	The specified remote MEP is unknown. Make sure the specified parameter is correct, and then try again.

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.

clear cfm l2traceroute-db

Clears CFM linktrace database information.

Syntax

```
clear cfm l2traceroute-db
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure is an example of clearing CFM linktrace database information.

Figure 38-13 Example of clearing CFM linktrace database information

```
> clear cfm l2traceroute-db
>
```

Display items

None

Impact on communication

None

Response messages

Table 38-19 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.

Notes

None

show cfm statistics

Displays the 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.

Operation 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.

Operation when all parameters are omitted:

All CFM statistics are displayed.

Example

The following figure is an example of displaying CFM statistics.

Figure 38-14 Example of displaying CFM statistics

```
> show cfm statistics domain-level 3

Date 2010/09/29 08:26:39 UTC
Domain Level 3 Name(str): ProviderDomain_3
  MA 300   Name(str) : Tokyo_to_Osaka_300
    MEP ID:300   0/1 (Up)    CFM:Enable
      CCM Tx:         23  Rx:         23  RxDiscard:         0
      LBM Tx:          5  Rx:          5  RxDiscard:         0
      LBR Tx:          5  Rx:          5  RxDiscard:         0
      LTM Tx:          3  Rx:          1  RxDiscard:         0
      LTR Tx:          1  Rx:          6  RxDiscard:         0
                                  Other RxDiscard:         0
  MIP Information
    0/17(Up)    CFM:Enable
      CCM Tx:          -  Rx:          -  RxDiscard:         -
      LBM Tx:          -  Rx:          5  RxDiscard:         0
      LBR Tx:          5  Rx:          -  RxDiscard:         -
      LTM Tx:          -  Rx:          4  RxDiscard:         0
      LTR Tx:          4  Rx:          -  RxDiscard:         -
                                  Other RxDiscard:         0

>
```

Display items

Table 38-20 Items displayed for CFM statistics

Item	Meaning	Displayed detailed information
Domain Level *<Level>*	Domain level and domain name	*<Level>*: Domain level `Name:-`: Indicates that the domain name is not used. `Name(str):`*<Name>*: A character string is used for the domain name. `Name(dns):`*<Name>*: A domain name server name is used for the domain name. `Name(mac):`*<MAC>*`(`*ID*`)`: A MAC address and ID are used for the domain name.
MA *<No.>*	MA ID number and MA name	*<No.>*: Configured MA ID number `Name(str):`*<Name>*: A character string is used for the MA name. `Name(id):`*<ID>*: A numeric value is used for the MA name. `Name(vlan):`*<VLAN ID>*: A VLAN ID is used for the MA name.
MEP ID	MEP ID for the Switch	--
<IF#>	Port number	MEP port number
CH*<Channel group#>*	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	Operating status of CFM on a port	The operating status of CFM on a 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	--
<IF#>	Port number	MIP port number
CH*<Channel group#>*	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.

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.
CFM		Operating status of CFM on a port	The operating status of CFM on a port to which MIP belongs. `Enable`: Indicates that CFM on the port is enabled. `Disable`: Indicates that CFM on the port is disabled.
CCM	Tx	Number of CCM transmissions	- is displayed for MIP.
	Rx	Number of CCM receptions	- is displayed for MIP.
	RxDiscard	Number of discarded CCMs	For an MEP, the following CCMs are discarded: ● CCM with an invalid format ● CCM for another MA ● CCM with the same MEP ID as the one set for the Switch ● CCM whose transmission interval is different from the Switch's MA ● CCM with a low domain level - 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.

Item		Meaning	Displayed detailed information
	RxDiscard	Number of loopback replies that have been discarded	For an MEP, the following loopback replies are discarded: ● A loopback reply with an invalid format ● A loopback reply whose destination MAC address is different from the MAC address of the MEP ● A loopback reply whose source MAC address is the multicast address or broadcast address ● A loopback reply whose `Loopback Transaction Identifier` value is different from that in the loopback message that was sent ● A loopback reply that was received after the wait time for a response that was set by an operation command expired - is displayed for MIP.
LTM	Tx	Number of linktrace messages that have been sent	- is displayed for MIP.
	Rx	Number of linktrace messages that have been received	--
	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

Item		Meaning	Displayed detailed information
			by an operation command expired - is displayed for MIP.
Other RxDiscard		Number of other CFM PDUs that have been discarded	A count of the number of unsupported CFM PDUs

Impact on communication

None

Response messages

Table 38-21 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.
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 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 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
<Channel group# list>]]
```

Input mode

User mode and administrator mode

Parameters

domain-level *<Level>*

Clears CFM statistics for the specified domain level.

ma *<No.>*

Clears CFM statistics for the specified MA ID number.

mep *<MEPID>*

Clears CFM statistics for the specified MEP ID.

mip

Clears CFM statistics for MIP.

port *<Port# list>*

Clears CFM 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 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*.

Operation 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.

Operation when all parameters are omitted:

All CFM statistics are cleared.

Example

The following figure is an example of clearing CFM statistics.

Figure 38-15 Example of clearing CFM statistics

```
> clear cfm statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 38-22 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.

Notes

None

39. SNMP

show snmp engineID local
set snmp-server engineID local

show snmp engineID local

Displays SNMP engine ID information.

Syntax

```
show snmp engineID local
```

Input mode

User mode and administrator mode

Parameters

None

Example 1

Figure 39-1 Example of displaying SNMP engine ID

```
> show snmp engineID local

Date 2011/02/13 09:18:56 UTC
Local SNMP engineID              : 8000554F043235333073203031323334353637383 9
Boot count since engineID change : 12

>
```

Display items

Table 39-1 Items displayed for SNMP engine ID information

Item	Meaning	Displayed detailed information
Local SNMP engineID	SNMP engine ID	--
Boot count since engineID change	Boot count after SNMP engine ID has been changed	--

Impact on communication

None

Response messages

None

Notes

None

set snmp-server engineID local

Sets the SNMP engine ID for SNMPv3 and the boot counts after the SNMP engine ID is changed.

For details on this command setting, see *23 Using SNMP to Manage Networks* in the *Configuration Guide Vol.2*.

Syntax

```
set snmp-server engineID local <engineid octet-string> <count>
```

Input mode

Administrator mode

Parameters

<engineid octet-string>

Specifies the SNMP engine ID or hyphen (-).

The specifiable range of values are a string of the even number of 2 to 64 digits in the hexadecimal representation or hyphen (-).

<count>

Specifies the value to be used for the boot count after the SNMP engine ID is changed.

The specifiable values are from 0 to 2147483647.

Example

```
set snmp-server engineID local - 0
```

Display items

None

Impact on communication

None

Response messages

Table 39-2 List of response messages for the set snmp-server engineID local command

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

Notes

- This command is to be used to correct the SNMP engine ID or the boot count after the SNMP engine ID is changed in the event that an unexpected restart takes place. This command is not intended for the regular operation.
- If the boot counts exceeds the upper limit 2147483647, all SNMP message authentication fails. In such case, execute the `snmp-server engineID local` configuration command to change the engine ID and initialize the boot count.

40. sFlow

show sflow
clear sflow statistics

show sflow

Displays the configuration setting status and operating 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 operating status of sFlow statistics.

Example

Figure 40-1 Example of displaying the setting status and the operating status of sFlow statistics

```
> show sflow

Date 2012/07/26 01:37:12 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared: 17:13:01
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: 0/2-4
 Configured sFlow egress ports : ----
 Received sFlow samples:       1043  Dropped sFlow samples        :          0
 Exported sFlow samples:       1043  Couldn't export sFlow samples:          0
 Overflow time of sFlow queue: 0 seconds
sFlow collector data :
 Collector IP address: 192.168.1.100  UDP: 6343  Source IP address: 192.168.1.253
  Send FlowSample UDP packets   :       1043  Send failed packets:          0
  Send CounterSample UDP packets:        372  Send failed packets:          0
 Collector IP address: 192.168.1.101  UDP: 6343  Source IP address: 192.168.1.253
  Send FlowSample UDP packets   :       1043  Send failed packets:          0
  Send CounterSample UDP packets:        372  Send failed packets:          0

>
```

Figure 40-2 Example of displaying detailed information about the setting status and the operating status of sFlow statistics

```
> show sflow detail

Date 2012/07/26 01:37:15 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared: 17:13:05
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: 0/2-4
 Configured sFlow egress ports : ----
```

```
 Received sFlow samples:       1043  Dropped sFlow samples        :          0
 Exported sFlow samples:       1043  Couldn't export sFlow samples:          0
 Overflow time of sFlow queue: 0 seconds
sFlow collector data :
 Collector IP address: 192.168.1.100  UDP: 6343  Source IP address: 192.168.1.253
  Send FlowSample UDP packets   :       1043  Send failed packets:          0
  Send CounterSample UDP packets:        372  Send failed packets:          0
 Collector IP address: 192.168.1.101  UDP: 6343  Source IP address: 192.168.1.253
  Send FlowSample UDP packets   :       1043  Send failed packets:          0
  Send CounterSample UDP packets:        372  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 2048 packets
 Target ports for CounterSample: 0/2-4

>
```

Display items

Table 40-1 Items displayed for sFlow statistics

Item	Displayed information
sFlow service status	Indicates the current operating status of sFlow statistics. (`disable` is displayed if the target port is not specified.)
Progress time from sFlow statistics cleared	Indicates the time elapsed after sFlow statistics has started or the time elapsed after the `clear sflow statistics` command was last executed. *hh*`:`*mm*`:`*ss*: (when the elapsed time is within 24 hours: *hh* = hours, *mm* = minutes, *ss* = seconds) *D* `day`: (when the elapsed time is over 24 hours: *D* = number of days)
sFlow service version	Version of the sFlow packet.
CounterSample interval rate	Sending interval (in seconds) between counter samples
Default configured rate	Sampling interval for the entire Switch set in the configuration.
Default actual rate	Actual sampling interval for the entire Switch
Configured sFlow ingress ports	Ports for which `sflow ingress` is set in the configuration and on which sFlow statistics are collected
Configured sFlow egress ports	Ports for which `sflow egress` is set in the configuration and on which sFlow statistics are collected
Received sFlow samples	Total number of packets which were sampled correctly
Dropped sFlow samples	Total number of packets discarded without being accumulated in the sFlow statistics queue for software if a higher-priority processing was processed on a Switch or notification over the Switch's performance was received. (The number of packets discarded because they could not be

Item	Displayed information
	accumulated in the sFlow statistics queue for the hardware is not included.)
Overflow time of sFlow queue	Length of time (in seconds) during which the sFlow statistics queue was full after the `clear sflow statistics` command was executed. If this value has increased, adjust the sampling interval.
Exported sFlow samples	Total number of sample packets contained in UDP packets sent to the collector
Couldn't export sFlow samples	Total number of sample packets contained in UDP packets that could not be sent
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[#1]
Send FlowSample UDP packets	Number of UDP packets for flow samples sent to the collector
Send failed packets	Number of UDP packets that could not be sent to the collector
Send CounterSample UDP packets	Number of UDP packets for counter samples sent to the collector
Max packet size	Maximum sFlow packet size
Packet information type	Basic data format for flow samples
Max header size	The maximum size of the sample packet when the header type is used as the basic data format
Extended information type	Extended data format for flow samples
Url port number	Port number used to determine if a packet is an HTTP packet when URL information is used for the extended data format
Sampling mode	Sampling method
random-number	Collection at a rate (random numbers) according to the sampling interval
Sampling rate to collector	Recommended sampling interval at which no packets are discarded. If there are problems at the current sampling interval, an applicable value is displayed. The value cannot be smaller than the value set in the configuration. If the sampling interval is changed, execute the `clear sflow statistics` command. The correct value might not be displayed until the command is executed.

Item	Displayed information
Target ports for CounterSample	Target port for counter samples

#1 If IPv6 routing information cannot be found (VLAN is in `DOWN` status), `----` is displayed.

Impact on communication

None

Response messages

Table 40-2 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 is not configured.	The sFlow functionality has not been configured. Check the configuration.

Notes

If the number of packets or the statistics counter exceeds the maximum value (32 bit counter), the value is reset to 0.

If no IP addresses or ports are set in the configuration, `----` is displayed.

clear sflow statistics

Clears statistics managed by sFlow statistics.

Syntax

```
clear sflow statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

```
> clear sflow statistics

>
```

Display items

None

Impact on communication

None

Response messages

Table 40-3 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 is not configured.	The sFlow functionality has not been configured. Check the configuration.

Notes

The number of packets that are discarded without being accumulated in the queue whose To-CPU queue number, which is displayed by executing the `show qos queueing` command, is 1 and queueing priority is 4 is also cleared.

Part 14: Management of Neighboring Device Information

41. LLDP

show lldp
clear lldp
show lldp statistics
clear lldp statistics

show lldp

Displays LLDP configuration information and neighboring device information.

Syntax

```
show lldp [port <port list>] [detail]
show lldp neighbors [port <port list>]
```

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*.

Operation 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.

Operation when this parameter is omitted:

The LLDP configuration information for the Switch and the neighboring device information are displayed in a simplified format.

neighbors

Displays summary information about the neighboring device.

Operation when this parameter is omitted:

LLDP configuration information and the neighboring device information are displayed.

Operation when all parameters are omitted:

The LLDP configuration information for the Switch and all neighboring device information are displayed in a simplified format.

Example 1

The following figure is an example of displaying the LLDP configuration information in a simplified format.

Figure 41-1 Example of displaying the LLDP configuration information and neighboring device information in a simplified format

```
> show lldp

Date 2012/11/30 14:44:03 UTC
Status: Enabled  Chassis ID: Type=MAC       Info=0012.e262.1faa
Interval Time: 30   Hold Count: 4  TTL: 120
Port Counts=4
  0/5         Link: Up    Neighbor Counts:   1  Draft Neighbor Counts:   0
  0/10        Link: Down  Neighbor Counts:   0  Draft Neighbor Counts:   0
  0/11        Link: Up    Neighbor Counts:   0  Draft Neighbor Counts:   1
  0/15(CH:7)  Link: Up    Neighbor Counts:   0  Draft Neighbor Counts:   0

>
```

Display items in Example 1

Table 41-1 Simplified display of LLDP setting information and neighboring device information

Item	Meaning	Displayed detailed information
Status	Status of the LLDP functionality on the Switch	`Enabled`: The LLDP functionality is enabled. `Disabled`: The LLDP functionality is disabled. When the status is `Disabled`, `LLDP is not configured` is displayed because there is no information.
Chassis ID	Chassis ID of the Switch	--
Type	Subtype for the chassis ID	`MAC`: Indicates that a MAC address is displayed for `Info`.
Info	MAC address of the Switch	--
Interval Time	Interval for sending 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
TTL	LLDPDU retention time to be reported to neighboring devices (in seconds)	10 to 65535
Port Counts	Number of ports	Number of ports that has been set for enable-port
<IF#>	Interface port number	Number of the interface 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 state	`Up`: Indicates that the port status is Up. `Down`: Indicates that the port status is Down.
Neighbor Counts	Number of neighboring devices whose information is retained	Number of neighboring devices whose information is retained by the applicable port
Draft Neighbor Counts	Total number of neighboring devices to be displayed that support IEEE 802.1AB/D6.0	Number of information items for neighboring devices to be displayed that support IEEE 802.1AB/D6.0

Example 2

The following is an example of displaying LLDP information when the `detail` parameter is specified.

Figure 41-2 Example of displaying detailed LLDP configuration information and neighboring device information

```
> show lldp detail

Date 2012/11/30 14:44:18 UTC
Status: Enabled  Chassis ID: Type=MAC     Info=0012.e262.1faa
Interval Time: 30  Hold Count: 4  TTL: 120
System Name: AX2530S-48T
System Description: ALAXALA AX2530 AX-2530-48T-B [AX2530S-48T] Switching software Ver.
3.5 [OS-L2B]
Neighbor Counts=1
Draft Neighbor Counts=1
Port Counts=4
Port 0/5
  Link: Up    PortEnabled: TRUE   AdminStatus: enabledRxTx                  ┐
  Neighbor Counts:   1  Draft Neighbor Counts:   0                          │
  Port ID: Type=MAC       Info=0012.e262.1faf                              │1
  Port Description: GigabitEther 0/5                                       │
  Tag ID: Untagged                                                         │
  LLDPDU Destination Address: 0180.c200.000e                               ┘
  Neighbor 1    TTL: 113                                                   ┐
    Chassis ID: Type=MAC       Info=0012.e292.b84d                         │
    System Name: AX2530S-24T231                                            │
    System Description: ALAXALA AX2530 AX-2530-24T-B [AX2530S-24T] Switching software
Ver. 3.5 [OS-L2B]                                                          │2
     Port ID: Type=MAC       Info=0012.e292.b84e                           │
     Port Description: GigabitEther 0/1                                    │
     Tag ID: Untagged                                                      │
     IPv4 Address: Untagged      172.31.0.231                              │
     IPv6 Address: Untagged      2001:172::231                             ┘
Port 0/10
  Link: Down  PortEnabled: FALSE  AdminStatus: enabledRxTx                 ┐1
  Neighbor Counts:   0  Draft Neighbor Counts:   0                         ┘
Port 0/11
  Link: Up    PortEnabled: TRUE   AdminStatus: enabledRxTx                 ┐
  Neighbor Counts:   0  Draft Neighbor Counts:   1                          │
  Port ID: Type=MAC       Info=0012.e262.1fb5                              │1
  Port Description: GigabitEther 0/11                                      │
  Tag ID: Untagged                                                         │
  LLDPDU Destination Address: 0100.8758.1310                               ┘
  Draft Neighbor 1    TTL: 115                                             ┐
    Chassis ID: Type=MAC       Info=0012.e288.c1c5                         │
    System Name: AX2430-24T2X                                              │
    System Description: ALAXALA AX2430 AX-2430-24T2XE-B [AX2430S-24T2X] Switching
software Ver. 11.5.B [OS-L2]                                               │3
     Port ID: Type=MAC       Info=0012.e288.c1d1                           │
     Port Description: GigabitEther 0/12                                   │
     Tag ID: Untagged                                                      │
     IPv4 Address: Untagged      192.168.4.240                             ┘
Port 0/15(CH:7)
  Link: Up    PortEnabled: TRUE   AdminStatus: enabledRxTx                 ┐
  Neighbor Counts:   0  Draft Neighbor Counts:   0                          │
  Port ID: Type=MAC       Info=0012.e262.1fb9                              │1
  Port Description: GigabitEther 0/15                                      │
  Tag ID: Untagged                                                         │
  LLDPDU Destination Address: 0100.8758.1310                               ┘

>
```

1. Information about the Switch's port
2. Information about neighboring devices (when received by LLDP IEEE 802.1AB-2005 or IEEE 802.1AB-2009)

3. Information about neighboring devices (when received by LLDP IEEE 802.1AB/D6.0)

Display items in Example 2

Table 41-2 Detailed display of LLDP setting information and neighboring device information

Item	Meaning	Displayed detailed information
Status	Status of the LLDP functionality on the Switch	`Enabled`: The LLDP functionality is enabled. `Disabled`: The LLDP functionality is disabled. When the status is `Disabled`, `LLDP is not configured` is displayed because there is no information.
Chassis ID	Chassis ID of the Switch	--
Type	Subtype for the chassis ID	`MAC`: Indicates that a MAC address is displayed for `Info`.
Info	MAC address of the Switch	--
Interval Time	Interval for sending 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
TTL	LLDPDU retention time to be reported to neighboring devices (in seconds)	10 to 65535
System Name	System name of the Switch	The character string that has been set by the `hostname` command parameter This item is not displayed if the information has not been set in the configuration.
System Description	System description of the Switch	The same character string as the string used for the MIB (sysDescr)
Neighbor Counts	Total number of neighboring devices that are to be displayed	Number of neighboring devices whose information is retained by the Switch
Draft Neighbor Counts	Total number of neighboring devices to be displayed that support IEEE 802.1AB/D6.0	Number of information items for neighboring devices to be displayed that support IEEE 802.1AB/D6.0
Port Counts	Number of ports	Number of ports for which the `lldp enable` configuration command is set
Port	Applicable port number	*<IF#>*

Item	Meaning	Displayed detailed information
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	Status that indicates whether LLDP operation is possible	`TRUE`: Indicates that LLDPDUs can be sent and received. `FALSE`: Indicates that LLDPDUs cannot be sent or received.
AdminStatus	LLDP administration status	Administration status that indicates whether to enable LLDP operation. `enabledRxTx`: Indicates that LLDPDUs can be sent and received. This item indicates whether the `lldp enable` configuration command has been executed. The value is fixed at `enabledRxTx` because port information is displayed only for the ports for which the `lldp enable` command has been executed.
Neighbor Counts	Number of neighboring devices	Number of neighboring devices whose information is retained by the applicable port
Draft Neighbor Counts	Number of neighboring devices that support IEEE 802.1AB/D6.0	Number of neighboring devices that support IEEE 802.1AB/D6.0 whose information is 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`. This item is always `MAC` (fixed).
Info	Information about the port ID	MAC address of the port
Port Description	Port description for the port	The same character string as the string used for the MIB (ifDescr).
Tag ID	List of VLANs to which the port belongs	VLAN ID list This item is not displayed if the information has not been set in the configuration.
IPv4 Address	Port IP address (IPv4)	This item is not displayed if the information has not been set in the configuration.
Untagged	VLAN to which an IP address has been assigned is `Untagged.`	--

Item	Meaning	Displayed detailed information
Tagged	VLAN ID for the VLAN to which an IP address has been assigned	The smallest ID is displayed if multiple IDs have been assigned.
<IP Address>	IP address that has been assigned	An IP address assigned to the VLAN that is described in the previous item.
IPv6 Address	Port IP address (IPv6)	This item is not displayed if the information has not been set in the configuration.
Untagged	VLAN to which an IP address has been assigned is `Untagged.`	--
Tagged	VLAN ID for the VLAN to which an IP address has been assigned	The smallest ID is displayed if multiple IDs have been assigned.
<IP Address>	IP address that has been assigned	An IP address assigned to the VLAN that is described in the previous item.
LLDPDU Destination Address	Destination MAC address to which LLDPDUs are sent by the applicable port	`0180.c200.000e`: Destination MAC address when LLDPDUs are sent `0100.8758.1310`: Destination MAC address when IEEE 802.1AB/D6.0 LLDPDUs are sent
Neighbor	Identification number of the neighboring device	A unique value for each port
Draft Neighbor	Identification number of the neighboring device that supports IEEE 802.1AB/D6.0	A 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 the alias of the device is displayed for `Info`. `IF-ALIAS`: Indicates that the alias of the interface is displayed for `Info`. `PORT-COMP`: Indicates that the alias of the physical port is displayed for `Info`. `MAC`: Indicates that the MAC address is displayed for `Info`. `NET`: Indicates that the network address is displayed for `Info`. `IF-NAME`: Indicates that the interface name is displayed for `Info`. `LOCAL`: Indicates that the locally defined value is displayed for `Info`.

Item	Meaning	Displayed detailed information
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 the alias of the interface is displayed for `Info`. `PORT-COMP`: Indicates that the alias of the physical port is displayed for `Info`. `MAC`: Indicates that the MAC address is displayed for `Info`. `NET`: Indicates that the network address is displayed for `Info`. `IF-NAME`: Indicates that the interface name is displayed for `Info`. `AGENT`: Indicates that the agent ID is displayed for `Info`. `LOCAL`: Indicates that locally defined value 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	Capabilities supported for the neighboring device	`Repeater`: Repeater functionality. `Bridge`: Bridge functionality. `WLAN-AP`: Wireless LAN access point `Router`: Router functionality `Telephone`: Voice call functionality. `DOCSIS`: DOCSIS cable device `Station`: Station only receiving `CVLAN-B`: C-VLAN Component of a VLAN bridge `SVLAN-B`: S-VLAN Component of a VLAN bridge. `TPMR`: Two-port MAC Relay `Other`: Other Multiple items are displayed if multiple capabilities have been reported. This item is not displayed if it has not been reported.
Enable Capabilities	Capabilities running on the neighboring device	`Repeater`: Repeater functionality. `Bridge`: Bridge functionality. `WLAN-AP`: Wireless LAN access

Item	Meaning	Displayed detailed information
		point `Router`: Router functionality `Telephone`: Voice call functionality. `DOCSIS`: DOCSIS cable device `Station`: Station only receiving `CVLAN-B`: C-VLAN Component of a VLAN bridge `SVLAN-B`: S-VLAN Component of a VLAN bridge. `TPMR`: Two-port MAC Relay `Other`: Other Multiple items are displayed if multiple capabilities have been 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.
Tag ID	List of VLANs to which the neighboring device port belongs	VLAN ID list This item is not displayed if it has not been reported.
IPv4 Address	IP address assigned to the neighboring device (IPv4)	This item is not displayed if it has not been reported.
Untagged	When the VLAN to which the IPv4 address of the neighboring device has been assigned is untagged	--
Tagged	VLAN ID for the VLAN to which the IPv4 address of the neighboring device has been assigned	The smallest ID is displayed if multiple IDs have been assigned.
<IP Address>	IPv4 address that has been assigned	An IP address assigned to the VLAN that is described in the previous item.
IPv6 Address	IP address assigned to the neighboring device (IPv6)	This item is not displayed if it has not been reported.
Untagged	When the VLAN to which the IPv6 address of the neighboring device has been assigned is untagged	--
Tagged	VLAN ID for the VLAN to which the IPv6 address of the neighboring device has been assigned	The smallest ID is displayed if multiple IDs have been assigned.
<IP Address>	IPv6 address that has been assigned	An IP address assigned to the VLAN that is described in the previous item.

Example 3

The following is an example of displaying summary information for neighboring devices when the `neighbors` parameter is specified.

Figure 41-3 Example of displaying neighboring device summary information

```
> show lldp neighbors

Date 2012/11/30 14:44:32 UTC
Neighbor Counts:   2
Neighbor Information
                Chassis                     Port
0/5             0012.e292.b84d              GigabitEther 0/1
0/11            0012.e288.c1c5              GigabitEther 0/12

>
```

Display items in Example 3

Table 41-3 Items displayed for neighboring device summary information

Item	Meaning	Displayed detailed information
Neighbor Counts	Total number of retained neighboring devices that are to be displayed	Number of retained information items for neighboring devices to be displayed
Neighbor Information	Neighboring device information	--
<IF#>	Interface port number	Interface port number of a port that retains information is to be displayed Only ports that retain neighboring device information are displayed.
CH	Channel group number	This item is displayed if the applicable port belongs to a channel group.
Chassis ID	Chassis ID of the neighboring device	Chassis ID in the retained neighboring device information. If the text is 25 characters or more, up to 24 characters are displayed, and the 25th and subsequent characters are omitted (the omitted part is replaced with `...`).
Port	Port description of the neighboring device	The port description of the retained neighboring device is displayed. If the text is 25 characters or more, up to 24 characters are displayed, and the 25th and subsequent characters are omitted (the omitted part is replaced with `...`). This item is not displayed if it has not been reported.

Impact on communication

None

Response messages

Table 41-4 List of response messages for the show lldp command

Message	Description
LLDP is not configured.	LLDP has not been configured. Check the configuration.

Notes

None

clear lldp

Clears LLDP neighboring device information.

Syntax

```
clear lldp
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 41-4 Example of executing the clear lldp command

```
> clear lldp

>
```

Display items

None

Impact on communication

None

Response messages

Table 41-5 List of response messages for the clear lldp command

Message	Description
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*.

Operation when this parameter is omitted:

Displays statistics for all LLDP frames by port.

Example

Figure 41-5 Example of displaying LLDP statistics

```
> show lldp statistics

Date 2012/11/30 14:44:40 UTC
Port Counts: 4
0/5    LLDPDUs     : Tx     =        40 Rx     =        40 Invalid=          0
                     Discard=         0 Ageouts=         0
       Discard TLV : TLVs   =         0 Unknown=         0
 Draft LLDPDUs     : Tx     =         0 Rx     =         0 Invalid=          0
       Discard TLV : TLVs   =         0
0/10   LLDPDUs     : Tx     =         0 Rx     =         0 Invalid=          0
                     Discard=         0 Ageouts=         0
       Discard TLV : TLVs   =         0 Unknown=         0
 Draft LLDPDUs     : Tx     =         0 Rx     =         0 Invalid=          0
       Discard TLV : TLVs   =         0
0/11   LLDPDUs     : Tx     =         0 Rx     =         0 Invalid=          0
                     Discard=         0 Ageouts=         0
       Discard TLV : TLVs   =         0 Unknown=         0
 Draft LLDPDUs     : Tx     =        46 Rx     =        47 Invalid=          0
       Discard TLV : TLVs   =         0
0/15   LLDPDUs     : Tx     =         0 Rx     =         0 Invalid=          0
                     Discard=         0 Ageouts=         0
       Discard TLV : TLVs   =         0 Unknown=         0
 Draft LLDPDUs     : Tx     =        30 Rx     =         7 Invalid=          0
       Discard TLV : TLVs   =         0

>
```

Display items

Table 41-6 Items displayed for the LLDP statistics

Item	Meaning	Displayed detailed information
Port counts	Number of ports subject to this statistics	--
Port	Port number	Port number for which statistics are to be displayed
LLDPDUs	Statistics for frames	Statistics for frames are displayed. Statistics for frames in IEEE 802.1AB/D6.0 are not included.
Tx	Number of LLDPDUs that have been sent	Number of LLDPDUs that have been sent. 0 to 4294967295
Rx	Number of LLDPDUs that have been received	Number of LLDPDUs that have been received. 0 to 4294967295
Invalid	Number of invalid LLDPDUs	Number of invalid LLDPDUs that have been received. 0 to 4294967295
Discard	Number of LLDPDUs that have been discarded	Number of LLDPDUs that have been discarded. 0 to 4294967295
Ageouts	Number of neighboring device information items whose retention period has expired	Number of neighboring device information items whose retention period has expired. 0 to 4294967295
Discard TLV	TLV statistics	TLV statistics are displayed. TLV statistics in IEEE 802.1AB/D6.0 are not included.
TLVs	Number of TLVs that have been discarded	Number of TLVs that have been discarded. 0 to 4294967295
Unknown	Number of TLVs that cannot be recognized	Number of TLVs that cannot be recognized. 0 to 4294967295
Draft	IEEE 802.1AB/D6.0 statistics	Statistics in IEEE 802.1AB/D6.0 are displayed.
LLDPDUs	Statistics for frames	Statistics for frames in IEEE 802.1AB/D6.0 are displayed
Tx	Number of LLDPDUs that have been sent	Number of IEEE 802.1AB/D6.0 LLDPDUs that have been sent. 0 to 4294967295
Rx	Number of LLDPDUs that have been received	Number of IEEE 802.1AB/D6.0 LLDPDUs that have been received. 0 to 4294967295

Item	Meaning	Displayed detailed information
Invalid	Number of invalid LLDPDUs	Number of invalid IEEE 802.1AB/D6.0 LLDPDUs that have been received. 0 to 4294967295
Discard TLV	TLV statistics	TLV statistics in IEEE 802.1AB/D6.0 are displayed.
TLVs	Number of TLVs that have been discarded	Number of IEEE 802.1AB/D6.0 TLVs that have been discarded. 0 to 4294967295

Impact on communication

None

Response messages

Table 41-7 List of response messages for the show lldp statistics command

Message	Description
LLDP is not configured.	LLDP has not been configured. Check the configuration.
There is no information. (lldp statistics)	There is no `lldp statistics` information.

Notes

None

clear lldp statistics

Clears LLDP statistics.

Syntax

```
clear lldp statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 41-6 Example of executing the clear lldp statistics command

```
> clear lldp statistics

>
```

Display items

None

Impact on communication

None

Response messages

Table 41-8 List of response messages for the clear lldp statistics command

Message	Description
LLDP is not configured.	LLDP has not been configured. Check the configuration.

Notes

None

Index

R

S

T

W