
AX6700S/AX6600S/AX6300S Software Manual

Operation Command Reference Vol. 2
For Version 11.7

AX63S-S011X-30

Alaxala

■ Relevant products

This manual applies to the models in the AX6700S, AX6600S, and AX6300S series of switches. It also describes the functionality of version 11.7 of the software for the AX6700S, AX6600S, and AX6300S series switches. The described functionality is that supported by the OS-S/OS-SE basic software and optional licenses.

■ 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

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

Ethernet is a registered trademark of Xerox Corporation.

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

IPX is a trademark of Novell, Inc.

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

Octpower is a registered trademark of NEC Corporation.

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

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

VitalQIP and VitalQIP Registration Manager are trademarks of Lucent Technologies.

VLANaccessClient is a trademark of NEC Soft, Ltd.

VLANaccessController and VLANaccessAgent are trademarks of NEC Corporation.

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

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

■ Reading and storing this manual

Before you use the 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 2012 (Edition 4) AX63S-S011X-30

■ Copyright

All Rights Reserved, Copyright(C), 2006, 2012, ALAXALA Networks, Corp.

History of Amendments

[For version 11.7]

Summary of amendments

Location and title	Changes
16 SNMP	<ul style="list-style-type: none">The following commands were added:<ul style="list-style-type: none">- show snmp- show snmp pending

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

[For version 11.4]

Summary of amendments

Item	Changes
DHCP snooping	<ul style="list-style-type: none">This chapter was added.

[For version 11.3]

The chapter Filters and all subsequent chapters that were in the manual *Operation Command Reference Vol.1* up to version 11.2 were moved to this manual.

For details about the summary of amendments for version 11.2 and earlier, see the manual *Operation Command Reference Vol. 1 For Version 11.7*.

Summary of amendments

Item	Changes
Access List Logging	<ul style="list-style-type: none">This chapter was added.

Preface

Applicable products and software versions

This manual applies to the models in the AX6700S, AX6600S, and AX6300S series of switches. It also describes the functionality of version 11.7 of the software for the AX6700S, AX6600S, and AX6300S series switches. The described functionality is that supported by the OS-S/OS-SE basic software and optional licenses.

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 functionality applicable to AX6700S, AX6600S, and AX6300S series switches. Functionality specific to a model is indicated as follows:

[AX6700S]:

The description applies to AX6700S switches.

[AX6600S]:

The description applies to AX6600S switches.

[AX6300S]:

The description applies to AX6300S switches.

Unless otherwise noted, this manual describes functionality applicable to the basic software OS-S/OS-SE. Functionality specific to an optional license is indicated as follows:

[OP-BGP]:

The description applies to the OP-BGP optional license.

[OP-DH6R]:

The description applies to the OP-DH6R optional license.

[OP-MBSE]:

The description applies to the OP-MBSE optional license.

[OP-NPAR]:

The description applies to the OP-NPAR optional license.

[OP-VAA]:

The description applies to the OP-VAA optional license.

Corrections to the manual

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

Intended readers

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

Readers must have an understanding of the following:

- The basics of network system management

Manual URL

You can view this manual on our website at:

<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.

● Unpacking the Switch and the basic settings for initial installation

AX6700S Quick Start Guide (AX67S-Q001X)	AX6600S Quick Start Guide (AX66S-Q001X)	AX6300S Quick Start Guide (AX63S-Q001X)
---	---	---

● Determining the hardware setup requirements and how to handle the hardware

AX6700S Hardware Instruction Manual (AX67S-H001X)	AX6600S Hardware Instruction Manual (AX66S-H001X)	AX6300S Hardware Instruction Manual (AX63S-H001X)
---	---	---

● Understanding the software functions, configuration settings, and operation commands

▽ First, see the following guides to check the functions and device capacities.

- | | | |
|--|----------------------------------|-----------------------------------|
| - Device capacities | - Filtering and QoS | - IPv4 and IPv6 packet forwarding |
| - Basic operations, such as logging in | - Layer 2 authentication | - IPv4 and IPv6 routing protocols |
| - VLANs and Spanning Tree Protocols | - High-reliability functionality | |

Configuration Guide Vol. 1 (AX63S-S001X)	Configuration Guide Vol. 2 (AX63S-S002X)	Configuration Guide Vol. 3 (AX63S-S003X)
---	---	---

▽ If necessary, see the following references.

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

Configuration Command Reference Vol. 1 (AX63S-S004X)	Configuration Command Reference Vol. 2 (AX63S-S010X)	Configuration Command Reference Vol. 3 (AX63S-S005X)
--	--	--

Operation Command Reference Vol. 1 (AX63S-S006X)	Operation Command Reference Vol. 2 (AX63S-S011X)	Operation Command Reference Vol. 3 (AX63S-S007X)
--	--	--

- Understanding messages and logs

Message and Log Reference (AX63S-S008X)
--

- Understanding MIBs

MIB Reference (AX63S-S009X)

● How to troubleshoot when a problem occurs

Troubleshooting Guide (AX36S-T001X)
--

Conventions: The terms "Switch" and "switch"

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

AX6700S series switch

AX6600S series switch

AX6300S series switch

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

Abbreviations used in the manual

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BCU	Basic Control Unit
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
BSU	Basic Switching Unit
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
CSU	Control and Switching Unit
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
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
LLPQ	Low Latency Priority Queueing
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LLRLQ	Low Latency Rate Limited 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
MSU	Management and Switching Unit
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
NIF	Network Interface
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
PRI	Primary Rate Interface

PS	Power Supply
PSNP	Partial Sequence Numbers PDU
PSP	Packet Switching Processor
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RGQ	Rate Guaranteed Queueing
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
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SOP	System Operational Panel
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
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
uRPF	unicast Reverse Path Forwarding
VAA	VLAN Access Agent
VLAN	Virtual LAN
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WGQ	Weighted Guaranteed Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

Conventions: KB, MB, GB, and TB

This manual uses the following conventions: 1 KB (kilobyte) is 1024 bytes. 1 MB (megabyte) is 1024² bytes. 1 GB (gigabyte) is 1024³ bytes. 1 TB (terabyte) is 1024⁴ bytes.

Contents

Preface	i
Applicable products and software versions	i
Corrections to the manual	i
Intended readers	i
Manual URL	ii
Reading sequence of the manuals	ii
Conventions: The terms "Switch" and "switch"	ii
Abbreviations used in the manual	iii
Conventions: KB, MB, GB, and TB	v

PART 1: Reading the Manual

1. Reading the Manual	1
Command description format	2
Specifiable values for parameters	4
List of character codes	6
Error messages displayed by the entry-error location detection functionality	7

PART 2: Filters

2. Filters	9
show access-filter	10
clear access-filter	16
3. Access List Logging	19
show access-log	20
clear access-log	22
show access-log flow	23
clear access-log flow	28
dump access-log	29
restart access-log	30
debug access-log	32
no debug access-log	34

PART 3: QoS

4. QoS	35
show qos-flow	36
clear qos-flow	42
show qos queueing	44
clear qos queueing	55
show qos queueing distribution	57
clear qos queueing distribution	65
show qos queueing interface	68
clear qos queueing interface	72
show qos queueing to-cpu	74
clear qos queueing to-cpu	79
show shaper	81

clear shaper	87
show shaper <port list>	88
clear shaper <port list>	94

PART 4: Layer 2 Authentication

5. IEEE802.1X 97

show dot1x statistics	98
show dot1x	103
clear dot1x statistics	112
clear dot1x auth-state	114
reauthenticate dot1x	117
restart dot1x	119
dump protocols dot1x	121
show dot1x logging	122
clear dot1x logging	131

6. Web Authentication 133

set web-authentication user	134
set web-authentication passwd	136
set web-authentication vlan	138
remove web-authentication user	139
show web-authentication user	141
show web-authentication login	143
show web-authentication logging	145
show web-authentication	160
show web-authentication statistics	164
clear web-authentication logging	167
clear web-authentication statistics	168
commit web-authentication	169
store web-authentication	171
load web-authentication	173
clear web-authentication auth-state	175
restart web-authentication	177
dump protocols web-authentication	179
set web-authentication html-files	180
clear web-authentication html-files	183
show web-authentication html-files	184

7. MAC-based Authentication 187

show mac-authentication login	188
show mac-authentication logging	190
show mac-authentication	203
show mac-authentication statistics	206
clear mac-authentication auth-state	208
clear mac-authentication logging	210
clear mac-authentication statistics	211
set mac-authentication mac-address	212
remove mac-authentication mac-address	214
commit mac-authentication	216
show mac-authentication mac-address	218
store mac-authentication	220
load mac-authentication	222
restart mac-authentication	224
dump protocols mac-authentication	225

8. Authentication VLANs [OP-VAA]	227
show fense server [OP-VAA]	228
show fense statistics [OP-VAA]	233
show fense logging [OP-VAA]	240
clear fense statistics [OP-VAA]	243
clear fense logging [OP-VAA]	244
restart vaa [OP-VAA]	245
dump protocols vaa [OP-VAA]	247

PART 5: Security

9. DHCP Snooping	249
show ip dhcp snooping binding	250
clear ip dhcp snooping binding	253
show ip dhcp snooping statistics	255
clear ip dhcp snooping statistics	257
show ip arp inspection statistics	258
clear ip arp inspection statistics	260
show ip dhcp snooping logging	261
clear ip dhcp snooping logging	274
restart dhcp snooping	275
dump protocols dhcp snooping	277

PART 6: High Reliability Based on Redundant Configurations

10. Redundancy of BCUs, CSUs, and MSUs	279
inactivate standby	280
activate standby	282
redundancy force-switchover	283
synchronize	285
11. GSRP	289
show gsrp	290
show gsrp aware	302
clear gsrp	304
set gsrp master	307
clear gsrp port-up-delay	309
clear gsrp forced-shift	311
restart gsrp	313
dump protocols gsrp	315
12. VRRP	317
show vrrpstatus (IPv4)	318
clear vrrpstatus (IPv4)	331
swap vrrp (IPv4)	333
show vrrpstatus (IPv6)	336
clear vrrpstatus (IPv6)	349
swap vrrp (IPv6)	351
show track (IPv4)	354
show track (IPv6)	358

PART 7: High Reliability Based on Network Failure Detection

13. IEEE 802.3ah/UDLD	363
show efmoam	364
show efmoam statistics	367
clear efmoam statistics	370
restart efmoam	371
dump protocols efmoam	373
14. L2 Loop Detection	375
show loop-detection	376
show loop-detection statistics	379
show loop-detection logging	382
clear loop-detection statistics	384
clear loop-detection logging	386
restart loop-detection	387
dump protocols loop-detection	389
15. CFM	391
l2ping	392
l2traceroute	395
show cfm	398
show cfm remote-mep	402
show cfm fault	408
show cfm l2traceroute-db	411
show cfm statistics	416
clear cfm remote-mep	421
clear cfm fault	423
clear cfm l2traceroute-db	425
clear cfm statistics	426
restart cfm	428
dump protocols cfm	430

PART 8: Remote Network Management

16. SNMP	431
show snmp	432
show snmp pending	437
snmp lookup	439
snmp get	440
snmp getnext	442
snmp walk	444
snmp getif	446
snmp getroute	448
snmp getarp	451
snmp getforward	453
snmp rget	456
snmp rgetnext	458
snmp rwalk	460
snmp rgetroute	462
snmp rgetarp	465
17. sFlow	467
show sflow	468
clear sflow statistics	471

restart sflow	472
dump sflow	473

PART 9: Management of Neighboring Device Information

18. LLDP 475

show lldp	476
show lldp statistics	482
clear lldp	484
clear lldp statistics	485
restart lldp	486
dump protocols lldp	488

19. OADP 489

show oadp	490
show oadp statistics	495
clear oadp	497
clear oadp statistics	499
restart oadp	501
dump protocols oadp	503

Index 505

Chapter

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 mode required to enter the command.

Parameters

Describes in detail the parameters that can be set by the command. For details on the behavior of a command when all omissible parameters are omitted, see *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 The time the command was accepted is displayed.

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

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

Input format	Interface name <interface name>
interface gigabitethernet	geth1/1 The numeric values represent <nif no.>/<port no.>.

Input format	Interface name <i><interface name></i>
interface tengigabitethernet	tengeth1/1 The numeric values represent <i><nif no.>/<port no.></i> .
interface vlan <i><vlan id></i>	VLAN0002 The last four digits represent <i><vlan id></i> .
interface loopback	loopback0 The numeric value represents <i><loopback id></i> .
interface null 0	null0
interface mgmt 0	MGMT0
interface async 1	ASync1

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 the entry-error location detection functionality are not described here. For details on these messages, see *Error messages displayed by the entry-error location detection functionality*.

The Switch assigns names to corresponding interfaces set by configuration. If *<interface name>* is shown in Response messages, the Switch displays any of the interface names listed in *Table 1-2: List of interface names assigned for input format*.

Notes

Provides cautionary information on using the command.

Specifiable values for parameters

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

Table 1-3: Specifiable values for parameters

Parameter type	Description	Input example
Name	For the names of access lists, alphabetic characters can be used for the first character, and alphanumeric characters, hyphens (-), underscores (_), and periods (.) can be used for the second and subsequent characters. Note that if the command input format permits specification of either a name, or a command name and parameters (or keywords), and you specify a name that is identical to a command name or a parameter (or keyword), the system assumes that the command or the parameter (or keyword) has been entered.	ip access-list standard <u>inbound1</u>
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
Wildcard mask	The same input format as IPv4 addresses. The set bits in an IPv4 address represent an arbitrary value.	255.255.0.0
IPv6 address	Specify this item in hexadecimal format, separating 2-byte hexadecimal values by colons (:).	3ffe:501:811:ff03::87ff:fed0:c7e0 fe80::200:87ff:fe5a:13c7
IPv6 address with an interface name (for a link-local address only)	Specify a percent (%) between an IPv6 address and an interface name. Only link-local IPv6 addresses can be used as this parameter type.	fe80::200:87ff:fe5a:13c7%VLAN0001

Range of <nif no.> and <port no.> values

The following tables list the range of parameter <nif no.> and <port no.> values.

Table 1-4: Range of <nif no.> values

#	Model	Range of <nif no.> values
1	AX6708S	1 to 8
2	AX6604S	1 to 4
3	AX6608S	1 to 8
4	AX6304S	1 to 4
5	AX6308S	1 to 8

Table 1-5: Range of <port no.> values [AX6700S] [AX6600S]

#	NIF type name abbreviation	Range of <port no.> values
1	NK1G-24T	1 to 24
2	NK1G-24S	1 to 24

#	NIF type name abbreviation	Range of <port no.> values
3	NK1GS-8M	1 to 8
4	NK10G-4RX	1 to 4
5	NK10G-8RX	1 to 8

Table 1-6: Range of <port no.> values [AX6300S]

#	NIF type name abbreviation	Range of <port no.> values
1	NH1G-16S	1 to 16
2	NH1G-24T	1 to 24
3	NH1G-24S	1 to 24
4	NH1G-48T	1 to 48
5	NH1GS-6M	1 to 6
6	NH10G-1RX	1
7	NH10G -4RX	1 to 4
8	NH10G -8RX	1 to 8

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

If <port list> is written in the parameter input format, use a hyphen (-), comma (,), or asterisk (*) in the <nif no.>/<port no.> format to specify multiple ports. You can also specify one port, as when <nif no.>/<port no.> is written as the parameter input format. The range of permitted values is the same as the range of <nif no.> and <port no.> values in the above tables.

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

1/1-3,5

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

/: Specify all ports on a switch

1/*: Specify all ports on a switch whose NIF number is 1.

How to specify <vlan id list>

If <vlan id list> is written in the parameter input format, use a hyphen (-) or comma (,) 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 comma (,):

1-3,5,10

How to specify <channel group list>

If <channel group list> is written in parameter input format, use a hyphen (-) or comma (,) 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 comma (,):

1-3,5,10

List of character codes

Character codes are listed in the following table.

Table 1-7: List of character codes

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

Note

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

Error messages displayed by the entry-error location detection functionality

The following table describes error messages output by the entry-error location detection functionality (see 5.2.3 *Entry-error location detection functionality* in the manual *Configuration Guide Vol. 1 For Version 11.7.*)

Table 1-8: List of error messages output by the entry-error location detection functionality

#	Message	Description	Occurrence condition
1	% illegal parameter at '^' marker	An invalid command or parameter is entered at '^'.	When an unsupported command or parameter is entered
2	% too long at '^' marker	A parameter entered at '^' exceeds the limit for the number of digits.	When a parameter that exceeds the limit for the number of digits is entered
3	% Incomplete command at '^' marker	Some parameters are missing.	When some parameters are missing
4	% illegal option at '^' marker	An invalid option is entered at '^'.	When an invalid option is entered
5	% illegal value at '^' marker	An invalid numeric value is entered at '^'.	When an invalid numeric value is entered
6	% illegal name at '^' marker	An invalid name is entered at '^'.	When an invalid name is entered
7	% out of range '^' marker	A numeric value entered at '^' is out of the valid range.	When a numeric value that is out of the valid range is entered
8	% illegal IP address format at '^' marker	An invalid IPv4 address or IPv6 address is entered at '^'.	When the input format of the IPv4 address or IPv6 address is invalid
9	% illegal combination or already appeared at '^' marker	A parameter entered at '^' has already been entered.	When a parameter that has already been entered is re-entered
10	% illegal format at '^' marker	The parameter entered at '^' has an invalid format.	When the input format of the parameter is invalid
11	% Permission denied	This command cannot be executed in user mode.	When a command that can be executed only in administrator mode is executed in user mode.
12	% internal program error	A program is faulty. Contact maintenance personnel.	When an invalid action other than described above occurs
13	% Command not authorized.	The executed command is not authorized.	When the executed command is not authorized by the RADIUS/TACACS+ server via RADIUS/TACACS+ command authorization
14	% illegal parameter at '<word>' word	An invalid character '<word>' is entered. <word>: Invalid word	When '<word>' is entered at positions where a character cannot be entered

Chapter

2. 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 (ip access-group, ipv6 traffic-filter, and mac access-group), the number of packets that met the filter conditions, and the number of packets discarded because they did not match any filter conditions in the access list.

Syntax

```
show access-filter
show access-filter <nif no.>/<port no.> [ { <access list number>
| <access list name> } ] [ { in | out } ]
[ layer2-forwarding ]
show access-filter interface vlan <vlan id> [ { <access list number>
| <access list name> } ] [ { in | out } ]
[ { layer2-forwarding | layer3-forwarding
| layer2-and-layer3-forwarding } ]
```

Input mode

User mode and administrator mode

Parameters

<nif no.>/<port no.>

Displays statistics for the specified Ethernet interface. For the specifiable range of <nif no.> and <port no.> values, see *Specifiable values for parameters*.

interface vlan <vlan id>

Displays statistics for the specified VLAN interface.

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

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

access list number: Access list number

access list name: Access list name

Displays statistics for the specified interface that has the specified access list number or access list name.

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.

{ layer2-forwarding | layer3-forwarding | layer2-and-layer3-forwarding }

layer2-forwarding: Specifies Layer 2 forwarding.

layer3-forwarding: Specifies Layer 3 forwarding.

layer2-and-layer3-forwarding: Specifies Layer 2 forwarding and Layer 3 forwarding.

Displays statistics for the specified interface that has the access list with the specified relay

layer settings. Note, however, that the statistics displayed by layer2-and-layer3-forwarding do not include the statistics from separate layer2-forwarding or layer3-forwarding specifications.

Operation when this parameter is omitted:

On the specified interface, displays statistics for the access list for which layer2-forwarding is specified and for the access list for which layer3-forwarding is specified.

Operation when all parameters are omitted:

On all interfaces, displays statistics for access lists with all types of forwarding specified.

Example

Figure 2-1: Result of displaying the extended MAC access list

```
> show access-filter 1/3 only-appletalk out
Date 2006/03/01 12:00:00 UTC
Using Port:1/3 out
Extended MAC access-list:only-appletalk layer2-forwarding
  remark "permit only appletalk"
  permit any any appletalk(0x809b)
    matched packets      :          74699826
  permit any any 0x80f3
    matched packets      :          718235
  implicitly denied packets:          2698
>
```

Figure 2-2: Result of displaying the standard IPv4 access list

```
> show access-filter interface vlan 10 12 out
Date 2006/03/01 12:00:00 UTC
Using Interface:vlan 10 out
Standard IP access-list: 12 layer3-forwarding
  remark "permit only host pc"
  permit host 10.10.10.1
    matched packets      :          32156826
  permit host 10.10.10.254
    matched packets      :          23486
  implicitly denied packets:          45
>
```

Figure 2-3: Result of displaying the extended IPv4 access list

```
> show access-filter interface vlan 100 128 in
Date 2006/03/01 12:00:00 UTC
Using Interface:vlan 100 in
Extended IP access-list: 128 layer3-forwarding
  remark "permit only http"
  permit tcp(6) any host 10.10.10.2 eq http(80)
    matched packets      :          6425800211584
  implicitly denied packets:          254178
>
```

Figure 2-4: Result of displaying the IPv6 access list

```
> show access-filter 1/15 only-telnet
Date 2006/03/01 12:00:00 UTC
Using Port:1/15 in
IPv6 access-list: only-telnet layer3-forwarding
  remark "permit only telnet ipv6"
  permit ipv6(41) any host 3ffe:501:811:ff00::1 eq telnet(23)
    matched packets      :          158468756
  implicitly denied packets:          37125
>
```

Figure 2-5: Result of displaying the Advance access list

```
> show access-filter interface vlan 10 only-telnet out
Date 2009/07/15 12:00:00 UTC
```

```

Using Interface: vlan 10 out
Advance access-list: only-telnet layer2-and-layer3-forwarding
    remark "permit only mac-ipv6"
    permit mac-ipv6 0012.e200.1234 ffff.ffff.0000 any ipv6(41) any host
2001:db8:1:fe20::1
    matched packets          :          468756
    implicitly denied packets:          15342
>

```

Figure 2-6: Result of displaying information when the access list ID is omitted

```

> show access-filter interface vlan 1500 in
Date 2006/03/01 12:00:00 UTC
Using Interface:vlan 1500 in
Standard IP access-list: pc-a1024 layer2-forwarding
    remark "permit only pc-a1024"
    permit host 192.168.1.254
        matched packets          :          5542166226
        implicitly denied packets:          767895
IPv6 access-list:only-smtp layer3-forwarding
    remark "permit only smtp ipv6"
    permit ipv6(41) any host 3ffe:501:811:ff00::1 eq smtp(25)
        matched packets          :          51218136
        implicitly denied packets:          66514
>

```

Figure 2-7: Result of displaying information when in or out is omitted

```

> show access-filter interface vlan 1500
Date 2006/03/01 12:00:00 UTC
Using Interface:vlan 1500 in
Standard IP access-list:pc-a1024 layer2-forwarding
    remark "permit only pc-a1024"
    permit host 192.168.1.254
        matched packets          :          5542166226
        implicitly denied packets:          767895
IPv6 access-list:only-smtp layer3-forwarding
    remark "permit only smtp ipv6"
    permit ipv6(41) any host 3ffe:501:811:ff00::1 eq smtp(25)
        matched packets          :          51218136
        implicitly denied packets:          66514

Using Interface:vlan 1500 out
Extended IP access-list:only-ssh layer3-forwarding
    remark "permit only ssh"
    permit tcp(6) any any eq ssh(22)
        matched packets          :          578213549
        implicitly denied packets:          843358
>

```

Figure 2-8: Result of displaying information when all parameters are omitted

```

> show access-filter
Date 2009/07/15 12:00:00 UTC
Using Port:1/7 in
Standard IP access-list: 12 layer2-forwarding
    remark "permit only host pc"
    permit host 10.10.10.1
        matched packets          :          54826
    permit host 10.10.10.254
        matched packets          :          494176
    implicitly denied packets:          298

Using Port:1/7 out
Extended IP access-list: 128 layer2-forwarding
    remark "permit only http "
    permit tcp(6) any host 10.10.10.2 eq http(80)
        matched packets          :          425684792129226
    implicitly denied packets:          11352654

```



```

Using Interface:vlan 15 out
IPv6 access-list:only-telnet layer3-forwarding
  remark "permit only telnet ipv6"
  permit ipv6(41) any host 3ffe:501:811:ff00::1 eq telnet(23)
    matched packets      :      385496541
    implicitly denied packets:      56645

Using Interface:vlan 19 in
Standard IP access-list:pc-a1024 layer2-forwarding
  remark "permit only pc-a1024"
  permit host 192.168.1.254
    matched packets      :      24826
    implicitly denied packets:      53
Standard IP access-list:pc-a1024 layer3-forwarding
  remark "permit only pc-a1024"
  permit host 192.168.1.254
    matched packets      :      6249299826
    implicitly denied packets:      95198
IPv6 access-list:smtp-server layer2-forwarding
  remark "permit only smtp server"
  permit ipv6(41) any host 3ffe:501:811:ff00::1
    matched packets      :      1699826
    implicitly denied packets:      2491
Advance access-list: only-http layer2-and-layer3-forwarding
  remark " permit only http "
  permit mac-ip 0012.e200.1234 ffff.ffff.0000 any tcp(6) any host 10.10.10.2
eq http(80)
    matched packets      :      158468756
    implicitly denied packets:      37125

Using Interface:vlan 100 in
Extended MAC access-list:only-appletalk layer2-forwarding
  remark "permit only appletalk"
  permit any any appletalk(0x809b)
    matched packets      :      826
  permit any any 0x80f3
    matched packets      :      55
    implicitly denied packets:      321314588
>

```

Display items

Display items of statistics for the access list applied to an interface by using an access group command are described below.

```

> show access-filter 1/7 12
Date 2006/03/01 12:00:00 UTC
Using Port:1/7 in
Standard IP access-list: 12 layer2-forwarding
  remark "permit only host pc"
  permit host 10.10.10.1
    matched packets      :      74699826
  permit host 10.10.10.254
    matched packets      :      264176
    implicitly denied packets:      2698

```

Table 2-1: Items displayed for the access list statistics

Item	Displayed information	
	Detailed information	Meaning
Interface information	Using Port:<nif no.>/<port no.> in	Information about an Ethernet interface to which an access list has been applied on the inbound side

Item	Displayed information	
	Detailed information	Meaning
	Using Port:<nif no.>/<port no.> out	Information about an Ethernet interface to which an access list has been applied on the outbound side
	Using Interface:vlan <vlan id> in	Information about a VLAN interface to which an access list has been applied on the inbound side
	Using Interface:vlan <vlan id> out	Information about a VLAN interface to which an access list has been applied on the outbound side
Access list ID, relay layer information	Extended MAC access-list:<access list name> layer2-forwarding	Extended MAC access list ID with Layer 2 forwarding specified when an access list is applied to the interface
	Standard IP access-list:{ <access list number> <access list name> } layer2-forwarding	Standard IPv4 access list ID with Layer 2 forwarding specified when an access list is applied to an interface
	Standard IP access-list:{ <access list number> <access list name> } layer3-forwarding	Standard IPv4 access list ID with Layer 3 forwarding specified when an access list is applied to an interface
	Extended IP access-list:{ <access list number> <access list name> } layer2-forwarding	Extended IPv4 access list ID with Layer 2 forwarding specified when an access list is applied to an interface
	Extended IP access-list:{ <access list number> <access list name> } layer3-forwarding	Extended IPv4 access list ID with Layer 3 forwarding specified when an access list is applied to an interface
	IPv6 access-list:<access list name> layer2-forwarding	IPv6 access list ID with Layer 2 forwarding specified when an access list is applied to an interface
	IPv6 access-list:<access list name> layer3-forwarding	IPv6 access list ID with Layer 3 forwarding specified when an access list is applied to an interface
	Advance access-list:<access list name> layer2-forwarding	Advance access list ID with Layer 2 forwarding specified when an access list is applied to an interface
	Advance access-list:<access list name> layer2-and-layer3-forwarding	Advance access list ID with Layer 2 forwarding and Layer 3 forwarding specified when an access list is applied to an interface
Access list information	Supplementary information and filter conditions set by an access list command (see 4. <i>Access Lists</i> in the manual <i>Configuration Command Reference Vol. 2 For Version 11.7</i>) are displayed.	
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 2-2: List of response messages for the show access-filter command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.

Message	Description
Can't execute.	The command could not be executed. Possible causes are as follows: <ul style="list-style-type: none"> There are no active BSUs, CSUs, and MSUs. Make sure at least one BSN, CSU, or MSU is active before re-executing the command. The command cannot be executed because the access list is being set. Wait a while, and then re-execute the command.
Illegal NIF -- <i><nif no.></i> .	The specified NIF number is invalid. Make sure the specified parameter is correct, and then try again. <i><nif no.></i> : NIF number
Illegal Port -- <i><port no.></i> .	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <i><port no.></i> : Port number
No configuration.	No access group was set for the Ethernet interface or VLAN interface. Make sure the specified parameter or access-group setting is correct, and then try again.
No such access-list.	The access list number or the access group of the access list name you specified has not been set. Make sure the specified parameter is correct, and then try again.
No such interface.	The specified interface has not been configured. Make sure the specified parameter is correct, and then try again.

Notes

To check the route information for policy-based routing, execute the `show ip cache policy` command. To check the destination interface information for policy-based switching, execute the `show cache policy-switch` command.

clear access-filter

For the access list information displayed by the `show access-filter` command, this command resets the number of packets that met the filter conditions (indicated in `matched packets`) and the number of packets discarded because they did not meet the filter conditions (indicated in `implicitly denied packets`).

Syntax

```
clear access-filter
clear access-filter <nif no.>/<port no.> [ { <access list number>
| <access list name> } ] [ { in | out } ]
[ layer2-forwarding ]
clear access-filter interface vlan <vlan id> [ { <access list number>
| <access list name> } ] [ { in | out } ]
[ { layer2-forwarding | layer3-forwarding
| layer2-and-layer3-forwarding } ]
```

Input mode

User mode and administrator mode

Parameters

<nif no.>/<port no.>

Clears statistics for the specified Ethernet interface. For the specifiable range of *<nif no.>* and *<port no.>* values, see *Specifiable values for parameters*.

interface vlan <vlan id>

Clears statistics for the specified VLAN interface.

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

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

access list number: Access list number

access list name: Access list name

Resets statistics for the specified access list number or access list name of the specified interface.

Operation when this parameter is omitted:

Resets statistics for all access lists applied to the specified interface.

{ in | out }

in: Inbound (Specifies the receiving side)

out: Outbound (Specifies the sending side)

Resets statistics for the receiving side or the sending side of the specified interface.

Operation when this parameter is omitted:

Resets statistics for the receiving side and the sending side of the specified interface.

{ layer2-forwarding | layer3-forwarding | layer2-and-layer3-forwarding }

layer2-forwarding: Specifies Layer 2 forwarding.

layer3-forwarding: Specifies Layer 3 forwarding.

layer2-and-layer3-forwarding: Specifies Layer 2 forwarding and Layer 3 forwarding.

Resets statistics for the access list with the specified relay layer set of the specified interface.

Note, however, that statistics for layer2-forwarding or layer3-forwarding is not cleared if statistics for layer2-and-layer3-forwarding are cleared.

Operation when this parameter is omitted:

Resets statistics for the access list when layer2-forwarding is set and the access list when layer3-forwarding is set in the specified interface.

Operation when all parameters are omitted:

Resets statistics for the access lists when all relays are set in all interfaces.

Example

Figure 2-9: Result of resetting the standard IPv4 access list statistics

```
> clear access-filter 1/7 12
Date 2006/03/01 12:00:00 UTC
>
```

Display items

None

Impact on communication

None

Response messages

Table 2-3: List of response messages for the clear access-filter command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Possible causes are as follows: <ul style="list-style-type: none"> There are no active BSUs, CSUs, and MSUs. Make sure at least one BSN, CSU, or MSU is active before re-executing the command. The command cannot be executed because the access list is being set. Wait a while, and then re-execute the command.
Illegal NIF -- <nif no.>.	The specified NIF number is invalid. Make sure the specified parameter is correct, and then try again. <nif no.>: NIF number
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Port number
No configuration.	No access group was set for the Ethernet interface or VLAN interface. Make sure the specified parameter or access-group setting is correct, and then try again.
No such access-list.	The access list number or the access group of the access list name you specified has not been set. Make sure the specified parameter is correct, and then try again.
No such interface.	The specified interface has not been configured. Make sure the specified parameter is correct, and then try again.

Notes

If this command is executed, MIB information of the axsAccessFilterStats group is also reset.

Chapter

3. Access List Logging

```
show access-log  
clear access-log  
show access-log flow  
clear access-log flow  
dump access-log  
restart access-log  
debug access-log  
no debug access-log
```

show access-log

Displays access list log information.

Syntax

```
show access-log
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 3-1: Displaying access list log information

```
> show access-log
Date 2009/12/14 12:00:00 UTC
Access list logging Information:
  rate-limit(pps)      :                100
  interval(minutes)   :                 5
  threshold(packets)  :                 -
  logging              :                enable
  display              :                disable
Access list logging Logged:
  Max                  :                2000
  Used                 :                1001
  NonIP                :                950
  IPv4                 :                 0
  IPv6                 :                 51
Access list logging Statistics:
  flow table full      :               17295
  rate-limit discard   :               51615
>
```

Display items

Table 3-1: Items displayed for access list logging

Item		Meaning	Displayed information
Access list logging Information:	rate-limit	Maximum number of packets transferred to the CPU per second	10 to 250: Maximum number of frames (pps) -: BSU or PSP is not operating.
	interval	Interval for outputting access list logs	5 to 1440: Interval (minutes) unlimit: No logs are output at the specified interval.
	threshold	Threshold	1 to 4294967295: Threshold value -: Not set
	logging	Output status of operation logs and syslog	enable: Enabled disable: Disabled
	display	Display status of an operation message sent to an operation terminal	enable: Enabled disable: Disabled
Access list logging Logged:	Max	Maximum number of items of managed access list log information	--

Item		Meaning	Displayed information
	Used	Number of items of managed access list log information	--
	NonIP	Number of items of access list log information for non-IP packets in the number of items of managed access list log information	--
	IPv4	Number of items of access list log information for IPv4 packets in the number of items of managed access list log information	--
	IPv6	Number of items of access list log information for IPv6 packets in the number of items of managed access list log information	--
Access list logging Statistics:	flow table full	Number of packets discarded because there is no available space in the access list log information table.	--
	rate-limit discard	Number of packets discarded because they exceed the rate limit.	--

Impact on communication

None

Response messages

Table 3-2: List of response messages for the show access-log command

Message	Description
Access list logging is not enable.	Access list logging is disabled. Check the configuration.
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to access list logging program.	The command cannot be executed because the access list logging program is not started. Wait until the access list logging program restarts, and then re-execute the command.

Notes

None

clear access-log

Clears the discarded packet statistics which were acquired through access list logging.

Syntax

```
clear access-log
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 3-2: Clearing statistics for the access list logging packets

```
> clear access-log  
Date 2009/12/14 12:00:00 UTC  
>
```

Display items

None

Impact on communication

None

Response messages

Table 3-3: List of response messages for the clear access-log command

Message	Description
Access list logging is not enable.	Access list logging is disabled. Check the configuration.
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to access list logging program.	The command cannot be executed because the access list logging program is not started. Wait until the access list logging program restarts, and then re-execute the command.

Notes

None

show access-log flow

Displays access list log information managed by access list logging.

For details about the information to be displayed as the command execution result, see the manual *Message and Log Reference For Version Ver. 11.7*.

Syntax

Display of access list log information for non-IP packets:

```
show access-log flow mac [<ethernet type>] [{<source mac> <source mac mask>
| host <source mac> | any} {<destination mac> <destination mac mask> |
host <destination mac> | any}] [{vlan <vlan id list> | port <port list>}]
[{in | out}] [packets-sort]
```

Display of access list log information for IPv4 packets:

```
show access-log flow ip [<protocol>] [{<source ipv4> <source ipv4 wildcard>
| host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard>
| host <destination ipv4> | any}] [{vlan <vlan id list> | port <port list>}]
[{in | out}] [packets-sort]
```

Display of access list log information for IPv6 packets:

```
show access-log flow ipv6 [<next header>]
[{<source ipv6>/<length> | host <source ipv6> | any}
{<destination ipv6>/<length> | host <destination ipv6>
| any}] [{vlan <vlan id list> | port <port list>}] [{in | out}] [packets-sort]
```

Display of access list log information for all protocols

```
show access-log flow [{vlan <vlan id list> | port <port list>}] [{in | out}]
[packets-sort]
```

Input mode

User mode and administrator mode

Parameters

{ mac | ip | ipv6 }

Specify the protocol to be displayed.

mac

Displays access list log information for non-IP packets.

ip

Displays access list log information for IPv4 packets.

ipv6

Displays access list log information for IPv6 packets.

Operation when this parameter is omitted:

Displays access list log information for all protocols.

<ethernet type>

Displays access list log information for the specified Ethernet type only.

Specify 0x0000 to 0xffff (in hexadecimal).

Operation when this parameter is omitted:

Displays access list log information for all Ethernet types.

{<source mac> <source mac mask> | host <source mac> | any} {<destination mac> <destination mac mask> | host <destination mac> | any}

Displays access list log information that matches the specified source MAC address or destination MAC address.

<source mac> <source mac mask>

Specify the source MAC address for <source mac>.

For <source mac mask>, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

host <source mac>

Displays access list log information of the source MAC address that perfectly matches <source mac>.

<destination mac> <destination mac mask>

Specify the destination MAC address for <destination mac>.

For <destination mac mask>, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

host <destination mac>

Displays access list log information of the destination MAC address that perfectly matches <destination mac>.

any

Displays access list log information for all MAC address.

Operation when this parameter is omitted:

The source MAC address and the destination MAC address are not included in display conditions.

<protocol>

Displays the access list log information that satisfies upper layer protocol conditions you specified.

Set 0 to 255 (in decimal) or a protocol name. The following table shows the specifiable protocol names.

Table 3-4: Protocol names that can be specified

Protocol name	Corresponding protocol number
icmp	1
igmp	2
tcp	6
udp	17

Operation when this parameter is omitted:

Displays access list log information that meets all upper layer protocol conditions.

{<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host {<destination ipv4> | any}}

Displays access list log information that matches the specified source IPv4 address or destination IPv4 address.

<source ipv4> <source ipv4 wildcard>

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

For *<source ipv4 wildcard>*, specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary.

host *<source ipv4>*

Displays access list log information of the source IPv4 address that perfectly matches *<source ipv4>*.

<destination ipv4> <destination ipv4 wildcard>

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

For *<destination ipv4 wildcard>*, specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary.

host *<destination ipv4>*

Displays access list log information of the destination IPv4 address that perfectly matches *<destination ipv4>*.

any

Displays access list log information for all IPv4 addresses.

Operation when this parameter is omitted:

The source IPv4 address and the destination IPv4 address are not included in display conditions.

<next header>

Displays the access list log information that matches with the next header number you specified.

Set 0 to 255 (in decimal) or a next header name. The following table shows the specifiable next header names.

Table 3-5: Specifiable next header names

Next header name	Corresponding next header number
icmp	58
tcp	6
udp	17

Operation when this parameter is omitted:

Displays access list log information for all next header conditions.

{*<source ipv6>/<length>* | host *<source ipv6>* | any} {*<destination ipv6>/<length>* | host
{*<destination ipv6>* | any }

Displays access list log information that matches the specified source IPv6 address or destination IPv6 address.

<source ipv6>/<length>

Specify the source IPv6 address for *<source ipv6>*.

For *<length>*, specify the part of the IPv6 address that meets conditions by using the first bits of the address.

host *<source ipv6>*

Displays access list log information of the source IPv6 address that perfectly matches *<source ipv6>*.

<destination ipv6>/<length>

Specify the destination IPv6 address for *<destination ipv6>*.

For *<length>*, specify the part of the IPv6 address that meets conditions by using the first bits of the address.

host *<destination ipv6>*

Displays access list log information of the destination IPv6 address that perfectly matches *<destination ipv6>*.

any

Displays access list log information for all IPv6 addresses.

Operation when this parameter is omitted:

The source IPv6 address and the destination IPv6 address are not included in display conditions.

{vlan *<vlan id list>* | port *<port list>*}

Displays access list log information of packets discarded in the specified interface.

vlan *<vlan id list>*

Specify the VLAN interface discarded by the filter. Displays information about the specified VLAN IDs in list format.

For details about how to specify *<vlan id list>*, see *Specifiable values for parameters*.

port *<port list>*

Specify the Ethernet interface. Displays information about the specified port number 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 information for all interfaces.

{in | out}

Specify the point of discard by the filter. Displays access list log information of packets discarded at the specified point.

in

Displays access list log information of packets discarded on the receiving side.

out

Displays access list log information of packets discarded on the sending side.

Operation when this parameter is omitted:

The point of discard by the filter is not included in display conditions.

packets-sort

Displays statistics of access list log information to be displayed (number of packets) in reverse chronological order.

Operation when this parameter is omitted:

Displays non-IP, IPv4, and IPv6 packets in that order in ascending order of source addresses.

Operation when all parameters are omitted:

Information about all access list logs is displayed.

Example

Figure 3-3: Displaying access list log information

```
> show access-log flow
Date 2009/12/14 12:00:00 UTC
ACL:denied:IN:0012.e25a.9839(vlan10 Ethernet1/1) -> 0012.e25a.7840, 2 packets
ACL:denied:IN:0012.e25a.983a(vlan10 Ethernet1/1) -> 0012.e25a.7840, 1 packet
ACL:denied:IN:tcp 192.168.1.3(1024, vlan10 Ethernet1/1) -> 192.168.2.1(22), 1
packet
ACL:denied:OUT:tcp 2001:db8::1(1024, vlan10 Ethernet1/1) -> 2001:db8::2(22,
vlan11 Ethernet3/1), 2 packets
>
```

Display items

None

Impact on communication

None

Response messages

Table 3-6: List of response messages for the show access-log flow command

Message	Description
Access list logging is not enable.	Access list logging is disabled. Check the configuration.
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to access list logging program.	The command cannot be executed because the access list logging program is not started. Wait until the access list logging program restarts, and then re-execute the command.
No access list logging entry.	There is no access list log information to be displayed. Check the specified contents of the parameter.

Notes

None

clear access-log flow

Clears access list log information and statistics managed by access list logging.

Syntax

```
clear access-log flow [packets]
```

Input mode

User mode and administrator mode

Parameters

packets

Clears statistics only.

This parameter can be specified only when `unlimit` is specified for the log message output interval (`interval`) for access list log information, which has been set in the configuration.

Operation when this parameter is omitted:

Clears access list log information and statistics that are being managed.

Example

Figure 3-4: Clearing access list log information and statistics

```
> clear access-log flow
Date 2009/12/14 12:00:00 UTC
>
```

Display items

None

Impact on communication

None

Response messages

Table 3-7: List of response messages for the clear access-log flow command

Message	Description
Access list logging is not enable.	Access list logging is disabled. Check the configuration.
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Can't specify packets parameter.	The <code>packets</code> parameter cannot be specified. Make sure <code>unlimit</code> is set for the access list log output interval (<code>interval</code>).
Connection failed to access list logging program.	The command cannot be executed because the access list logging program is not started. Wait until the access list logging program restarts, and then re-execute the command.

Notes

None

dump access-log

Outputs, to a file, event trace information and control table information collected by the access list logging program.

Syntax

```
dump access-log
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 3-5: Dumping the access list log

```
> dump access-log
>
```

Display items

None

Impact on communication

None

Response messages

Table 3-8: List of response messages for the dump access-log command

Message	Description
Access list logging is not enable.	Access list logging is disabled. Check the configuration.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to access list logging program.	The command cannot be executed because the access list logging program is not started. Wait until the access list logging program restarts, and then re-execute the command.

Notes

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

Storage directory: /usr/var/ac1log/

Output file: ac1logd_dump.gz

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

restart access-log

Restarts the access list logging program.

Syntax

```
restart access-log [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the access list logging program without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs a core file of the access list logging program when it is restarted.

Operation when this parameter is omitted:

A core file is not output.

Operation when all parameters are omitted:

After the confirmation message for restarting the program is output, the access list logging program is restarted.

Example

Figure 3-6: Restarting the access list logging program

```
> restart access-log
Access list logging restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Response messages

Table 3-9: List of response messages for the restart access-log command

Message	Description
Access list logging doesn't seem to be running.	The command cannot be executed because the access list logging program is not started. Make sure access list logging for the configuration is enabled.
Access list logging program failed to be restarted.	Restarting the access list logging program has failed. Re-execute the command.
Can't execute.	The command could not be executed. Re-execute the command.

Notes

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

Storage directory: `/usr/var/core/`

Core file: `ac1logd.core`

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

debug access-log

Displays operation messages of operation logs output by access list logging and starts sending syslog messages.

Syntax

```
debug access-log [display]
```

Input mode

User mode and administrator mode

Parameters

display

Displays operation messages of operation logs and starts sending syslog messages.

Operation when this parameter is omitted:

Starts collecting operation logs and sending syslog messages. No operation messages are displayed.

Example

Figure 3-7: Starting output of the access list log

```
> debug access-log
monitor: start access list logging event-log monitor (without screen display)
>
```

Display items

None

Impact on communication

None

Response messages

Table 3-10: List of response messages for the debug access-log command

Message	Description
Access list logging is not enable.	Access list logging is disabled. Check the configuration.
Already displayed for event-log.	The access list log entry has already been displayed on the operation terminal.
Already printed for event-log.	Output of access list log entries has already started.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to access list logging program.	The command cannot be executed because the access list logging program is not started. Wait until the access list logging program restarts, and then re-execute the command.
start access list logging event-log monitor	Output of access list log entries has started. The data is also displayed on the operation terminal.
start access list logging event-log monitor (without screen display)	Output of access list log entries has started. The data is not displayed on the operation terminal.

Notes

None

no debug access-log

Stops displaying operation messages of operation logs output by access list logging and sending syslog messages.

Syntax

```
no debug access-log
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 3-8: Stopping output of the access list log

```
> no debug access-log
monitor: stop access list logging event-log monitor
>
```

Display items

None

Impact on communication

None

Response messages

Table 3-11: List of response messages for the no debug access-log command

Message	Description
Access list logging is not enable.	Access list logging is disabled. Check the configuration.
Already does not printed for event-log.	Output of access list log entries has already stopped.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to access list logging program.	The command cannot be executed because the access list logging program is not started. Wait until the access list logging program restarts, and then re-execute the command.
stop access list logging event-log monitor	Output of access list log entries has started.

Notes

None

Chapter

4. QoS

```
show qos-flow
clear qos-flow
show qos queueing
clear qos queueing
show qos queueing distribution
clear qos queueing distribution
show qos queueing interface
clear qos queueing interface
show qos queueing to-cpu
clear qos queueing to-cpu
show shaper
clear shaper
show shaper <port list>
clear shaper <port list>
```

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
show qos-flow <nif no.>/<port no.> [ <qos flow list name> ] [ { in | out } ]
[ layer2-forwarding ]
show qos-flow interface vlan <vlan id> [ <qos flow list name> ] [ { in | out } ]
[ { layer2-forwarding | layer3-forwarding
| layer2-and-layer3-forwarding } ]
```

Input mode

User mode and administrator mode

Parameters

<nif no.>/<port no.>

Displays statistics for the specified Ethernet interface. For the specifiable range of <nif no.> and <port no.> values, see *Specifiable values for parameters*.

interface vlan <vlan id>

Displays statistics for the specified VLAN interface.

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

<qos flow list name>

<qos flow list name>: Specify the QoS flow list name.

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.

{ 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.

{ layer2-forwarding | layer3-forwarding | layer2-and-layer3-forwarding }

layer2-forwarding: Specifies Layer 2 forwarding.

layer3-forwarding: Specifies Layer 3 forwarding.

layer2-and-layer3-forwarding: Specifies Layer 2 forwarding and Layer 3 forwarding.

For the specified interfaces, displays statistics for the specified forwarding layer set in the QoS flow list. Note, however, that the statistics displayed by layer2-and-layer3-forwarding do not include the statistics from separate layer2-forwarding or layer3-forwarding specifications.

Operation when this parameter is omitted:

Displays statistics for the QoS flow list for Layer 2 forwarding and the QoS flow list for Layer 3 forwarding in the specified interface.

Operation when all parameters are omitted:

Displays statistics for the QoS flow list of all types of forwarding in all interfaces.

Example

- The following shows an example of displaying QoS flow list information when bandwidth monitoring is not used.

Figure 4-1: Result of displaying MAC QoS flow list information

```
> show qos-flow 1/3 apple-talk-qos out
Date 2006/03/01 12:00:00 UTC
Using Port:1/3 out
MAC qos-flow-list:appletalk-qos layer2-forwarding
    remark "QoS for appletalk"
    any any appletalk(0x809b) action priority-class 5 discard-class 2
    matched packets      :                5642
>
```

Figure 4-2: Result of displaying IPv4 QoS flow list information

```
> show qos-flow 1/7 http-qos out layer2-forwarding
Date 2006/03/01 12:00:00 UTC
Using Port:1/7 out
IP qos-flow-list:http-qos layer2-forwarding
    remark "QoS for http"
    tcp(6) any host 10.10.10.2 eq http(80) action priority-class 4
    matched packets      :                74699826
>
```

Figure 4-3: Result of displaying IPv6 QoS flow list information

```
> show qos-flow interface vlan 11 telnet-qos in
Date 2006/03/01 12:00:00 UTC
Using Interface:vlan 11 in
IPv6 qos-flow-list:telnet-qos layer2-forwarding
    remark "QoS for telnet"
    tcp(6) any host 3ffe:501:811:ff00::1 eq telnet(23) action priority-class 6
    discard-class 2
    matched packets      :                612359745
>
```

Figure 4-4: Result of displaying Advance QoS flow list information

```
> show qos-flow interface vlan 11 telnet-qos in
Date 2009/07/15 12:00:00 UTC
Using Interface:vlan 11 in
Advance qos-flow-list:telnet-qos layer2-and-layer3-forwarding
    remark "QoS for mac-ipv6"
    mac-ipv6 0012.e200.1234 ffff.ffff.0000 any tcp any host
    2001:db8:1:fe00::1 action priority-class 5 discard-class 1
    matched packets      :                345356711
>
```

Figure 4-5: Result of displaying information when the QoS flow list name is omitted

```
> show qos-flow interface vlan 19 in
Date 2006/03/01 12:00:00 UTC
Using Interface:vlan 19 in
IP qos-flow-list:ftp-qos layer2-forwarding
    remark "QoS for ftp"
    tcp(6) any any eq ftp(21) action priority-class 3 discard-class 1
    matched packets      :                5488465101
IP qos-flow-list:ftp-qos layer3-forwarding
    remark "QoS for ftp"
    tcp(6) any any eq ftp(21) action priority-class 3 discard-class 1
    matched packets      :                24884656
```

```
IPv6 qos-flow-list:telnet-qos layer2-forwarding
    remark "QoS for telnet"
    tcp(6) any host 3ffe:501:811:ff00::1 eq telnet(23) action priority-class 6
discard-class 4
    matched packets      :          387252415
>
```

Figure 4-6: Result of displaying information when in or out is omitted

```
> show qos-flow interface vlan 100
Date 2006/03/01 12:00:00 UTC
Using Interface:vlan 100 in
IP qos-flow-list:ftp-qos layer2-forwarding
    remark "QoS for ftp"
    tcp(6) any any eq ftp(21) action priority-class 3 discard-class 1
    matched packets      :          1684236799
IP qos-flow-list:ftp-qos layer3-forwarding
    remark "QoS for ftp"
    tcp(6) any any eq ftp(21) action priority-class 3 discard-class 1
    matched packets      :          17375692
IPv6 qos-flow-list:telnet-qos layer2-forwarding
    remark "QoS for telnet"
    tcp(6) any host 3ffe:501:811:ff00::1 eq telnet(23) action priority-class 6
discard-class 4
    matched packets      :          3454813846

Using Interface:vlan 100 out
IP qos-flow-list:smtp-qos layer2-forwarding
    remark "QoS for smtp"
    tcp(6) any any eq smtp(25) action priority-class 5 discard-class 3
    matched packets      :          5484365
>
```

Figure 4-7: Result of displaying information when all parameters are omitted

```
> show qos-flow
Date 2009/07/15 12:00:00 UTC
Using Port:1/12 in
IP qos-flow-list:http-qos layer2-forwarding
    remark "QoS for http"
    tcp(6) any host 10.10.10.2 eq http(80) action priority-class 4
    matched packets      :          745268726368

Using Port:1/12 out
IP qos-flow-list:http-qos layer2-forwarding
    remark "QoS for http"
    tcp(6) any host 10.10.10.2 eq http(80) action priority-class 4
    matched packets      :          564712387460

Using Interface:vlan 25 in
IP qos-flow-list:ftp-qos layer2-forwarding
    remark "QoS for ftp"
    tcp(6) any any eq ftp(21) action priority-class 3 discard-class 1
    matched packets      :          6278921654
IP qos-flow-list:ftp-qos layer3-forwarding
    remark "QoS for ftp"
    tcp(6) any any eq ftp(21) action priority-class 3 discard-class 1
    matched packets      :          564712387460
IPv6 qos-flow-list:telnet-qos layer2-forwarding
    remark "QoS for telnet"
    tcp(6) any host 3ffe:501:811:ff00::1 eq telnet(23) action priority-class 6
discard-class 4
    matched packets      :          905671862
Advance qos-flow-list:http-qos layer2-and-layer3-forwarding
    remark "QoS for http"
    mac-ip 0012.e200.1234 ffff.ffff.0000 any tcp any host 10.10.10.2 eq
http action priority-class 4
    matched packets      :          562383337460
```

```

Using Interface:vlan 25 out
IP qos-flow-list:smtp-qos layer2-forwarding
    remark "QoS for smtp"
    tcp(6) any any eq smtp(25) action priority-class 5 discard-class 3
    matched packets      :          91384186

Using Interface:vlan 100 out
MAC qos-flow-list:apple-talk-qos layer2-forwarding
    remark "QoS for apple-talk"
    any any appletalk(0x809b) action priority-class 5 discard-class 2
    matched packets      :          73156
IP qos-flow-list:smtp-qos layer3-forwarding
    remark "QoS for smtp"
    tcp(6) any any eq smtp(25) action priority-class 5 discard-class 3
    matched packets      :          26444786
>

```

- The following shows an example of displaying QoS flow list information when bandwidth monitoring is used.

Figure 4-8: Result of displaying IPv4 QoS flow list information when minimum bandwidth monitoring is used

```

> show qos-flow interface vlan 10 http-qos-min
Date 2006/10/01 12:00:00 UTC
Using Interface:vlan 10 out
IP qos-flow-list:http-qos-min layer3-forwarding
    remark "http min-rate 256k"
    tcp(6) any any eq http(80) action priority-class 4 min-rate 256
min-rate-burst 4000 penalty-discard-class 1
    matched packets
        (min-rate over) :          146723
        (min-rate under):          2118673486
>

```

Figure 4-9: Result of displaying IPv4 QoS flow list information when maximum bandwidth control is used

```

> show qos-flow interface vlan 100 http-qos-max
Date 2006/10/01 12:00:00 UTC
Using Interface:vlan 100 in
IP qos-flow-list:http-qos-max layer3-forwarding
    remark "http max-rate 256k"
    tcp(6) any any eq http(80) action priority-class 4 max-rate 256
max-rate-burst 4000
    matched packets
        (max-rate over) :          7246485
        (max-rate under):          1547819347
>

```

Figure 4-10: Result of displaying IPv4 QoS flow list information when minimum bandwidth monitoring and maximum bandwidth control are used

```

> show qos-flow interface vlan 1000 http-qos-max-min
Date 2006/10/01 12:00:00 UTC
Using Interface:vlan 1000 in
IP qos-flow-list:http-qos-max-min layer3-forwarding
    remark "http max 512 min 64"
    tcp(6) any any eq http(80) action priority-class 4 max-rate 512 min-rate
64 penalty-discard-class 1
    matched packets
        (max-rate over) :          92720
        (min-rate over) :          547895
        (min-rate under):          1672368291
>

```

Display items

Display items are described below.

4. QoS

```
> show qos-flow 1/7 http-qos
Date 2006/03/01 12:00:00 UTC
Using Port:1/7 in
IP qos-flow-list:http-qos layer2-forwarding
remark "QoS for http"
tcp any host 10.10.10.2 eq http action priority-class 4
information
matched packets : 74699826
--Interface information
--QoS flow list name
--QoS flow list information
--QoS flow list
--Statistics information
```

Table 4-1: Items displayed for the QoS flow list statistics

Item	Displayed information	
	Detailed information	Meaning
Interface information	Using Port:<nif no.>/<port no.> in	Information about an Ethernet interface to which a QoS flow list is applied on the inbound side
	Using Port:<nif no.>/<port no.> out	Information about an Ethernet interface to which a QoS flow list is applied on the outbound side
	Using Interface:vlan <vlan id> in	Information about a VLAN interface to which a QoS flow list is applied on the inbound side
	Using Interface:vlan <vlan id> out	Information about a VLAN interface to which a QoS flow list is applied on the outbound side
QoS flow list name	MAC qos-flow-list:<qos flow list name> layer2-forwarding	Name of a MAC QoS flow list for which Layer 2 forwarding is set when a QoS flow list is applied to an interface
	IP qos-flow-list:<qos flow list name> layer2-forwarding	Name of an IPv4 QoS flow list for which Layer 2 forwarding is set when a QoS flow list is applied to an interface
	IP qos-flow-list:<qos flow list name> layer3-forwarding	Name of an IPv4 QoS flow list for which Layer 3 forwarding is set when a QoS flow list is applied to an interface
	IPv6 qos-flow-list:<qos flow list name> layer2-forwarding	Name of an IPv6 QoS flow list for which Layer 2 forwarding is set when a QoS flow list is applied to an interface
	IPv6 qos-flow-list:<qos flow list name> layer3-forwarding	Name of an IPv6 QoS flow list for which Layer 3 forwarding is set when a QoS flow list is applied to an interface
	Advance qos-flow-list:<qos flow list name> layer2-forwarding	Name of an Advance QoS flow list for which Layer 2 forwarding is set when a QoS flow list is applied to an interface
	Advance qos-flow-list:<qos flow list name> layer2-and-layer3-forwarding	Name of an Advance QoS flow list for which Layer 2 forwarding is set when a QoS flow list is applied to an interface
QoS flow list information	Displays supplementary, flow detection conditions, and operations set by using a QoS flow list command (see 7. <i>QoS</i> in the manual <i>Configuration Command Reference Vol. 2 For Version 11.7</i>).	
Statistics	matched packets:<packets>	Number of packets that meet the flow detection conditions in the QoS flow list
	matched packets (max-rate over) :<packets>	Number of packets that match the flow detection conditions but violate the maximum bandwidth control conditions of the QoS flow list

Item	Displayed information	
	Detailed information	Meaning
	(max-rate under):<packets>	Number of packets that match the flow detection conditions and conform to the maximum bandwidth control conditions of the QoS flow list.
	(min-rate over) :<packets>	Number of packets that match the flow detection conditions but violate the minimum bandwidth monitoring conditions of the QoS flow list
	(min-rate under):<packets>	Number of packets that match the flow detection conditions and conform to the minimum bandwidth monitoring conditions of the QoS flow list

Impact on communication

None

Response messages

Table 4-2: List of response messages for the show qos-flow command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Possible causes are as follows: <ul style="list-style-type: none"> There are no active BSUs, CSUs, and MSUs. Make sure at least one BSU, CSU, or MSU is active before re-executing the command. The command cannot be executed because the QoS flow list is being set. Wait a while, and then re-execute the command.
Illegal NIF -- <nif no.>.	The NIF number is outside the valid range. Make sure the specified parameter is correct, and then try again. <nif no.>: NIF number
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Port number
No configuration.	No QoS flow group was set for the Ethernet interface or VLAN interface. Make sure the specified parameter or QoS flow group setting is correct, and then try again.
No such interface.	The specified interface has not been configured. Make sure the specified parameter is correct, and then try again.
No such qos-flow-list-name.	No QoS flow group that is specified with the QoS flow list name <qos flow list name> was applied to the interface. Make sure the specified parameter is correct, and then try again.

Notes

None

clear qos-flow

Clears the number of packets (indicated by `matched packets`) that met the flow detection conditions in the QoS flow list, which is displayed by the `show qos-flow` command.

Syntax

```
clear qos-flow
clear qos-flow <nif no.>/<port no.> [ <qos flow list name> ] [ { in | out } ]
               [ layer2-forwarding ]
clear qos-flow interface vlan <vlan id> [ <qos flow list name> ] [ { in | out } ]
               [ { layer2-forwarding | layer3-forwarding
                 | layer2-and-layer3-forwarding } ]
```

Input mode

User mode and administrator mode

Parameters

<nif no.>/<port no.>

Clears statistics for the specified Ethernet interface. For the specifiable range of *<nif no.>* and *<port no.>* values, see *Specifiable values for parameters*.

interface vlan <vlan id>

Clears 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.

Clears statistics for the specified QoS flow list of the specified interface.

Operation when this parameter is omitted:

Clears statistics for all QoS flow lists applied to the specified interface.

{ in | out }

in: Inbound (Specifies the receiving side)

out: Outbound (Specifies the sending side)

Clears statistics for the receiving side or the sending side of the specified interface.

Operation when this parameter is omitted:

Clears statistics for the receiving side and the sending side of the specified interface.

{ layer2-forwarding | layer3-forwarding | layer2-and-layer3-forwarding }

layer2-forwarding: Specifies Layer 2 forwarding.

layer3-forwarding: Specifies Layer 3 forwarding.

layer2-and-layer3-forwarding: Specifies Layer 2 forwarding and Layer 3 forwarding.

For the specified interfaces, clears statistics for the specified forwarding layer set in the QoS flow list. Note, however, that statistics for *layer2-forwarding* or *layer3-forwarding* is not cleared if statistics for *layer2-and-layer3-forwarding* are cleared.

Operation when this parameter is omitted:

Clears statistics for the QoS flow list of Layer 2 forwarding and the QoS flow list of Layer 3 forwarding in the specified interface.

Operation when all parameters are omitted:

Clears statistics for the QoS flow list of all types of forwarding for all interfaces.

Example

Figure 4-11: Result of clearing information

```
> clear qos-flow 1/7 http-qos
Date 2006/03/01 12:00:00 UTC
>
```

Display items

None

Impact on communication

None

Response messages

Table 4-3: List of response messages for the clear qos-flow command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Possible causes are as follows: <ul style="list-style-type: none"> There are no active BSUs, CSUs, and MSUs. Make sure at least one BSN, CSU, or MSU is active before re-executing the command. The command cannot be executed because the QoS flow list is being set. Wait a while, and then re-execute the command.
Illegal NIF -- <nif no.>.	The specified NIF number is invalid. Make sure the specified parameter is correct, and then try again. <nif no.>: NIF number
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Port number
No configuration.	No QoS flow group was applied to the Ethernet interface or VLAN interface. Make sure the specified parameter or QoS flow group setting is correct, and then try again.
No such interface.	The specified interface has not been configured. Make sure the specified parameter is correct, and then try again.
No such qos-flow-list-name.	No QoS flow group that is specified with the QoS flow list name <qos flow list name> was set. Make sure the specified parameter is correct, and then try again.

Notes

If this command is executed, MIB information of the axsQosFlowStats group is also cleared.

show qos queueing

Displays all input and output queues which are set for a Switch.

Displays the following to monitor the traffic status:

- Length of a priority queue
- Maximum queue length
- Number of packets accumulated in a queue
- Number of bytes accumulated in a queue
- Statistics for the total of the items

Figure 4-12: Queues to be displayed (other than NK1GS-8M) [AX6700S]

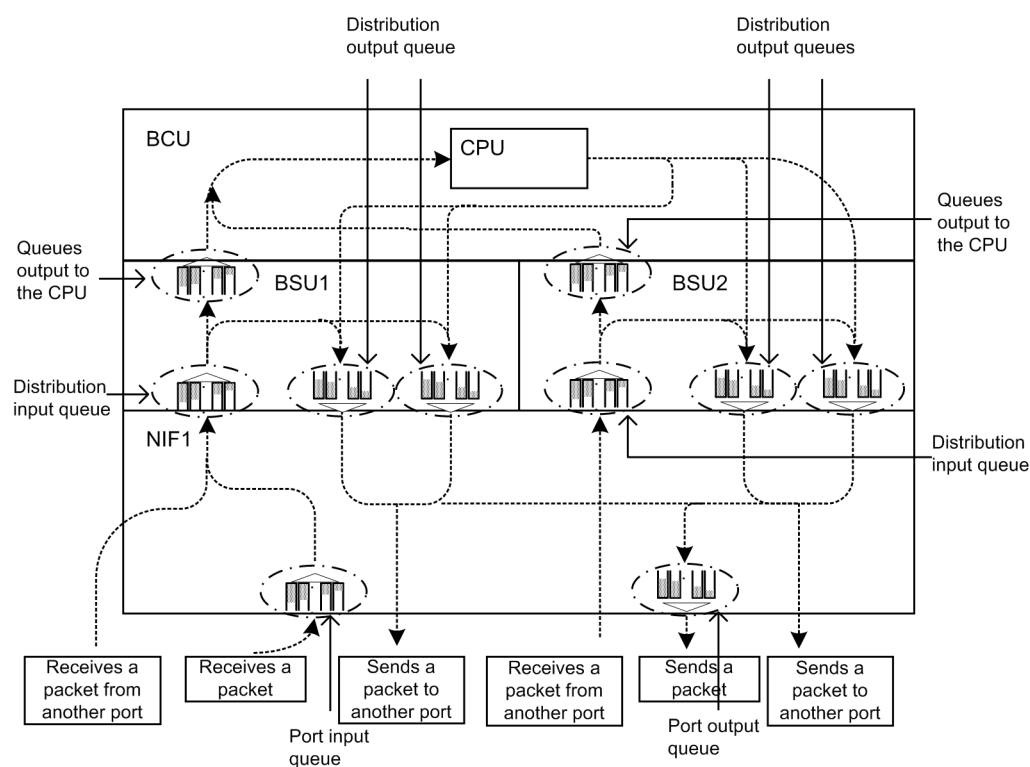


Figure 4-13: Queues to be displayed (for NK1GS-8M) [AX6700S]

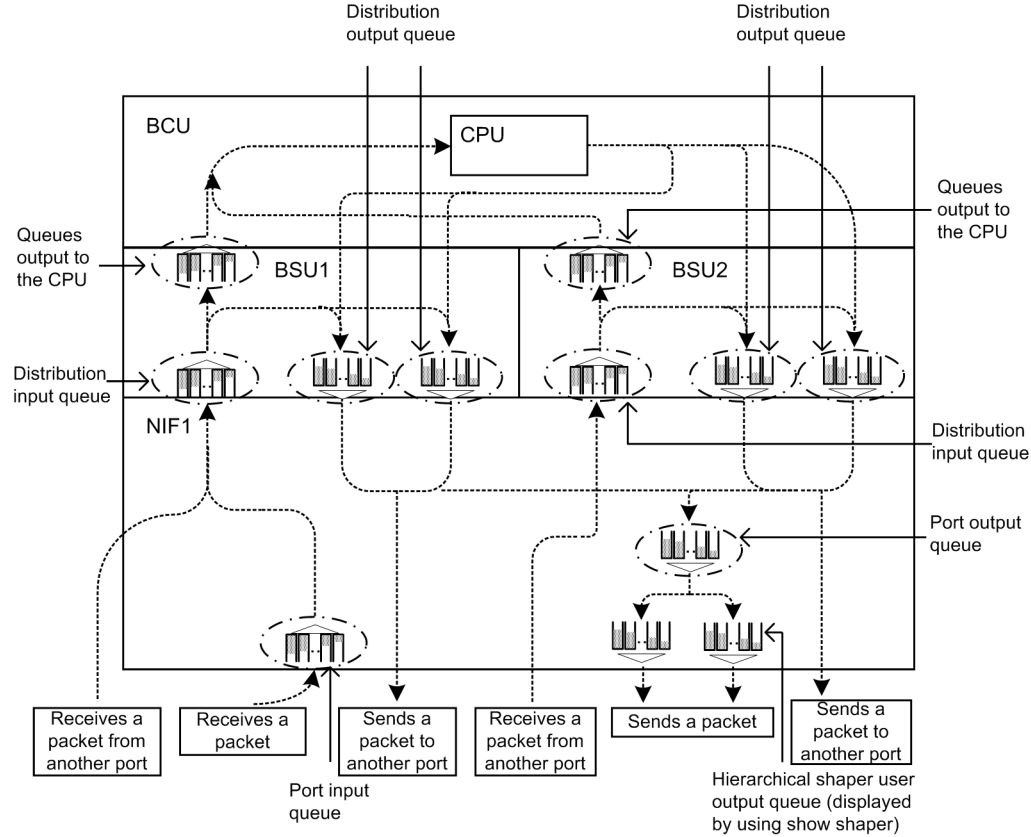


Figure 4-14: Queues to be displayed (other than NK1GS-8M) [AX6600S]

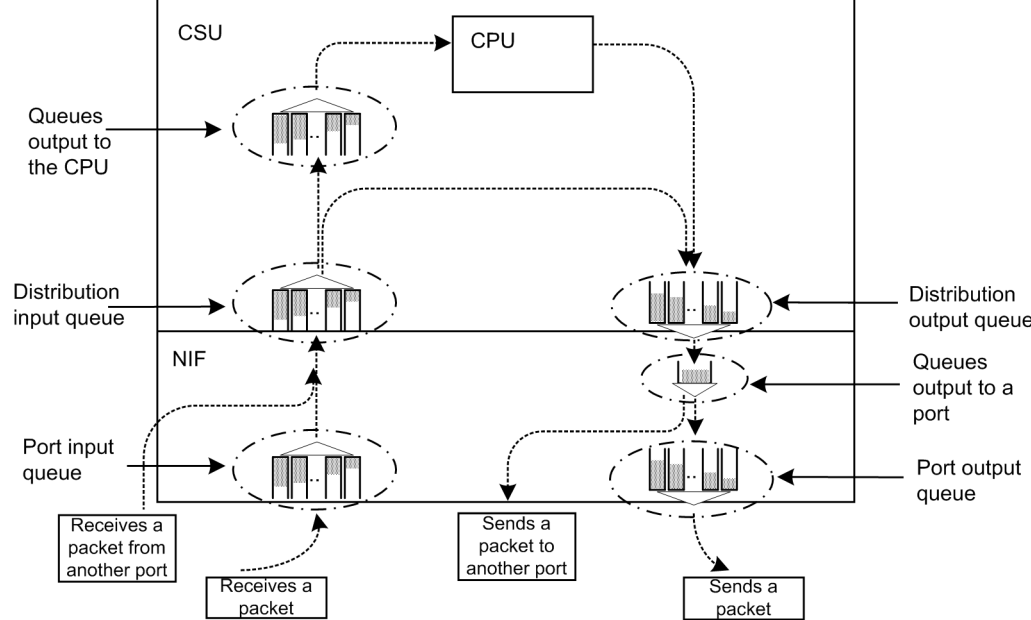


Figure 4-15: Queues to be displayed (for NK1GS-8M) [AX6600S]

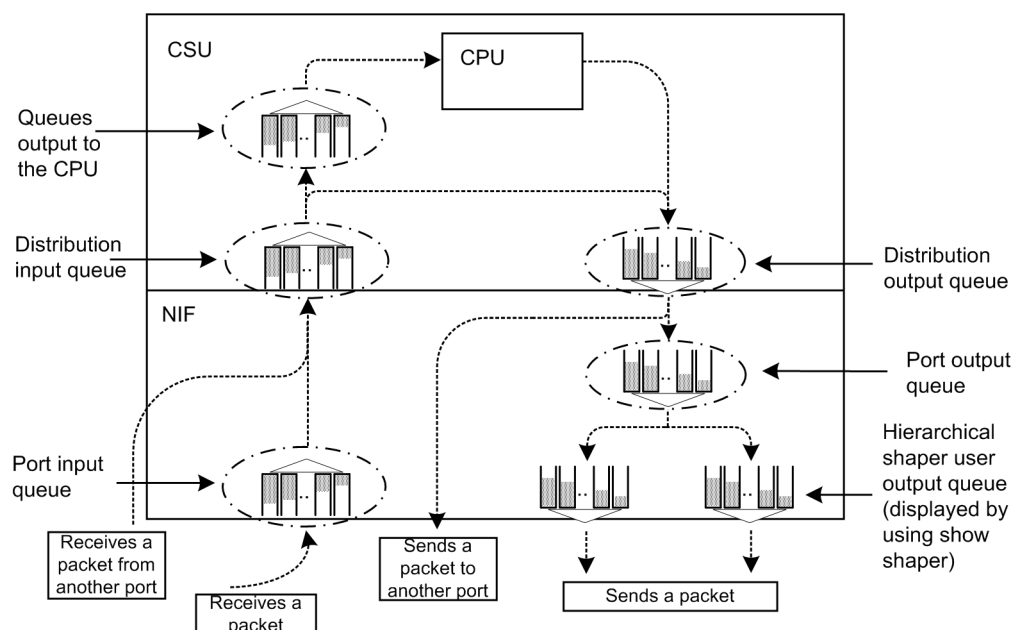


Figure 4-16: Queues to be displayed (other than NH1GS-6M and NH10G-1RX) [AX6300S]

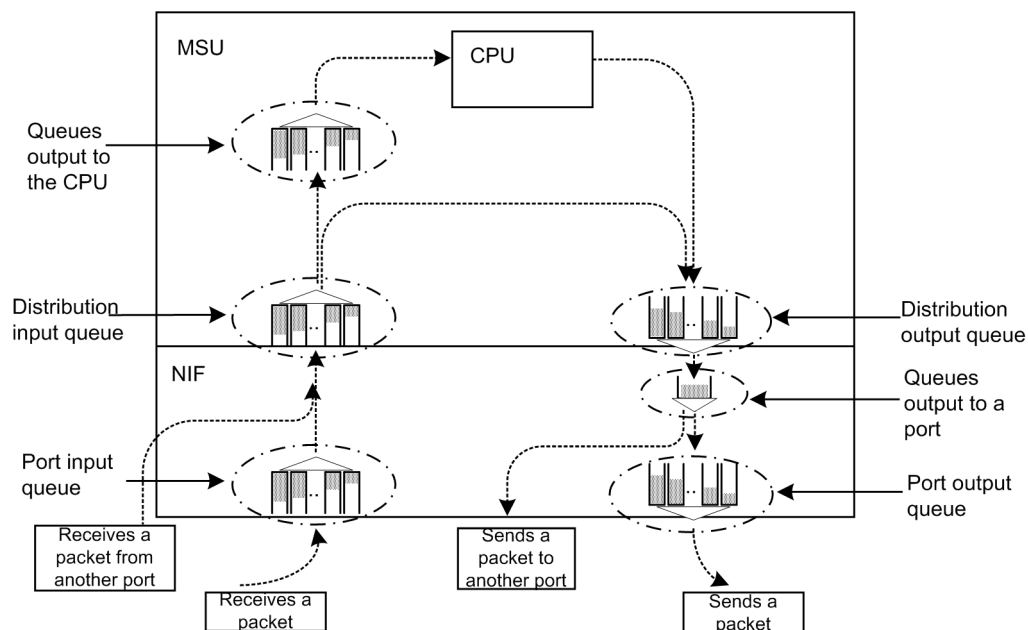


Figure 4-17: Queues to be displayed (for NH1GS-6M) [AX6300S]

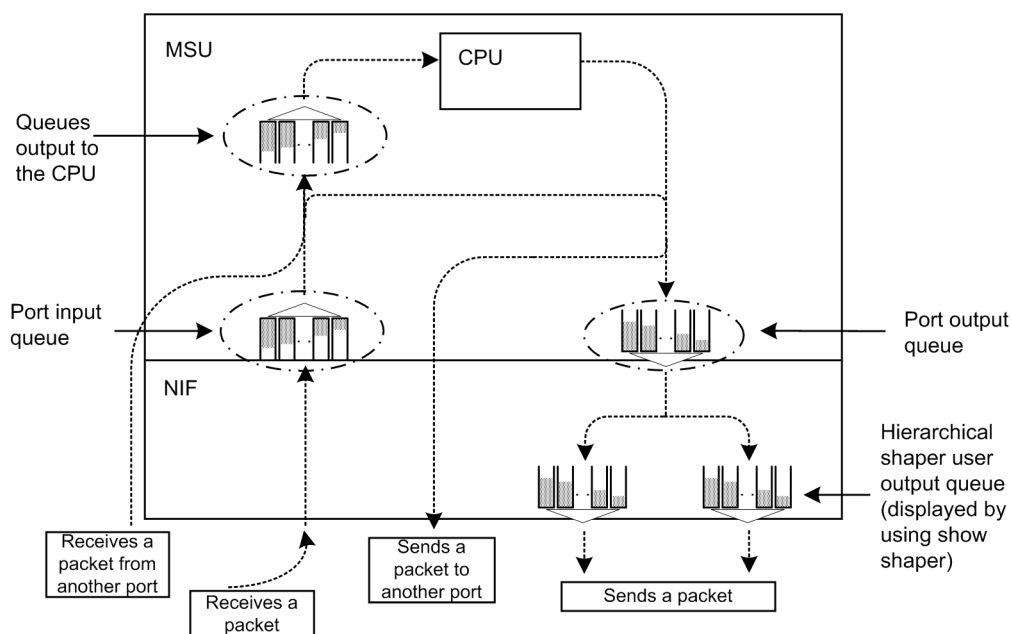
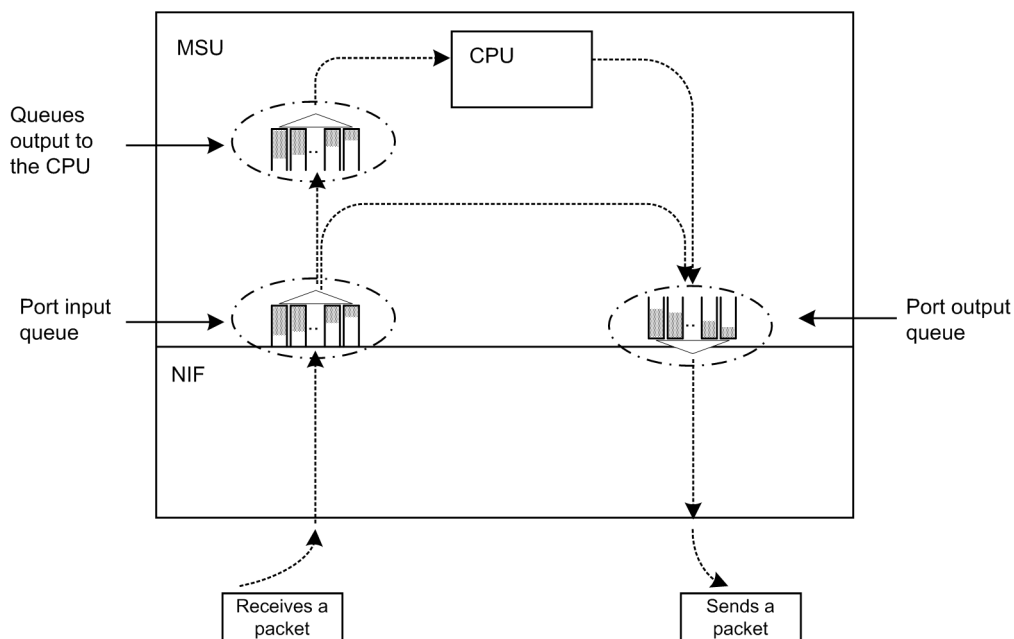


Figure 4-18: Queues to be displayed (for NH10G-1RX)



Syntax

```
show qos queueing [<port list> [{inbound | outbound}]]
```

Input mode

User mode and administrator mode

Parameters

<port list>

Specify the port number in list format. Displays information about all distribution input and output queues and port input and output queues that include one or more ports specified in the

list.[#] For details about how to specify *<port list>* and the specifiable range of values, see *Specifiable values for parameters*.

[#]: Queues output to the CPU are not displayed.

Operation when this parameter is omitted:

The following information is displayed:

- Queues output to the CPU
- All distribution input and output queues implemented on the device
- All port input and output queues implemented on the device

{inbound | outbound}

Specify an input queue or an output queue. This parameter can be specified only when *<port list>* is specified.

inbound

Displays information about an input queue.

outbound

Displays information about an output queue.

Operation when this parameter is omitted:

Displays information about input and output queues.

Example

- The following is an example of displaying information about all input and output queues.

Figure 4-19: Result of displaying information about all input and output queues [AX6700S] [AX6600S]

```
> show qos queueing
Date 2008/04/16 12:00:00 UTC
BSU1:To-CPU
Max_Queue=16
Queue1: Qlen=0, Peak_Qlen=0, Limit_Qlen=1023
  discard      send_pkt      discard_pkt      send_byte
  1             0             0             -
  2             0             0             -
  3             0             0             -
  4             0             0             -
  total         0             0             0
      :
      :
BSU1:NIF1/Port1-24 (Distribution_Queue1, outbound)
Max_Queue=8
Queue1: Qlen=0, Peak_Qlen=0, Limit_Qlen=2047
  discard      send_pkt      discard_pkt      send_byte
  1             0             0             -
  2             0             0             -
  3             0             0             -
  4             0             0             -
  total         0             0             0
      :
      :
BSU1:NIF1/Port1-24 (Distribution_Queue2, outbound)
Max_Queue=8
Queue1: Qlen=0, Peak_Qlen=2, Limit_Qlen=2047
  discard      send_pkt      discard_pkt      send_byte
  1             0             0             -
  2             0             0             -
  3             0             0             -
```

```

4              1594804              0              -
total          1594804              0              2308.7M
:
:
NIF1/Port1 (outbound)
Max_Queue=8, Rate=100Mbit/s, Schedule_mode=pq
Queue1: Qlen=32, Peak_Qlen=255, Limit_Qlen=255, Drop_mode=tail_drop
          send_pkt      discard_pkt      send_byte
total          813432              85              1174.4M
:
:
BSU1:NIF1/Port1,3,5,7,9,11,13,15,17,19,21,23 (Distribution_Queue, inbound)
Max_Queue=1
Queue1: Qlen=0, Peak_Qlen=1, Limit_Qlen=127
          send_pkt      discard_pkt      send_byte
total          8              0              480

NIF1/Port1 (inbound)
Max_Queue=1
Queue1: Qlen=0, Peak_Qlen=1, Limit_Qlen=63
discard      send_pkt      discard_pkt      send_byte
1              8              0              -
2              0              0              -
total          8              0              480
:
:
NIF1/Port24 (inbound)
Max_Queue=1
Queue1: Qlen=0, Peak_Qlen=1, Limit_Qlen=63
discard      send_pkt      discard_pkt      send_byte
1              4              0              -
2              0              0              -
total          4              0              240
>

```

Note:

"-" is displayed for the items that do not exist in the statistics counter.
If the command is executed on an AX600S Switch, information displayed for BSU is displayed for CSU.

Figure 4-20: Result of displaying information about all input and output queues [AX6300S]

```

> show qos queueing
Date 2008/04/16 12:00:00 UTC
To-CPU
Max_Queue=8
Queue1: Qlen=0, Peak_Qlen=384, Limit_Qlen=1023
discard      send_pkt      discard_pkt      send_byte
1              93411          3165766          -
2              0              0              -
3              0              0              -
4              0              0              -
total          93411          3165766          14.5M
:
:
NIF1/Port1-24 (Distribution_Queue, outbound)
Max_Queue=8
Queue1: Qlen=0, Peak_Qlen=2, Limit_Qlen=2047
discard      send_pkt      discard_pkt      send_byte
1              0              0              -
2              0              0              -
3              0              0              -
4              6405232          0              -
total          6405232          0              9272.7M
:
:
To_Port_Queue
          discard_pkt
To NIF1/Port 1- 4              0

```

```

To NIF1/Port 5- 8          0
To NIF1/Port 9-12         0
To NIF1/Port13-16        0
To NIF1/Port17-20        0
To NIF1/Port21-24        0

NIF1/Port1 (outbound)
Max_Queue=8, Rate=100Mbit/s, Schedule_mode=pq
Queue1: Qlen=0, Peak_Qlen=51, Limit_Qlen=255, Drop_mode=tail_drop
      send_pkt      discard_pkt      send_byte
total          3203665              0          4625.6M
      :
      :
NIF1/Port1-24 (Distribution_Queue, inbound)
Max_Queue=1
Queue1: Qlen=0, Peak_Qlen=2, Limit_Qlen=127
      send_pkt      discard_pkt      send_byte
total          34877867              0          38.1G

NIF1/Port1 (inbound)
Max_Queue=1
Queue1: Qlen=0, Peak_Qlen=1, Limit_Qlen=255
discard      send_pkt      discard_pkt      send_byte
1              192              0              -
2              0              0              -
total          192              0          15.8k
      :
      :
NIF1/Port24 (inbound)
Max_Queue=1
Queue1: Qlen=0, Peak_Qlen=1, Limit_Qlen=255
discard      send_pkt      discard_pkt      send_byte
1              192              0              -
2              0              0              -
total          192              0          15.8k
>
Note: "-" is displayed for the items that do not exist in the statistics counter.

```

Display items

Table 4-4: Items displayed for statistics [AX6700S] [AX6600S]

Item	Displayed information	
	Detailed information	Meaning
Interface information	NIF<nif no.>/Port<port no.> (outbound)	Port output queue
	NIF<nif no.>/Port<port no.>-<port no.> (outbound)	Port output queue
	NIF<nif no.>/Port<port no.> (inbound)	Port input queue
	NIF<nif no.>/Port<port no.>-<port no.> (inbound)	Port input queue
	For AX6700 S series switches: BSU<bsu no.>:NIF<nif no.>/Port<port no.> (Distribution_Queue1, outbound)	Distribution output queue 1
	BSU<bsu no.>:NIF<nif no.>/Port<port no.>-<port no.> (Distribution_Queue1, outbound)	Distribution output queue 1
	BSU<bsu no.>:NIF<nif no.>/Port<port no.> (Distribution_Queue2, outbound)	Distribution output queue 2

Item	Displayed information		
	Detailed information		Meaning
		BSU<bsu no.>:NIF<nif no.>/ Port<port no.>- <port no.> (Distribution_Queue2, outbound)	Distribution output queue 2
		BSU<bsu no.>:NIF<nif no.>/ Port<port no.>- <port no.> (Distribution_Queue, inbound)	Distribution input queue [#] when allocation per port was configured for load balancing of BSUs
		BSU<bsu no.>:NIF<nif no.>/ Port<port no.>- <port no.> (Distribution_Queue1, inbound)	Distribution input queue 1 [#] when allocation per source MAC address was configured for load balancing of BSUs
		BSU<bsu no.>:NIF<nif no.>/ Port<port no.>- <port no.> (Distribution_Queue2, inbound)	Distribution input queue 2 [#] when allocation per source MAC address was configured for load balancing of BSUs
		BSU<bsu no.>:To-CPU	Queues output to the CPU
	For AX6600 S series switches:	CSU<csu no.>:NIF<nif no.>/ Port<port no.> (Distribution_Queue, outbound)	Distribution output queue
		CSU<csu no.>:NIF<nif no.>/ Port<port no.>- <port no.> (Distribution_Queue, outbound)	Distribution output queue
		CSU<csu no.>:NIF<nif no.>/ Port<port no.> (Distribution_Queue, inbound)	Distribution input queue
		CSU<csu no.>:NIF<nif no.>/ Port<port no.>- <port no.> (Distribution_Queue, inbound)	Distribution input queue
		CSU<csu no.>:To-CPU	Queues output to the CPU
QoS information	Max_Queue=<number of queue>		Number of queues
	Rate=<rate>		Bandwidth for which the legacy shaper functionality is performed. <ul style="list-style-type: none"> When auto-negotiation is unresolved (including when processing is in progress) or for hierarchical Shaper NIF: - For other than the above, the bandwidth to be displayed varies depending on whether port bandwidth control by legacy shaper is specified or not. When port bandwidth control is set: Set bandwidth When port bandwidth control is not set: Line speed
	Schedule_mode=<schedule mode>		Displays scheduling mode. For details about scheduling, see 6.1.2 Scheduling in the manual Configuration Guide Vol. 2 For Version 11.7.
Queue information	Queue<queue no.>:		Queue number
	Qlen=<queue length>		Number of in-use packet buffers in a queue

Item	Displayed information	
	Detailed information	Meaning
	Peak_Qlen=<queue length>	Greatest number of in-use packet buffers in a queue
	Limit_Qlen=<queue length>	Limit of the number of in-use packet buffers in a queue
	Drop_mode=tail_drop	Drop control mode: tail_drop
Statistics	discard	Queuing priority <ul style="list-style-type: none"> For details about queuing priority, see the description about the number of discard classes in <i>Table 6-32 Correspondence between NIF models and send control functionality (2 of 3)</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i> and <i>Table 6-33 Correspondence between NIF models and send control functionality (3 of 3)</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i> in 6.10 <i>Correspondence between NIF models and send control functionality</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i>.
	send_pkt	Number of packets accumulated in a queue
	discard_pkt	Number of packets discarded without being accumulated in a queue
	send_byte	Number of bytes in packets accumulated in a queue (unit k indicates 1024, M indicates 1024 ² , and G indicates 1024 ³). The range from the MAC header to DATA and PAD (excluding FCS) is included.
	total	Total of the items (unit k indicates 1024, M indicates 1024 ² , and G indicates 1024 ³).

#: Port numbers corresponding to BSUs are displayed when hash mode is set.

Table 4-5: Items displayed for statistics [AX6300S]

Item	Displayed information	
	Detailed information	Meaning
Interface information	NIF<nif no.>/Port<port no.> (outbound)	Port output queue
	NIF<nif no.>/Port<port no.>-<port no.> (outbound)	Port output queue
	NIF<nif no.>/Port<port no.> (inbound)	Port input queue
	NIF<nif no.>/Port<port no.>-<port no.> (inbound)	Port input queue
	NIF<nif no.>/Port<port no.>- <port no.> (Distribution_Queue, outbound)	Distribution output queue
	NIF<nif no.>/Port<port no.>- <port no.> (Distribution_Queue, inbound)	Distribution input queue
	To_Port_Queue To NIF<nif no.>/Port<port no.>- <port no.>	Queues output to a port

Item	Displayed information	
	Detailed information	Meaning
	To-CPU	Queues output to the CPU
QoS information	Max_Queue=<number of queue>	Number of queues
	Rate=<rate>	Bandwidth for which the legacy shaper functionality is performed. <ul style="list-style-type: none"> When auto-negotiation is unresolved (including when processing is in progress) or for hierarchical Shaper NIF: - For other than the above, the bandwidth to be displayed varies depending on whether port bandwidth control by legacy shaper is specified or not. When port bandwidth control is set: Set bandwidth When port bandwidth control is not set: Line speed
	Schedule_mode=<schedule mode>	Displays scheduling mode. For details about scheduling, see 6.1.2 <i>Scheduling</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i> .
Queue information	Queue<queue no.>:	Queue number
	Qlen=<queue length>	Number of in-use packet buffers in a queue
	Peak_Qlen=<queue length>	Greatest number of in-use packet buffers in a queue
	Limit_Qlen=<queue length>	Limit of the number of in-use packet buffers in a queue
	Drop_mode=tail_drop	Drop control mode: tail_drop
Statistics	discard	Queuing priority <ul style="list-style-type: none"> For details about queuing priority, see the description about the number of discard classes in Table 6-35 <i>Correspondence between NIF models and send control functionality (2 of 3)</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i> and Table 6-36 <i>Correspondence between NIF models and send control functionality (3 of 3)</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i> in 6.10 <i>Correspondence between NIF models and send control functionality</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i>.
	send_pkt	Number of packets accumulated in a queue
	discard_pkt	Number of packets discarded without being accumulated in a queue
	send_byte	Number of bytes in packets accumulated in a queue (unit k indicates 1024, M indicates 1024 ² , and G indicates 1024 ³). The range from the MAC header to DATA and PAD (excluding FCS) is included.

Item	Displayed information	
	Detailed information	Meaning
	total	Total of the items (unit k indicates 1024, M indicates 1024 ² , and G indicates 1024 ³).

Impact on communication

None

Response messages

Table 4-6: List of response messages for the show qos queueing command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. There are no active BSUs, CSUs, and MSUs. Make sure at least one BSU, CSU, or MSU is active before re-executing the command.
Illegal NIF -- <nif no.>.	The specified NIF number is invalid. Make sure the specified parameter is correct, and then try again. <nif no.>: NIF number
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Port number
No operational port.	There is no port that is active. Make sure the specified NIF is active, and then re-execute the command.

Notes

None

clear qos queueing

Clears all queue statistics displayed by executing the `show qos queueing` command.

Syntax

```
clear qos queueing [<port list>] [{inbound | outbound}]
```

Input mode

User mode and administrator mode

Parameters

<port list>

Specify the port number in list format. Clears information about one or more distribution queues and port input and output queues for ports specified in the list.[#] For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

[#]: Queues output to the CPU are not displayed.

{inbound | outbound}

Specify an input queue or an output queue. This parameter can be specified only when <port list> is specified.

inbound

Clears statistics for an input queue.

outbound

Clears statistics for an output queue.

Operation when this parameter is omitted:

Clears statistics for input and output queues.

Example

- The following shows an example of clearing statistics for all input and output queues.

Figure 4-21: Result of clearing statistics for all input and output queues

```
> clear qos queueing
Date 01.03.06 12:00:00 PM UTC
>
```

Display items

None

Impact on communication

None

Response messages

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

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.

Message	Description
Can't execute.	The command could not be executed. There are no active BSUs, CSUs, and MSUs. Make sure at least one BSV, CSU, or MSU is active before re-executing the command.
Illegal NIF -- <nif no.>.	The specified NIF number is invalid. Make sure the specified parameter is correct, and then try again. <nif no.>: NIF number
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Port number
No operational port.	There is no port that is active. Make sure the specified NIF is active, and then re-execute the command.

Notes

- If this command is executed, MIB information of the axxEtherTxQoS group is also cleared.
- If this command is executed, the number of discarded packets (Dropped Queue) displayed by executing the `show sflow` command is also cleared.

show qos queueing distribution

Displays information about distribution input and output queues of the specified port list.

Displays the following to monitor the traffic status:

- Length of a priority queue
- Maximum queue length
- Number of packets accumulated in a queue
- Number of bytes accumulated in a queue
- Statistics for the total of the items

For details about queues to be displayed, see the figures below in *show qos queueing*.

For AX6700S series switches: *Figure 4-12: Queues to be displayed (other than NK1GS-8M) [AX6700S]* and *Figure 4-13: Queues to be displayed (for NK1GS-8M) [AX6700S]*

For AX6600S series switches: *Figure 4-14: Queues to be displayed (other than NK1GS-8M) [AX6600S]* and *Figure 4-15: Queues to be displayed (for NK1GS-8M) [AX6600S]*

For AX6300S series switches: *Figure 4-16: Queues to be displayed (other than NH1GS-6M and NH10G-1RX) [AX6300S]*

Syntax

For AX6700S series switches:

```
show qos queueing distribution [<bsu no.>] <port list>
                               [{inbound | outbound [queue <queue number list>]}]
```

For AX6600S series switches:

```
show qos queueing distribution [<csu no.>] <port list>
                               [{inbound | outbound [queue <queue number list>]}]
```

For AX6300S series switches:

```
show qos queueing distribution <port list>
                               [{inbound | outbound [queue <queue number list>]}]
```

Input mode

User mode and administrator mode

Parameters

<bsu no.> [AX6700S]

Specifies the BSU number.

The specifiable range of BSU numbers is from 1 to 3. This parameter can be specified if the following applies:

1. When a distribution output queue is displayed
2. When the distribution input queue is displayed when allocation per source MAC address was configured for load balancing of BSUs

Note that the specified BSU number is ignored if allocation per port was configured for load balancing of BSUs and a distribution input queue is displayed.

Operation when this parameter is omitted:

Displays information of all BSUs to be installed.

<csu no.> [AX6600S]

Specify the CSU number.

The specifiable range of CSU numbers is from 1 to 2. This parameter can be specified if the following applies:

1. When a distribution output queue is displayed

Note that the specified CSU number is ignored if a distribution input queue is displayed.

Operation when this parameter is omitted:

Displays information of all CSUs to be installed.

<port list>

Specify the port number in list format. For the ports specified in the list, displays information about one or more associated queues. For details about how to specify *<port list>* and the specifiable range of values, see *Specifiable values for parameters*.

{inbound | outbound}

Specify an input queue or an output queue.

inbound

Displays information about an input queue.

outbound

Displays information about an output queue.

Operation when this parameter is omitted:

Displays information about input and output queues.

queue *<queue number list>*

Specify the queue number in list format. Displays information about the specified queue number.

The specifiable range of queue numbers is from 1 to 8.

This parameter can be specified only when an output queue is specified.

Operation when this parameter is omitted:

Displays information about all queue numbers.

Operation when all parameters are omitted:

Displays information about distribution input and output queues of the specified port list.

Example

- The following shows an example of displaying information when a distribution input queue is specified.

Figure 4-22: Result of displaying information when a distribution input queue is specified [AX6700S]

```
> show qos queueing distribution 1 1/1-24 inbound
Date 2008/04/16 17:38:47 UTC
Specified BSU number ignored in displaying of Distribution Inbound Queue.
BSU1:NIF1/Port1,3,5,7,9,11,13,15,17,19,21,23 (Distribution_Queue, inbound)
Max_Queue=1
Queue1: Qlen=0, Peak_Qlen=1, Limit_Qlen=127
        send_pkt      discard_pkt      send_byte
total          8              0          480
        :
        :
BSU1:NIF1/Port2,4,6,8,10,12,14,16,18,20,22,24 (Distribution_Queue, inbound)
Max_Queue=1
```

```

Queue1: Qlen=0, Peak_Qlen=1, Limit_Qlen=127
        send_pkt      discard_pkt      send_byte
total      10473035          0          14.7G
>

```

Note: "-" is displayed for the items that do not exist in the statistics counter.

Figure 4-23: Result of displaying information when a distribution input queue is specified [AX6600S]

```

> show qos queueing distribution 1 1/1-24 inbound
Date 2008/12/16 17:38:47 UTC
CSU1:NIF1/Port1,3,5,7,9,11,13,15,17,19,21,23 (Distribution_Queue, inbound)
Max_Queue=1
Queue1: Qlen=0, Peak_Qlen=1, Limit_Qlen=127
        send_pkt      discard_pkt      send_byte
total      10473035          0          14.7G
>

```

Note: "-" is displayed for the items that do not exist in the statistics counter.

Figure 4-24: Result of displaying information when a distribution input queue is specified [AX6300S]

```

> show qos queueing distribution 1/11 inbound
Date 2008/04/16 17:44:03 UTC
NIF1/Port1-24 (Distribution_Queue, inbound)
Max_Queue=1
Queue1: Qlen=0, Peak_Qlen=2, Limit_Qlen=127
        send_pkt      discard_pkt      send_byte
total      34877867          0          38.1G
>

```

Note: "-" is displayed for the items that do not exist in the statistics counter.

- The following shows an example of displaying information when a distribution output queue is specified.

Figure 4-25: Result of displaying information when a distribution output queue is specified [AX6700S]

```

> show qos queueing distribution 1 1/11 outbound
Date 2008/04/16 12:00:00 UTC
BSU1:NIF1/Port1-24 (Distribution_Queue1, outbound)
Max_Queue=8
Queue1: Qlen=0, Peak_Qlen=0, Limit_Qlen=2047
discard      send_pkt      discard_pkt      send_byte
1             0             0             -
2             0             0             -
3             0             0             -
4             0             0             -
total        0             0             0
:
:
BSU1:NIF1/Port1-24 (Distribution_Queue2, outbound)
Max_Queue=8
Queue1: Qlen=0, Peak_Qlen=2, Limit_Qlen=2047
discard      send_pkt      discard_pkt      send_byte
1             0             0             -
2             0             0             -
3             0             0             -
4            2122452         0             -
total        2122452         0            3072.6M
:
:
Queue8: Qlen=0, Peak_Qlen=2, Limit_Qlen=2047
discard      send_pkt      discard_pkt      send_byte
1             0             0             -
2             0             0             -

```

```

3              0              0              -
4          2122478              0              -
total        2122478              0          3072.6M
>

```

Note: "-" is displayed for the items that do not exist in the statistics counter.

Figure 4-26: Result of displaying information when a distribution output queue is specified [AX6600S]

```

> show qos queueing distribution 1 1/11 outbound
Date 2008/12/16 12:00:00 UTC
CSU1:NIF1/Port1-24 (Distribution_Queue, outbound)
Max_Queue=8
Queue1: Qlen=0, Peak_Qlen=0, Limit_Qlen=2047
  discard      send_pkt      discard_pkt      send_byte
  1              0              0              -
  2              0              0              -
  3              0              0              -
  4              0              0              -
total          0              0              0
      :
      :
Queue8: Qlen=0, Peak_Qlen=2, Limit_Qlen=2047
  discard      send_pkt      discard_pkt      send_byte
  1              0              0              -
  2              0              0              -
  3              0              0              -
  4          2122478              0              -
total        2122478              0          3072.6M
>

```

Note: "-" is displayed for the items that do not exist in the statistics counter.

Figure 4-27: Result of displaying information when a distribution output queue is specified [AX6300S]

```

> show qos queueing distribution 1/11 outbound
Date 2008/04/16 12:00:00 UTC
NIF1/Port1-24 (Distribution_Queue, outbound)
Max_Queue=8
Queue1: Qlen=0, Peak_Qlen=2, Limit_Qlen=2047
  discard      send_pkt      discard_pkt      send_byte
  1              0              0              -
  2              0              0              -
  3              0              0              -
  4          6405232              0              -
total        6405232              0          9272.7M
      :
      :
Queue8: Qlen=0, Peak_Qlen=3, Limit_Qlen=2047
  discard      send_pkt      discard_pkt      send_byte
  1              0              0              -
  2              0              0              -
  3              0              0              -
  4          6833698              0              -
total        6833698              0          9290.1M

To_Port_Queue
              discard_pkt
To NIF1/Port 9-12              0
>

```

Note: "-" is displayed for the items that do not exist in the statistics counter.

Display items

Table 4-8: Items displayed for statistics [AX6700S] [AX6600S]

Item	Displayed information		
	Detailed information		Meaning
BSU number specification information	Specified BSU number ignored in displaying of Distribution Inbound Queue.		Indicates that the BSU number specified for the distribution input queue is ignored. This information is displayed only if the BSU number is specified when allocation per port was configured for load balancing of BSUs.
Interface information	For AX6700S series switches:	BSU<bsu no.>:NIF<nif no.>/Port<port no.> (Distribution_Queue1, outbound)	Distribution output queue 1
		BSU<bsu no.>:NIF<nif no.>/Port<port no.>-<port no.> (Distribution_Queue1, outbound)	Distribution output queue 1
		BSU<bsu no.>:NIF<nif no.>/Port<port no.> (Distribution_Queue2, outbound)	Distribution output queue 2
		BSU<bsu no.>:NIF<nif no.>/Port<port no.>-<port no.> (Distribution_Queue2, outbound)	Distribution output queue 2
		BSU<bsu no.>:NIF<nif no.>/Port<port no.>-<port no.> (Distribution_Queue, inbound)	Distribution input queue [#] when allocation per port was configured for load balancing of BSUs
		BSU<bsu no.>:NIF<nif no.>/Port<port no.>-<port no.> (Distribution_Queue1, inbound)	Distribution input queue 1 [#] when allocation per source MAC address was configured for load balancing of BSUs
		BSU<bsu no.>:NIF<nif no.>/Port<port no.>-<port no.> (Distribution_Queue2, inbound)	Distribution input queue 2 [#] when allocation per source MAC address was configured for load balancing of BSUs
	For AX6600S series switches:	CSU<csu no.>:NIF<nif no.>/Port<port no.> (Distribution_Queue, outbound)	Distribution output queue
		CSU<csu no.>:NIF<nif no.>/Port<port no.>-<port no.> (Distribution_Queue, outbound)	Distribution output queue
		CSU<csu no.>:NIF<nif no.>/Port<port no.> (Distribution_Queue, inbound)	Distribution input queue
		CSU<csu no.>:NIF<nif no.>/Port<port no.>-<port no.> (Distribution_Queue, inbound)	Distribution input queue
QoS information	Max_Queue=<number of queue>		Number of queues
Queue information	Queue<queue no.>:		Queue number
	Qlen=<queue length>		Number of in-use packet buffers in a queue

Item	Displayed information	
	Detailed information	Meaning
	Peak_Qlen=<queue length>	Greatest number of in-use packet buffers in a queue
	Limit_Qlen=<queue length>	Limit of the number of in-use packet buffers in a queue
Statistics	discard	Queuing priority <ul style="list-style-type: none"> For details about queuing priority, see the description about the number of discard classes in <i>Table 6-32 Correspondence between NIF models and send control functionality (2 of 3)</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i> and <i>Table 6-33 Correspondence between NIF models and send control functionality (3 of 3)</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i> in 6.10 <i>Correspondence between NIF models and send control functionality</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i>.
	send_pkt	Number of packets accumulated in a queue
	discard_pkt	Number of packets discarded without being accumulated in a queue
	send_byte	Number of bytes in packets accumulated in a queue (unit k indicates 1024, M indicates 1024 ² , and G indicates 1024 ³). The range from the MAC header to DATA and PAD (excluding FCS) is included.
	total	Total of the items (unit k indicates 1024, M indicates 1024 ² , and G indicates 1024 ³).

Note: Port numbers corresponding to BSUs are displayed when hash mode is set.

Table 4-9: Items displayed for statistics [AX6300S]

Item	Displayed information	
	Detailed information	Meaning
Interface information	NIF<nif no.>/Port<port no.>- <port no.> (Distribution_Queue, outbound)	Distribution output queue
	NIF<nif no.>/Port<port no.>- <port no.> (Distribution_Queue, inbound)	Distribution input queue
	To_Port_Queue To NIF<nif no.>/Port<port no.>- <port no.>	Queues output to a port
QoS information	Max_Queue=<number of queue>	Number of queues
Queue information	Queue<queue no.>:	Queue number
	Qlen=<queue length>	Number of in-use packet buffers in a queue
	Peak_Qlen=<queue length>	Greatest number of in-use packet buffers in a queue

Item	Displayed information	
	Detailed information	Meaning
	Limit_Qlen=<queue length>	Limit of the number of in-use packet buffers in a queue
Statistics	discard	Queuing priority <ul style="list-style-type: none"> For details about queuing priority, see the description about the number of discard classes in <i>Table 6-35 Correspondence between NIF models and send control functionality (2 of 3)</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i> and <i>Table 6-36 Correspondence between NIF models and send control functionality (3 of 3)</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i> in <i>6.10 Correspondence between NIF models and send control functionality</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i>.
	send_pkt	Number of packets accumulated in a queue
	discard_pkt	Number of packets discarded without being accumulated in a queue
	send_byte	Number of bytes in packets accumulated in a queue (unit k indicates 1024, M indicates 1024 ² , and G indicates 1024 ³). The range from the MAC header to DATA and PAD (excluding FCS) is included.
	total	Total of the items (unit k indicates 1024, M indicates 1024 ² , and G indicates 1024 ³).

Impact on communication

None

Response messages

Table 4-10: List of response messages for the show qos queuing distribution command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. There are no active BSUs, CSUs, and MSUs. Make sure at least one BSU, CSU, or MSU is active before re-executing the command.
Illegal NIF -- <nif no.>.	The specified NIF number is invalid. Make sure the specified parameter is correct, and then try again. <nif no.>: NIF number
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Port number
No operational port.	There is no port that is active. Make sure the specified NIF is active, and then re-execute the command.
No support parameter -- <parameter>.	The specified parameter is not supported. Make sure the specified parameter is correct, and then try again. <parameter>: Parameter

4. QoS

Notes

None

clear qos queueing distribution

Clears all queue statistics displayed by executing the `show qos queueing distribution` command.

Syntax

For the AX6700S series:

```
clear qos queueing distribution [<bsu no.>] <port list> [{inbound | outbound}]
```

For the AX6600S series:

```
clear qos queueing distribution [<csu no.>] <port list> [{inbound | outbound}]
```

For the AX6300S series:

```
clear qos queueing distribution <port list> [{inbound | outbound}]
```

Input mode

User mode and administrator mode

Parameters

<bsu no.> [AX6700S]

Specifies the BSU number.

The specifiable range of BSU numbers is from 1 to 3. This parameter can be specified if the following applies:

1. When a distribution output queue is cleared
2. When the distribution input queue is cleared if allocation per source MAC address was configured for load balancing of BSUs

If a distribution input queue is cleared when allocation per port was configured for load balancing of BSUs, the specified BSU number is ignored and statistics for the BSU number with which <port list> is associated are cleared.

Operation when this parameter is omitted:

Clears statistics for all BSUs to be installed.

<csu no.> [AX6600S]

Specify the CSU number.

The specifiable range of CSU numbers is from 1 to 2. This parameter can be specified if the following applies:

1. When a distribution output queue is cleared

If the distribution input queue is cleared, the specified CSU number is ignored and statistics for the CSU number with which <port list> is associated are cleared.

Operation when this parameter is omitted:

Clears statistics for all CSUs to be installed.

<port list>

Specify the port number in list format. Clears information about the queue that includes one or more ports specified in the list. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

{inbound | outbound}

Specify an input queue or an output queue.

inbound

Clears statistics for an input queue.

outbound

Clears statistics for an output queue.

Operation when this parameter is omitted:

Clears statistics for input and output queues.

Operation when all parameters are omitted:

Clears distribution input and output queues for the specified port list.

Example

- The following shows an example of clearing statistics for a distribution input queue.

Figure 4-28: Result of clearing statistics for a distribution input queue (when the BSU number is specified) [AX6700S]

```
> clear qos queueing distribution 1 1/11
Specified BSU number ignored in clearing of Distribution Inbound Queue.
(Executed BSU1)
>
```

Figure 4-29: Result of clearing statistics for a distribution input queue (when the CSU number is specified) [AX6600S]

```
> clear qos queueing distribution 1 1/11
Date 2008/12/24 12:00:00 UTC
>
```

Figure 4-30: Result of clearing statistics for the distribution input queue

```
> clear qos queueing distribution 1/11 inbound
Date 2008/12/24 12:00:00 UTC
>
```

Display items

Table 4-11: Items displayed for statistics [AX6700S]

Item	Displayed information	
	Detailed information	Meaning
BSU number specification information	Specified BSU number ignored in clearing of Distribution Inbound Queue. (Executed BSU<bsu no.>)	Indicates that the BSU number specified for the distribution input queue is ignored. The BSU number that was actually cleared is displayed. This information is displayed only if the BSU number is specified when allocation per port was configured for load balancing of BSUs.

Display items

None

Impact on communication

None

Response messages

Table 4-12: List of response messages for the clear qos queueing distribution command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.

Message	Description
Can't execute.	The command could not be executed. There are no active BSUs, CSUs, and MSUs. Make sure at least one BSN, CSU, or MSU is active before re-executing the command.
Illegal NIF -- <i><nif no.></i> .	The specified NIF number is invalid. Make sure the specified parameter is correct, and then try again. <i><nif no.></i> : NIF number
Illegal Port -- <i><port no.></i> .	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <i><port no.></i> : Port number
No operational port.	There is no port that is active. Make sure the specified NIF is active, and then re-execute the command.
No support parameter -- <i><parameter></i> .	The specified parameter is not supported. Make sure the specified parameter is correct, and then try again. <i><parameter></i> : Parameter

Notes

- If this command is executed, MIB information of the axsEtherTxQoS group is also cleared.
- If this command is executed, the number of discarded packets (Dropped Queue) displayed by executing the `show sflow` command is also cleared.

show qos queueing interface

Displays information about port input and output queues of the specified port list.

Displays the following to monitor the traffic status:

- Length of a priority queue
- Maximum queue length
- Number of packets accumulated in a queue
- Number of bytes accumulated in a queue
- Statistics for the total of the items

For details about queues to be displayed, see figures from *Figure 4-12: Queues to be displayed (other than NK1GS-8M) [AX6700S]* to *Figure 4-18: Queues to be displayed (for NH10G-1RX)* in *show qos queueing*.

Syntax

```
show qos queueing interface <port list>
                        [{inbound | outbound [queue <queue number list>]}]
```

Input mode

User mode and administrator mode

Parameters

<port list>

Specify the port number in list format. For the ports specified in the list, displays information about one or more associated queues. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

{inbound | outbound}

Specify an input queue or an output queue.

inbound

Displays information about an input queue.

outbound

Displays information about an output queue.

Operation when this parameter is omitted:

Displays information about input and output queues.

queue <queue number list>

Specify the queue number in list format. Displays information about the specified queue number.

The specifiable range of queue numbers is from 1 to 8.

This parameter can be specified only when an output queue is specified.

Operation when this parameter is omitted:

Displays information about all queue numbers.

Operation when all parameters are omitted:

Displays information about input and output queues.

Example

- The following shows an example of displaying information when a port output queue is specified.

Figure 4-31: Result of displaying information when a port output queue is specified

```
> show qos queueing interface 1/1 outbound
Date 2008/04/16 12:00:00 UTC
NIF1/Port1 (outbound)
  Max_Queue=8, Rate=100Mbit/s, Schedule_mode=pq
  Queue1: Qlen=0, Peak_Qlen=51, Limit_Qlen=255, Drop_mode=tail_drop
            send_pkt      discard_pkt      send_byte
total          3203665              0          4625.6M
            :
            :
  Queue8: Qlen=0, Peak_Qlen=5, Limit_Qlen=255, Drop_mode=tail_drop
            send_pkt      discard_pkt      send_byte
total          3209301              0          4625.9M
>
Note: "-" is displayed for the items that do not exist in the statistics counter.
```

Display items

Table 4-13: Items displayed for statistics

Item	Displayed information	
	Detailed information	Meaning
Interface information	NIF< <i>nif no.</i> >/Port< <i>port no.</i> > (outbound)	Port output queue
	NIF< <i>nif no.</i> >/Port< <i>port no.</i> >-< <i>port no.</i> > (outbound)	Port output queue
	NIF< <i>nif no.</i> >/Port< <i>port no.</i> > (inbound)	Port input queue
	NIF< <i>nif no.</i> >/Port< <i>port no.</i> >-< <i>port no.</i> > (inbound)	Port input queue
QoS information	Max_Queue=< <i>number of queue</i> >	Number of queues
	Rate=< <i>rate</i> >	Bandwidth for which the legacy shaper functionality is performed. <ul style="list-style-type: none"> • When auto-negotiation is unresolved (including when processing is in progress) or for hierarchical Shaper NIF: - • For other than the above, the bandwidth to be displayed varies depending on whether port bandwidth control by legacy shaper is specified or not. When port bandwidth control is set: Set bandwidth When port bandwidth control is not set: Line speed
	Schedule_mode=< <i>schedule mode</i> >	Displays scheduling mode. For details about scheduling, see 6.1.2 <i>Scheduling</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i> .
Queue information	Queue< <i>queue no.</i> >:	Queue number
	Qlen=< <i>queue length</i> >	Number of in-use packet buffers in a queue
	Peak_Qlen=< <i>queue length</i> >	Greatest number of in-use packet buffers in a queue

Item	Displayed information	
	Detailed information	Meaning
	Limit_Qlen=<queue length>	Limit of the number of in-use packet buffers in a queue
	Drop_mode=tail_drop	Drop control mode: tail_drop
Statistics	discard	Queuing priority <ul style="list-style-type: none"> For details about queuing priority, see the description about the number of discard classes in <i>Table 6-32 Correspondence between NIF models and send control functionality (2 of 3)</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i> and <i>Table 6-33 Correspondence between NIF models and send control functionality (3 of 3)</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i> in <i>6.10 Correspondence between NIF models and send control functionality</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i>.
	send_pkt	Number of packets accumulated in a queue
	discard_pkt	Number of packets discarded without being accumulated in a queue
	send_byte	Number of bytes in packets accumulated in a queue (unit k indicates 1024, M indicates 1024 ² , and G indicates 1024 ³). The range from the MAC header to DATA and PAD (excluding FCS) is included.
	total	Total of the items (unit k indicates 1024, M indicates 1024 ² , and G indicates 1024 ³).

Impact on communication

None

Response messages

Table 4-14: List of response messages for the show qos queueing interface command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. There are no active BSUs, CSUs, and MSUs. Make sure at least one BSU, CSU, or MSU is active before re-executing the command.
Illegal NIF -- <nif no.>.	The specified NIF number is invalid. Make sure the specified parameter is correct, and then try again. <nif no.>: NIF number
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Port number
Illegal Queue -- <queue no.>.	The specified NIF number is invalid. Make sure the specified parameter is correct, and then try again. <queue no.>: Queue number

Message	Description
No operational port.	There is no port that is active. Make sure the specified NIF is active, and then re-execute the command.

Notes

None

clear qos queueing interface

Clears all queue statistics displayed by executing the `show qos queueing interface` command.

Syntax

```
clear qos queueing interface <port list> [{inbound | outbound}]
```

Input mode

User mode and administrator mode

Parameters

<port list>

Specify the port number in list format. Clears information about the queue that includes one or more ports specified in the list. For details about how to specify *<port list>* and the specifiable range of values, see *Specifiable values for parameters*.

{inbound | outbound}

Specify an input queue or an output queue.

inbound

Clears statistics for an input queue.

outbound

Clears statistics for an output queue.

Operation when this parameter is omitted:

Clears statistics for input and output queues.

Operation when all parameters are omitted:

Clears statistics for port input and output queues.

Example

- The following shows an example of clearing statistics for a port.

Figure 4-32: Result of clearing statistics for a port

```
> clear qos queueing interface 1/11
Date 2007/05/15 12:00:00 UTC
>
```

Display items

None

Impact on communication

None

Response messages

Table 4-15: List of response messages for the clear qos queueing interface command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.

Message	Description
Can't execute.	The command could not be executed. There are no active BSUs, CSUs, and MSUs. Make sure at least one Bsu, CSU, or MSU is active before re-executing the command.
Illegal NIF -- <i><nif no.></i> .	The specified NIF number is invalid. Make sure the specified parameter is correct, and then try again. <i><nif no.></i> : NIF number
Illegal Port -- <i><port no.></i> .	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <i><port no.></i> : Port number
No operational port.	There is no port that is active. Make sure the specified NIF is active, and then re-execute the command.

Notes

- If this command is executed, MIB information of the axsEtherTxQoS group is also cleared.
- If this command is executed, the number of discarded packets (Dropped Queue) displayed by executing the `show sflow` command is also cleared.

show qos queueing to-cpu

Displays information about queues output to the CPU.

Displays the following to monitor the traffic status:

- Length of a priority queue
- Maximum queue length
- Number of packets accumulated in a queue
- Number of bytes accumulated in a queue
- Statistics for the total of the items

For details about queues to be displayed, see figures from *Figure 4-12: Queues to be displayed (other than NK1GS-8M) [AX6700S]* to *Figure 4-18: Queues to be displayed (for NH10G-1RX)* in *show qos queueing*.

Syntax

For AX6700S series switches:

```
show qos queueing to-cpu [<bsu no.>] [queue <queue number list>]
```

For AX6600S series switches:

```
show qos queueing to-cpu [<csu no.>] [queue <queue number list>]
```

For AX6300S series switches:

```
show qos queueing to-cpu [queue <queue number list>]
```

Input mode

User mode and administrator mode

Parameters

<bsu no.> [AX6700S]

Specifies the BSU number.

The specifiable range of BSU numbers is from 1 to 3. This parameter can be specified if the following applies:

1. When a distribution output queue is displayed
2. When the distribution input queue is displayed when allocation per source MAC address was configured for load balancing of BSUs

Note that the specified BSU number is ignored if allocation per port was configured for load balancing of BSUs and a distribution input queue is displayed.

Operation when this parameter is omitted:

Displays information of all BSUs to be installed.

<csu no.> [AX6600S]

Specify the CSU number.

The specifiable range of CSU numbers is from 1 to 2. This parameter can be specified if the following applies:

1. When queues output to the CPU are displayed

Operation when this parameter is omitted:

Displays information of all CSUs to be installed.

queue <queue number list>

Specify the queue number in list format. Displays information about the specified queue number.

For AX6700S and AX6600S series switches, the specifiable range of queue numbers is from 1 to 16.

For AX6300S series switches, the specifiable range of queue numbers is from 1 to 8.

This parameter can be set only if a queue for a port is specified as the queue type and the output queue is specified.

Operation when this parameter is omitted:

Displays information about all queue numbers.

Operation when all parameters are omitted:

Displays information about queues output to the CPU.

Example

- The following shows an example of displaying information when queues output to the CPU are specified.

Figure 4-33: Result of displaying information when queues output to the CPU are specified [AX6700S]

```
> show qos queueing to-cpu 1
Date 2008/04/16 12:00:00 UTC
BSU1:To-CPU
Max_Queue=16
Queue1: Qlen=0, Peak_Qlen=1, Limit_Qlen=1023
  discard      send_pkt      discard_pkt      send_byte
  1              0              0              -
  2              0              0              -
  3              0              0              -
  4             107              0              -
  total         107              0             9.7k
      :
      :
Queue16: Qlen=0, Peak_Qlen=2, Limit_Qlen=1023
  discard      send_pkt      discard_pkt      send_byte
  1              0              0              -
  2              0              0              -
  3              0              0              -
  4             277              0              -
  total         277              0            16.2k
>
```

Note: "-" is displayed for the items that do not exist in the statistics counter.

Figure 4-34: Result of displaying information when queues output to the CPU are specified [AX6600S]

```
> show qos queueing to-cpu 1
Date 2008/12/16 12:00:00 UTC
CSU1:To-CPU
Max_Queue=8
Queue1: Qlen=0, Peak_Qlen=1, Limit_Qlen=1023
  discard      send_pkt      discard_pkt      send_byte
  1              0              0              -
  2              0              0              -
  3              0              0              -
  4             107              0              -
  total         107              0             9.7k
      :
      :
Queue8: Qlen=0, Peak_Qlen=2, Limit_Qlen=1023
```

4. QoS

```

discard      send_pkt      discard_pkt      send_byte
1            0             0             -
2            0             0             -
3            0             0             -
4            277           0             -
total        277           0             16.2k

```

>

Note: "-" is displayed for the items that do not exist in the statistics counter.

Figure 4-35: Result of displaying information when queues output to the CPU are specified [AX6300S]

```

> show qos queueing to-cpu
Date 2008/04/16 12:00:00 UTC
To-CPU
Max_Queue=8
Queue1: Qlen=0, Peak_Qlen=384, Limit_Qlen=1023
discard      send_pkt      discard_pkt      send_byte
1            93411         3165766         -
2            0             0             -
3            0             0             -
4            2             0             -
total        93413         3165766         14.5M
:
:
Queue8: Qlen=0, Peak_Qlen=0, Limit_Qlen=1023
discard      send_pkt      discard_pkt      send_byte
1            0             0             -
2            0             0             -
3            0             0             -
4            0             0             -
total        0             0             0

```

>

Note: "-" is displayed for the items that do not exist in the statistics counter.

Display items

Table 4-16: Items displayed for statistics [AX6700S] [AX6600S]

Item	Displayed information	
	Detailed information	Meaning
Interface information	BSU<bsu no.>:To-CPU	Queues output to the CPU [AX6700S]
	CSU<csu no.>:To-CPU	Queues output to the CPU [AX6600S]
QoS information	Max_Queue=<number of queue>	Number of queues
Queue information	Queue<queue no.>:	Queue number
	Qlen=<queue length>	Number of in-use packet buffers in a queue
	Peak_Qlen=<queue length>	Greatest number of in-use packet buffers in a queue
	Limit_Qlen=<queue length>	Limit of the number of in-use packet buffers in a queue

Item	Displayed information	
	Detailed information	Meaning
Statistics	discard	<p>Queuing priority</p> <ul style="list-style-type: none"> For details about queuing priority, see the description about the number of discard classes in <i>Table 6-32 Correspondence between NIF models and send control functionality (2 of 3)</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i> and <i>Table 6-33 Correspondence between NIF models and send control functionality (3 of 3)</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i> in <i>6.10 Correspondence between NIF models and send control functionality</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i>.
	send_pkt	Number of packets accumulated in a queue
	discard_pkt	Number of packets discarded without being accumulated in a queue
	send_byte	<p>Number of bytes in packets accumulated in a queue (unit k indicates 1024, M indicates 1024², and G indicates 1024³).</p> <p>The range from the MAC header to DATA and PAD (excluding FCS) is included.</p>
	total	Total of the items (unit k indicates 1024, M indicates 1024 ² , and G indicates 1024 ³).

Table 4-17: Items displayed for statistics [AX6300S]

Item	Displayed information	
	Detailed information	Meaning
Interface information	To-CPU	Queues output to the CPU
QoS information	Max_Queue=<number of queue>	Number of queues
Queue information	Queue<queue no.>:	Queue number
	Qlen=<queue length>	Number of in-use packet buffers in a queue
	Peak_Qlen=<queue length>	Greatest number of in-use packet buffers in a queue
	Limit_Qlen=<queue length>	Limit of the number of in-use packet buffers in a queue

Item	Displayed information	
	Detailed information	Meaning
Statistics	discard	Queuing priority <ul style="list-style-type: none"> For details about queuing priority, see the description about the number of discard classes in <i>Table 6-35 Correspondence between NIF models and send control functionality (2 of 3)</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i> and <i>Table 6-36 Correspondence between NIF models and send control functionality (3 of 3)</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i> in <i>6.10 Correspondence between NIF models and send control functionality</i> in the manual <i>Configuration Guide Vol. 2 For Version 11.7</i>.
	send_pkt	Number of packets accumulated in a queue
	discard_pkt	Number of packets discarded without being accumulated in a queue
	send_byte	Number of bytes in packets accumulated in a queue (unit k indicates 1024, M indicates 1024 ² , and G indicates 1024 ³). The range from the MAC header to DATA and PAD (excluding FCS) is included.
	total	Total of the items (unit k indicates 1024, M indicates 1024 ² , and G indicates 1024 ³).

Impact on communication

None

Response messages

Table 4-18: List of response messages for the show qos queueing to-cpu command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. There are no active BSUs, CSUs, and MSUs. Make sure at least one BSU, CSU, or MSU is active before re-executing the command.
Illegal NIF -- <nif no.>.	The specified NIF number is invalid. Make sure the specified parameter is correct, and then try again. <nif no.>: NIF number
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Port number
No operational port.	There is no port that is active. Make sure the specified NIF is active, and then re-execute the command.

Notes

None

clear qos queueing to-cpu

Clears all queue statistics displayed by executing the `show qos queueing to-cpu` command.

Syntax

For the AX6700S series switches:
`clear qos queueing to-cpu [<bsu no.>]`

For the AX6600S series switches:
`clear qos queueing to-cpu [<csu no.>]`

For the AX6300S series switches:
`clear qos queueing to-cpu`

Input mode

User mode and administrator mode

Parameters

<bsu no.> [AX6700S]

Specifies the BSU number.

The specifiable range of BSU numbers is from 1 to 3. This parameter can be specified if the following applies:

1. When a distribution output queue is cleared
2. When the distribution input queue is cleared if allocation per source MAC address was configured for load balancing of BSUs

If a distribution input queue is cleared when allocation per port was configured for load balancing of BSUs, the specified BSU number is ignored and statistics for the BSU number with which <port list> is associated are cleared.

Operation when this parameter is omitted:

Clears statistics for all BSUs to be installed.

<csu no.> [AX6600S]

Specifies the CSU number.

The specifiable range of CSU numbers is from 1 to 2. This parameter can be specified if the following applies:

1. When a queue output to the CPU is cleared

Operation when this parameter is omitted:

Clears statistics for all CSUs to be installed.

Operation when all parameters are omitted:

Clears statistics for the queue output to the CPU.

Example

- The following shows an example of clearing statistics for the queue output to the CPU.

Figure 4-36: Result of clearing statistics for the queue output to the CPU

```
> clear qos queueing to-cpu
Date 2007/09/11 12:00:00 UTC
>
```

Display items

None

Impact on communication

None

Response messages*Table 4-19:* List of response messages for the clear qos queueing to-cpu command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. There are no active BSUs, CSUs, and MSUs. Make sure at least one BCU, CSU, or MSU is active before re-executing the command.

Notes

- If this command is executed, MIB information of the axxEtherTxQoS group is also cleared.
- If this command is executed, the number of discarded packets (Dropped Que) displayed by executing the `show sflow` command is also cleared.

show shaper

Outputs statistics for the hierarchical shaper functionality.

Displays the following to monitor the traffic status:

- Port buffer information.
- Number of output or discarded packets in output queues, number of output and discarded bytes, and queue length

Syntax

```
show shaper [{ all | discard-mode }]
```

Input mode

User mode and administrator mode

Parameters

all

Displays all statistics for a hierarchical shaper.

- Port buffer information.
- Number of output or discarded packets in output queues, number of output or discarded bytes, queue length, and discard mode.

discard-mode

Displays the following statistics about drop control:

Number of discarded packets in output queues, number of discarded bytes, discard mode, and queue length.

Operation when all parameters are omitted:

Displays statistics for the number of output or discarded packets in a queue and the queue length.

Example

Figure 4-37: Displayed information when all is specified

```
> show shaper all
Date 2008/06/24 12:00:00 UTC
NIF 1/Port 1, Shaper_mode:RGQ
Set_default_user_priority:disable
Predicted_tail_drop:disable, Vlan_user_map:disable
Port Rate_limit=1Gbit/s
Buffer
  QoS1=   194/   1812/   2000 QoS2=    82/   1784/   2000
  QoS3=    74/   1582/   1500 QoS4=    71/   1422/   1500
  QoS5=    68/   1398/   1500 QoS6=    61/   1284/   1500
  QoS7=    51/   1231/   1000 QoS8=    41/   1098/   1000

User:default-user, DEFAULT-LIST
Schedule_mode=PQ
Peak_rate=1Mbit/s, Min_rate=500kbit/s, Weight=1
Queue      send_pkt      discard_pkt  Queue_length
1           6533          3451        10/ 120/ 120
2           2564          1581         5/ 120/ 120
3        2256877          235         4/ 100/ 100
4        4698951           0         4/  90/ 100
5        15875213           0         3/  70/  80
6        25987192           0         1/  65/  80
7        28753135           0         1/  45/  50
```

4. QoS

```

      8          38419319          0    1/ 43/ 50
total        116008881          5267    -

Queue      send_byte      discard_byte  discard_mode
1           9.5M          5.0M      tail-drop2
2           3.7M          2.3M      tail-drop2
3           3.2G          348.4k     tail-drop2
4           6.6G           0        tail-drop2
5          22.4G           0        tail-drop2
6          36.7G           0        tail-drop2
7          40.6G           0        tail-drop2
8          54.3G           0        tail-drop2
total        164.0G          7.6M      -

User:ID=1, USER-A
Schedule_mode=PQ
Peak_rate=500Mbit/s, Min_rate=250Mbit/s, Weight=10
Queue      send_pkt      discard_pkt  Queue_length
1           6324          3781      12/ 120/ 120
2           2873          1761      4/ 120/ 120
3          2200134          331      3/ 100/ 100
4          4781911           0      1/ 89/ 100
5          14890111          0      1/ 65/ 80
6          23091811          0      1/ 63/ 80
7          27576011          0      1/ 41/ 50
8          37910013          0      1/ 35/ 50
total       110459188          5873      -

Queue      send_byte      discard_byte  discard_mode
1           9.2M          5.5M      tail-drop2
2           4.2M          2.5M      tail-drop2
3           3.1G          348.4k     tail-drop2
4           6.8G           0        tail-drop2
5          21.1G           0        tail-drop2
6          32.6G           0        tail-drop2
7          40.0G           0        tail-drop2
8          53.6G           0        tail-drop2
total       156.2G          8.5M      -

...
...
...

NIF 1/Port 2, Shaper_mode:RGQ
Set_default_user_priority:disable
Predicted_tail_drop:disable, Vlan_user_map:disable
Port Rate_limit=1Gbit/s

...
...
...

Discard packets(User not configured):          2585910248
>

```

Figure 4-38: Displayed information when discard-mode is specified

```

> show shaper discard-mode
Date 2008/06/24 12:00:00 UTC
NIF 1/Port 1, Shaper_mode:RGQ
Set_default_user_priority:disable
Predicted_tail_drop:disable, Vlan_user_map:disable
Port Rate_limit=1Gbit/s
Buffer
QoS1=   194/   1812/   2000 QoS2=    82/   1784/   2000
QoS3=    74/   1582/   1500 QoS4=    71/   1422/   1500
QoS5=    68/   1398/   1500 QoS6=    61/   1284/   1500
QoS7=    51/   1231/   1000 QoS8=    41/   1098/   1000

```

```

User:default-user, DEFAULT-LIST
Schedule_mode=PQ
Peak_rate=1Mbit/s, Min_rate=500kbit/s, Weight=1
Queue      discard_pkt  discard_byte  discard_mode
1           3451         5.0M         tail-drop2
2           1581         2.3M         tail-drop2
3            235        348.4k         tail-drop2
4             0           0         tail-drop2
5             0           0         tail-drop2
6             0           0         tail-drop2
7             0           0         tail-drop2
8             0           0         tail-drop2
total       5267         7.6M         -

User:ID=1, USER-A
Schedule_mode=PQ
Peak_rate=500Mbit/s, Min_rate=250Mbit/s, Weight=10
Queue      discard_pkt  discard_byte  discard_mode
1           3781         5.5M         tail-drop2
2           1761         2.5M         tail-drop2
3            331        348.4k         tail-drop2
4             0           0         tail-drop2
5             0           0         tail-drop2
6             0           0         tail-drop2
7             0           0         tail-drop2
8             0           0         tail-drop2
total       5873         8.5M         -

...
...
...

NIF 1/Port 2, Shaper_mode:RGQ
Set_default_user_priority:disable
Predicted_tail_drop:disable, Vlan_user_map:disable
Port Rate_limit=1Gbit/s

...
...
...

Discard packets(User not configured):123456789012345678
>

```

Figure 4-39: Displayed information when all parameters are omitted

```

> show shaper
Date 2008/06/24 12:00:00 UTC
NIF 1/Port 1, Shaper_mode:RGQ
Set_default_user_priority:disable
Predicted_tail_drop:disable, Vlan_user_map:disable
Port Rate_limit=1Gbit/s

User:default-user, DEFAULT-LIST
Schedule_mode=PQ
Peak_rate=1Mbit/s, Min_rate=500kbit/s, Weight=1
Queue      send_pkt      discard_pkt  Queue_length
1           6533          3451        10/ 120/ 120
2           2564          1581         5/ 120/ 120
3        2256877           235         4/ 100/ 100
4        4698951            0         4/  90/ 100
5        15875213            0         3/  70/  80
6        25987192            0         1/  65/  80
7        28753135            0         1/  45/  50
8        38419319            0         1/  43/  50
total      116008881         5267         -

User:ID=1, USER-A
Schedule_mode=PQ

```

```

Peak_rate=500Mbit/s, Min_rate=250Mbit/s, Weight=10
Queue      send_pkt      discard_pkt  Queue_length
1           6324           3781      12/ 120/ 120
2           2873           1761      4/ 120/ 120
3          2200134           331      3/ 100/ 100
4          4781911            0      1/ 89/ 100
5          14890111            0      1/ 65/ 80
6          23091811            0      1/ 63/ 80
7          27576011            0      1/ 41/ 50
8          37910013            0      1/ 35/ 50
total      110459188          5873      -

```

```

...
...
...

```

```

NIF 1/Port 2, Shaper_mode:RGQ
Set_default_user_priority:disable
Predicted_tail_drop:disable, Vlan_user_map:disable
Port Rate_limit=1Gbit/s

```

```

...
...
...

```

```

>

```

Display items

Table 4-20: Items displayed for statistics

Item	Displayed information		
	Detailed information		Meaning
Port information	NIF<nif no.>/Port<port no.>		Ethernet interface information
	Shaper_mode:<shaper mode>		Shaper mode. "-" is displayed when this item is not set.
	Set_default_user_priority		Indicates whether modification of default user priority is set. enable: Set disable: Not set
	Predicted_tail_drop		Indicates whether predicted tail drop is set. enable: Set disable: Not set
	Vlan_user_map		Indicates whether VLAN user mapping is set. enable: Set disable: Not set
	Port Rate_limit=<rate>		Port bandwidth control setting value. "(*)" is displayed if the line speed is less than the specified bandwidth.
	Buffer	QoS<no.>=<buffer>/<peak buffer>/<limit buffer>	Port buffer information. QoS<no.>: Queue number <buffer>: Number of currently in-use buffers <peak buffer>: Greatest number of in-use buffers <limit buffer>: Specified buffer size
Group information [AX6700S] [AX6600S]	Group:	WGQ	WGQ bandwidth control is used.

Item	Displayed information		
	Detailed information		Meaning
	Rate_limit=<rate>		A value set as the maximum bandwidth for a group. " (*) " is displayed if the line speed is less than the specified bandwidth.
User information	User:	ID=<user id>, <user list name>	User ID, and user list name
		llrlq1, <user list name> [AX6700S] [AX6600S]	llrlq1 user, and user list name
		llrlq2, <user list name> [AX6700S] [AX6600S]	llrlq2 user, and user list name
		default-user, <user list name>	Default user, and user list name
	Schedule_mode=<schedule mode>		Scheduling mode
	Peak_rate=<rate>		A value set as the maximum bandwidth for user bandwidth control " (*) " is displayed if the line speed is less than the maximum bandwidth.
	Min_rate=<rate>		A value set as the minimum bandwidth for user bandwidth control If the total of the minimum bandwidth for ports is greater than the line speed, " (*) " is displayed.
	Weight=<weight>		A value set as weighting for user bandwidth control
	LLPQ_peak_rate=<rate> [AX6700S] [AX6600S]		A value set as the maximum bandwidth for LLPQ. " (*) " is displayed if the line speed is less than the specified bandwidth.
Queue information	Queue		Queue number
Statistics	send_pkt		Number of packets accumulated in a queue
	discard_pkt		Number of packets discarded without being accumulated in a queue
	Queue_length	<queue length>/<peak queue length>/<limit queue length>	Queue length information. <queue length>: Number of in-use buffers <peak queue length>: Greatest number of in-use buffers <limit queue length>: Limit of the number of in-use buffers
	send_byte		Number of bytes in packets accumulated in a queue [#]
	discard_byte		Number of bytes in packets discarded without being accumulated in a queue [#]
	discard_mode		Specified discard mode. "-" is displayed if VLAN user mapping is set.
	total		Total value of the items

Item	Displayed information	
	Detailed information	Meaning
	Discard packets(User not configured)	Total number of discarded packets of a user for whom configuration is not specified in the hierarchical shaper information

#: The range from the MAC header to FCS is used.

Impact on communication

None

Response messages

Table 4-21: List of response messages for the show shaper command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
No operational port.	There is no port that is active. Possible causes are as follows: <ul style="list-style-type: none"> Make sure the specified NIF is active, and then re-execute the command. The NIF number and the port number you specified are invalid. Make sure the specified parameter is correct, and then try again.
Not support NIF.	The specified NIF does not support the hierarchical shaper functionality. Execute the command for the supported NIF.

Notes

Discard packets(User not configured) is the total number of discarded packets of a user for whom configuration is not specified in the hierarchical shaper information. Therefore if a user is added in the configuration, the number of discarded packets of the user is subtracted from the total value.

clear shaper

Clears statistics for all hierarchical shaper functionality.

Syntax

```
clear shaper
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 4-40: Result of clearing information

```
> clear shaper
Date 2008/06/24 12:00:00 UTC
>
```

Display items

None

Impact on communication

None

Response messages

Table 4-22: List of response messages for the clear shaper command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
No operational port.	There is no port that is active. Possible causes are as follows: <ul style="list-style-type: none"> Make sure the specified NIF is active, and then re-execute the command. The NIF number and the port number you specified are invalid. Make sure the specified parameter is correct, and then try again.
Not support NIF.	The specified NIF does not support the hierarchical shaper functionality. Execute the command for the supported NIF.

Notes

If this command is executed, MIB information of the axsShaperUser group is also cleared.

show shaper <port list>

Outputs statistics for a hierarchical shaper of the specified Ethernet interface.

Displays the following to monitor the traffic status:

- Port buffer information.
- Number of output or discarded packets in output queues, number of output or discarded bytes, queue length, and communication rate.

Syntax

For AX6700S and AX6600S series switches:

```
show shaper <port list> [ user <user id list> ] [ default-user ] [ llrlq1 ] [ llrlq2 ]
[{ all | discard-mode | rate }]
```

For AX6300S series switches:

```
show shaper <port list> [ user <user id list> ] [ default-user ] [{ all | discard-mode
| rate }]
```

Input mode

User mode and administrator mode

Parameters

<port list>

Specify the port number in list format. For the ports specified in the list, displays information about one or more associated queues. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

user <user id list>

Displays statistics for the specified user ID.

<user id list>

Multiple user IDs can be specified by using a hyphen (-) or a comma (,).

You can also specify one user ID, as when <user id> is written as the parameter input format.

If a hyphen (-) or a comma (,) is used, the specifiable range is user ID values set in the configuration.

For AX6700S and AX6600S, the specifiable range of user IDs is from 1 to 1023.

For AX6300S, the specifiable range of user IDs is from 1 to 511.

If VLAN user mapping is used, specify the VLAN ID.

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

1-3,5,10

default-user

Displays statistics of the default user.

llrlq1 [AX6700S] [AX6600S]

Displays statistics for llrlq1.

llrlq2 [AX6700S] [AX6600S]

Displays statistics for llrlq2.

all

Displays all statistics for a hierarchical shaper.

- Port buffer information.
- Number of output or discarded packets in output queues, number of output or discarded bytes, queue length, and discard mode.

discard-mode

Displays the following statistics about drop control:

Number of discarded packets in output queues, number of discarded bytes, discard mode, and queue length.

rate

Displays the following information about the communication rate:

Number of output packets in output queues, number of output bytes, and communication rate (bits per second, packets per second).

For calculation of communication rate (bits per second), the range from the MAC header to FCS is used.

Example

Figure 4-41: Displayed information when all is specified

```
> show shaper 1/1 user 1 all
Date 2008/06/24 12:00:00 UTC
NIF 1/Port 1, Shaper_mode:RGQ
Set_default_user_priority:disable
Predicted_tail_drop:disable, Vlan_user_map:disable
Port Rate_limit=1Gbit/s
Buffer
QoS1=   194/   1812/   2000 QoS2=    82/   1784/   2000
QoS3=    74/   1582/   1500 QoS4=    71/   1422/   1500
QoS5=    68/   1398/   1500 QoS6=    61/   1284/   1500
QoS7=    51/   1231/   1000 QoS8=    41/   1098/   1000

User:ID=1, USER-A
Schedule_mode=PQ
Peak_rate=500Mbit/s, Min_rate=250Mbit/s, Weight=10
Queue      send_pkt      discard_pkt      Queue_length
1           6324           3781      12/ 120/ 120
2           2873           1761      4/ 120/ 120
3          2200134           331      3/ 100/ 100
4          4781911            0      1/  89/ 100
5          14890111            0      1/  65/  80
6          23091811            0      1/  63/  80
7          27576011            0      1/  41/  50
8          37910013            0      1/  35/  50
total      110459188           5873      -

Queue      send_byte      discard_byte      discard_mode
1           9.2M           5.5M      tail-drop2
2           4.2M           2.5M      tail-drop2
3           3.1G          348.4k      tail-drop2
4           6.8G            0      tail-drop2
5          21.1G            0      tail-drop2
6          32.6G            0      tail-drop2
7          40.0G            0      tail-drop2
8          53.6G            0      tail-drop2
total      156.2G           8.5M      -

Discard packets(User not configured):      2585910248
>
```

Figure 4-42: Displayed information when discard-mode is specified

```

> show shaper 1/1 user 1 discard-mode
Date 2008/06/24 12:00:00 UTC
NIF 1/Port 1, Shaper_mode:RGQ
Set_default_user_priority:disable
Predicted_tail_drop:disable, Vlan_user_map:disable
Port Rate_limit=1Gbit/s
Buffer
  QoS1=   194/   1812/   2000 QoS2=    82/   1784/   2000
  QoS3=    74/   1582/   1500 QoS4=    71/   1422/   1500
  QoS5=    68/   1398/   1500 QoS6=    61/   1284/   1500
  QoS7=    51/   1231/   1000 QoS8=    41/   1098/   1000

User:ID=1, USER-A
Schedule_mode=PQ
Peak_rate=500Mbit/s, Min_rate=250Mbit/s, Weight=10
Queue      discard_pkt  discard_byte  discard_mode
1           3781        5.5M      tail-drop2
2           1761        2.5M      tail-drop2
3            331       348.4k     tail-drop2
4              0          0      tail-drop2
5              0          0      tail-drop2
6              0          0      tail-drop2
7              0          0      tail-drop2
8              0          0      tail-drop2
total       5873        8.5M      -

Discard packets(User not configured):123456789012345678
>

```

Figure 4-43: Displayed information when rate is specified

```

> show shaper 1/1 user 1 rate
Date 2008/06/24 12:00:00 UTC
NIF 1/Port 1, Shaper_mode:RGQ
Set_default_user_priority:disable
Predicted_tail_drop:disable, Vlan_user_map:disable
Port Rate_limit=1Gbit/s

User:ID=1, USER-A
Schedule_mode=PQ
Peak_rate=500Mbit/s, Min_rate=250Mbit/s, Weight=10
Queue      send_pkt      send_byte  packet/s  bit/s
1           6533          9.2M       1k        98k
2           2873          4.2M       2k       258k
3        2200134          3.1G       15k       198k
4        4781911          6.8G        3k      1024k
5       14890111         21.1G       10k       157k
6       23091811         32.6G        8k       283k
7       27576011         40.0G        90k      384k
8       37910013         53.6G        56k      829k
total     110459188       156.2G      185k     3231k
>

```

Display items

Table 4-23: Items displayed for statistics

Item	Displayed information	
	Detailed information	Meaning
Port information	NIF<nif no.>/Port<port no.>	Ethernet interface information
	Shaper_mode:<shaper mode>	Shaper mode. " - " is displayed when this item is not set.

Item	Displayed information		
	Detailed information		Meaning
	Set_default_user_priority		Indicates whether modification of default user priority is set. enable: Set disable: Not set
	Predicted_tail_drop		Indicates whether predicted tail drop is set. enable: Set disable: Not set
	Vlan_user_map		Indicates whether VLAN user mapping is set. enable: Set disable: Not set
	Port Rate_limit=<rate>		Port bandwidth control setting value. " (*) " is displayed if the line speed is less than the specified bandwidth.
	Buffer	QoS<no.>=<buffer>/<peak buffer>/<limit buffer>	Port buffer information. QoS<no.>: Queue number <buffer>: Number of currently in-use buffers <peak buffer>: Greatest number of in-use buffers <limit buffer>: Specified buffer size
Group information [AX6700S] [AX6600S]	Group:	WGQ	WGQ bandwidth control is used.
	Rate_limit=<rate>		A value set as the maximum bandwidth for a group. " (*) " is displayed if the line speed is less than the specified bandwidth.
User information	User:	ID=<user id>, <user list name>	User ID, and user list name
		llrlq1, <user list name> [AX6700S] [AX6600S]	llrlq1 user, and user list name
		llrlq2, <user list name> [AX6700S] [AX6600S]	llrlq2 user, and user list name
		default-user, <user list name>	Default user, and user list name
	Schedule_mode=<schedule mode>		Scheduling mode
	Peak_rate=<rate>		A value set as the maximum bandwidth for user bandwidth control " (*) " is displayed if the line speed is less than the maximum bandwidth.
	Min_rate=<rate>		A value set as the minimum bandwidth for user bandwidth control If the total of the minimum bandwidth for ports is greater than the line speed, " (*) " is displayed.
	Weight=<weight>		A value set as weighting for user bandwidth control

Item	Displayed information	
	Detailed information	Meaning
	LLPQ_peak_rate=<rate> [AX6700S] [AX6600S]	A value set as the maximum bandwidth for LLPQ. "(*)" is displayed if the line speed is less than the specified bandwidth.
Queue information	Queue	Queue number
Statistics	send_pkt	Number of packets accumulated in a queue
	discard_pkt	Number of packets discarded without being accumulated in a queue
	Queue_length	Queue length information. <queue length>: Number of in-use buffers <peak queue length>: Greatest number of in-use buffers <limit queue length>: Limit of the number of in-use buffers
	send_byte	Number of bytes in packets accumulated in a queue [#]
	discard_byte	Number of bytes in packets discarded without being accumulated in a queue [#]
	discard_mode	Specified discard mode. "-" is displayed if VLAN user mapping is set.
	total	Total value of the items
	Discard packets(User not configured)	Total number of discarded packets of a user for whom configuration is not specified in the hierarchical shaper information
	packet/s	Packet transfer speed calculated using the time when a command is entered as the start point and the time 1 second later as the end point.
	bit/s	Data transfer speed calculated using the time when a command is entered as the start point and the time 1 second later as the end point. The speed is calculated using data from the MAC header to FCS.

[#]: The range from the MAC header to FCS is used.

Impact on communication

None

Response messages

Table 4-24: List of response messages for the show shaper <port list> command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
Illegal user id.	The specified user ID is invalid. Make sure the specified parameter is correct, and then try again.
No operational port.	There is no port that is active. Possible causes are as follows: <ul style="list-style-type: none"> Make sure the specified NIF is active, and then re-execute the command. The NIF number and the port number you specified are invalid. Make sure the specified parameter is correct, and then try again.
Not support NIF.	The specified NIF does not support the hierarchical shaper functionality. Execute the command for the supported NIF.

Notes

- The value displayed when the communication rate is specified might be slightly inaccurate because the value is calculated by software. As a result, a value exceeding the physical bandwidth might be displayed.
- Discard packets(User not configured) is the total number of discarded packets of a user for whom configuration is not specified in the hierarchical shaper information. Therefore if a user is added in the configuration, the number of discarded packets of the user is subtracted from the total value.

clear shaper <port list>

Clears statistics for the hierarchical shaper functionality of the specified Ethernet interface.

Syntax

For AX6700S and AX6600S series switches:

```
clear shaper <port list> [ user <user id list> ] [ default-user ] [ llrlq1 ] [ llrlq2 ]
```

For AX6300S series switches:

```
clear shaper <port list> [ user <user id list> ] [ default-user ]
```

Input mode

User mode and administrator mode

Parameters

<port list>

Specify the port number in list format. For the ports specified in the list, displays information about one or more associated queues. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

user <user id list>

Clears statistics for the specified user ID.

<user id list>

Multiple user IDs can be specified by using a hyphen (-) or a comma (,).

You can also specify one user ID, as when <user id> is written as the parameter input format.

If a hyphen (-) or a comma (,) is used, the specifiable range is user ID values set in the configuration.

For AX6700S and AX6600S, the specifiable range of user IDs is from 1 to 1023.

For AX6300S, the specifiable range of user IDs is from 1 to 511.

If VLAN user mapping is used, specify the VLAN ID.

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

1-3,5,10

default-user

Clears statistics for the default user.

llrlq1 [AX6700S] [AX6600S]

Clears statistics for llrlq1.

llrlq2 [AX6700S] [AX6600S]

Clears statistics for llrlq2.

Example

Figure 4-44: Result of clearing information

```
> clear shaper 1/1
Date 2008/06/24 12:00:00 UTC
>
```

Display items

None

Impact on communication

None

Response messages*Table 4-25:* List of response messages for the clear shaper <port list> command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Illegal user id.	The specified user ID is invalid. Make sure the specified parameter is correct, and then try again.
No operational port.	There is no port that is active. Possible causes are as follows: <ul style="list-style-type: none"> Make sure the specified NIF is active, and then re-execute the command. The NIF number and the port number you specified are invalid. Make sure the specified parameter is correct, and then try again.
Not support NIF.	The specified NIF does not support the hierarchical shaper functionality. Execute the command for the supported NIF.

Notes

If this command is executed, MIB information of the axsShaperUser group is also cleared.

Chapter

5. IEEE802.1X

```
show dot1x statistics
show dot1x
clear dot1x statistics
clear dot1x auth-state
reauthenticate dot1x
restart dot1x
dump protocols 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>
| vlan {<vlan id list> | dynamic} }]
```

Input mode

User mode and administrator mode

Parameters

{ port <port list> | channel-group-number <channel group list> | vlan {<vlan id list> | dynamic} }

port <port list>

Displays statistics for port-based authentication for the physical ports specified in list format. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Displays statistics for port-based authentication for the channel groups specified in list format. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

vlan <vlan id list>

Displays statistics for VLAN-based authentication (static) of the specified VLANs in list format.

For details about how to specify <vlan id list>, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

vlan dynamic

Displays statistics for VLAN-based authentication (dynamic).

Operation when this parameter is omitted:

Statistics for all the above types are displayed.

Example

Figure 5-1: Displaying the statistics for each port that uses IEEE 802.1X port-based authentication

```
> show dot1x statistics port 1/10
Date 2006/03/23 12:32:00 UTC
[EAPOL frames]
Port 1/10 TxTotal      :      30 TxReq/Id   :      10 TxReq      :      10
          TxSuccess    :      10 TxFailure  :      0 TxNotify   :      0
          RxTotal      :      20 RxStart    :      0 RxLogoff   :      0
          RxResp/Id    :      10 RxResp     :      10 RxNotify   :      0
          RxInvalid    :      0 RxLenErr   :      0

[EAPoverRADIUS frames]
Port 1/10 TxTotal      :      10 TxNakResp  :      0 TxNoNakRsp:      10
          RxTotal      :      30 RxAccAccpt:      10 RxAccRejct:      10
          RxAccChllg    :      10 RxInvalid  :      0

>
```

Figure 5-2: Displaying statistics for each channel group that uses IEEE 802.1X port-based authentication

```

> show dot1x statistics channel-group-number 11
Date 2006/03/23 12:32:00 UTC
[EAPOL frames]
ChGr 11 TxTotal : 30 TxReq/Id : 10 TxReq : 10
      TxSuccess : 10 TxFailure : 0 TxNotify : 0
      RxTotal : 20 RxStart : 0 RxLogoff : 0
      RxResp/Id : 10 RxResp : 10 RxNotify : 0
      RxInvalid : 0 RxLenErr : 0

[EAPoverRADIUS frames]
ChGr 11 TxTotal : 10 TxNakResp : 0 TxNoNakRsp: 10
      RxTotal : 30 RxAccAcpt: 10 RxAccRejct: 10
      RxAccChllg: 10 RxInvalid : 0
>

```

Figure 5-3: Displaying statistics about each VLAN for IEEE 802.1X VLAN-based authentication (static)

```

> show dot1x statistics vlan 20
Date 2006/03/23 12:32:00 UTC
[EAPOL frames]
VLAN 20 TxTotal : 30 TxReq/Id : 10 TxReq : 10
      TxSuccess : 10 TxFailure : 0 TxNotify : 0
      RxTotal : 20 RxStart : 0 RxLogoff : 0
      RxResp/Id : 10 RxResp : 10 RxNotify : 0
      RxInvalid : 0 RxLenErr : 0

[EAPoverRADIUS frames]
VLAN 20 TxTotal : 10 TxNakResp : 0 TxNoNakRsp: 10
      RxTotal : 30 RxAccAcpt: 10 RxAccRejct: 10
      RxAccChllg: 10 RxInvalid : 0
>

```

Figure 5-4: Displaying statistics for IEEE 802.1X VLAN-based authentication (dynamic)

```

> show dot1x statistics vlan dynamic
Date 2006/03/23 12:32:00 UTC
[EAPOL frames]
VLAN TxTotal : 30 TxReq/Id : 10 TxReq : 10
(Dynamic) TxSuccess : 10 TxFailure : 0 TxNotify : 0
      RxTotal : 20 RxStart : 0 RxLogoff : 0
      RxResp/Id : 10 RxResp : 10 RxNotify : 0
      RxInvalid : 0 RxLenErr : 0

[EAPoverRADIUS frames]
VLAN TxTotal : 10 TxNakResp : 0 TxNoNakRsp: 10
(Dynamic) RxTotal : 30 RxAccAcpt: 10 RxAccRejct: 10
      RxAccChllg: 10 RxInvalid : 0
>

```

Figure 5-5: Displaying statistics for all types of IEEE 802.1X authentication (port-based authentication and VLAN-based authentication)

```

> show dot1x statistics
Date 2006/03/23 12:32:00 UTC
[EAPOL frames]
Port 1/10 TxTotal : 30 TxReq/Id : 10 TxReq : 10
      TxSuccess : 10 TxFailure : 0 TxNotify : 0
      RxTotal : 20 RxStart : 0 RxLogoff : 0
      RxResp/Id : 10 RxResp : 10 RxNotify : 0
      RxInvalid : 0 RxLenErr : 0

ChGr 11 TxTotal : 30 TxReq/Id : 10 TxReq : 10
      TxSuccess : 10 TxFailure : 0 TxNotify : 0
      RxTotal : 20 RxStart : 0 RxLogoff : 0
      RxResp/Id : 10 RxResp : 10 RxNotify : 0
      RxInvalid : 0 RxLenErr : 0

VLAN 20 TxTotal : 30 TxReq/Id : 10 TxReq : 10
      TxSuccess : 10 TxFailure : 0 TxNotify : 0
      RxTotal : 20 RxStart : 0 RxLogoff : 0

```

```

RxResp/Id :      10 RxResp      :      10 RxNotify :      0
RxInvalid :      0 RxLenErr :      0
VLAN TxTotal :      30 TxReq/Id :      10 TxReq :      10
(Dynamic) TxSuccess :      10 TxFailure :      0 TxNotify :      0
RxTotal :      20 RxStart :      0 RxLogoff :      0
RxResp/Id :      10 RxResp :      10 RxNotify :      0
RxInvalid :      0 RxLenErr :      0

[EAPoverRADIUS frames]
Port 1/10 TxTotal :      10 TxNakResp :      0 TxNoNakResp :      10
RxTotal :      30 RxAccAccpt :      10 RxAccRejct :      10
RxAccChllg :      10 RxInvalid :      0
ChGr 11 TxTotal :      10 TxNakResp :      0 TxNoNakResp :      10
RxTotal :      30 RxAccAccpt :      10 RxAccRejct :      10
RxAccChllg :      10 RxInvalid :      0
VLAN 20 TxTotal :      10 TxNakResp :      0 TxNoNakResp :      10
RxTotal :      30 RxAccAccpt :      10 RxAccRejct :      10
RxAccChllg :      10 RxInvalid :      0
VLAN TxTotal :      10 TxNakResp :      0 TxNoNakResp :      10
(Dynamic) RxTotal :      30 RxAccAccpt :      10 RxAccRejct :      10
RxAccChllg :      10 RxInvalid :      0
>

```

Display items

Table 5-1: Items displayed for statistics about IEEE 802.1X authentication

Item	Meaning	Displayed information
Port/ChGr/VLAN/VLAN(Dynamic)	Indicates the type of authentication. Port <nif no.> / <port no.>: Indicates a port for port-based authentication. ChGr <channel group number>: Indicates the channel group for port-based authentication. VLAN <vlan id>: Indicates a VLAN ID for VLAN-based authentication (static). VLAN (Dynamic): Indicates VLAN-based authentication (dynamic).	
[EAPOL frames]	Statistics for EAPOL frames. For details about the items, see the 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	
RxStart	The number of EAPOL Start frames that have been received	
RxLogoff	The number of EAPOL Logoff frames that have been received	
RxResp/Id	The number of EAP Response/Identity frames that have been received	
RxResp	The number of EAP Response frames (excluding Identity and Notification frames) that have been received	
RxNotify	The number of EAP Response/Notification frames that have been received	
RxInvalid	The number of invalid EAPOL frames that have been received (the number of discarded frames)	

Item	Meaning	Displayed information
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	
RxAccAcpt	The number of AccessAccept/EAP Success frames that have been received	
RxAccRejct	The number of AccessReject/EAP Failure frames that have been received	
RxAccChllg	The number of AccessChallenge frames that have been received	
RxInvalid	The number of invalid EAPoverRADIUS frames that have been received	

Impact on communication

None

Response messages

Table 5-2: List of response messages for the show dot1x statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Receive Error)	An attempt to receive data from the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Send Error)	An attempt to send data to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Dot1x doesn't seem to be running.	The IEEE 802.1X setting has not been enabled. Check the configuration.
No operational Channel Group.	There are no available channel groups. Check the authentication mode set by the configuration.
No operational Port.	There are no available ports. Check the authentication mode set by the configuration.
No operational VLAN(Dynamic).	VLAN-based authentication (dynamic) was not configured. Check the authentication mode set by the configuration.
No operational VLAN.	There are no available VLANs. Check the authentication mode set by the configuration.

5. IEEE802.1X

Message	Description
Now another user is using dot1x command, please try again.	Another user is using the <code>dot1x</code> command. Wait a while, and then retry the operation.

Notes

None

show dot1x

Displays status information about IEEE 802.1X authentication.

Syntax

```
show dot1x [{ port <port list> | channel-group-number <channel group list> | vlan
{<vlan id list> | dynamic [<vlan id list>]} } ] [detail]
```

Input mode

User mode and administrator mode

Parameters

```
{ port <port list> | channel-group-number <channel group list> | vlan {<vlan id list> | dynamic
[<vlan id list>]} }
```

port <port list>

Displays status information about port-based authentication for the physical ports specified in list format. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Displays status information about port-based authentication for the channel groups specified in list format. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

vlan <vlan id list>

Displays status information about VLAN-based authentication (static) for VLANs specified in list format.

For details about how to specify <vlan id list>, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

vlan dynamic <vlan id list>

Displays status information about VLAN-based authentication (dynamic).

For details about how to specify <vlan id list>, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

If <vlan id list> is omitted, status information about VLAN-based authentication (dynamic) for all VLANs is displayed.

detail

Displays detailed information. The status information about each supplicant (user) that has already been authenticated is displayed.

Operation when all parameters are omitted:

The status information for the entire switch is displayed.

Example

Figure 5-6: Displaying the status information for the IEEE 802.1X switch

```
> show dot1x
Date 2006/03/23 12:32:00 UTC
System 802.1X : Enable
  AAA Authentication Dot1x      : Enable
  Authorization Network         : Enable
  Accounting Dot1x              : Enable
```

Port/ChGr/VLAN	AccessControl	PortControl	Status	Supplicants
Port 1/1	---	Auto	Authorized	1
Port 1/10	Multiple-Auth	Auto	---	1
ChGr 11	Multiple-Auth	Auto	---	1
VLAN 20	Multiple-Auth	Auto	---	1
VLAN(Dynamic)	Multiple-Auth	Auto	---	1

Figure 5-7: Displaying the status information for each port that uses IEEE 802.1X port-based authentication (no display type is specified)

```
> show dot1x port 1/1
Date 2006/03/23 12:32:00 UTC
Port 1/1
AccessControl : ---
Status        : Authorized
Supplicants   : 1 / 1
TxTimer(s)    : --- / 30
ReAuthSuccess : 4
KeepUnauth(s) : --- / 3600
PortControl   : Auto
Last EAPOL    : 0012.e200.0021
ReAuthMode    : Enable
ReAuthTimer(s): 123 / 300
ReAuthFail    : 0
```

Figure 5-8: Displaying the status information for each port that uses IEEE 802.1X port-based authentication (detail display)

```
> show dot1x port 1/1 detail
Date 2006/03/23 17:57:03 UTC
Port 1/1
AccessControl : ---
Status        : Authorized
Supplicants   : 1 / 1
TxTimer(s)    : --- / 30
ReAuthSuccess : 4
KeepUnauth(s) : --- / 3600
PortControl   : Auto
Last EAPOL    : 0012.e200.0021
ReAuthMode    : Enable
ReAuthTimer(s): 123 / 300
ReAuthFail    : 0

Supplicants MAC      Status      AuthState      BackEndState      ReAuthSuccess
                  SessionTime(s) Date/Time
0012.e200.0021      Authorized  Authenticated  Idle               0
                  177                2006/03/23 17:55:00
```

Figure 5-9: Displaying the status information for each channel group that uses IEEE 802.1X port-based authentication (no display type is specified)

```
> show dot1x channel-group-number 11
Date 2008/12/17 12:32:00 UTC
ChGr 11
AccessControl : Multiple-Auth
Status        : ---
Supplicants   : 2 / 2 / 256
TxTimer(s)    : 15 / 30
ReAuthSuccess : 4
SuppDetection : Shortcut
PortControl   : Auto
Last EAPOL    : 0012.e200.0011
ReAuthMode    : Enable
ReAuthTimer(s): 123 / 300
ReAuthFail    : 0
```

Figure 5-10: Displaying the status information about each channel group for the IEEE 802.1X port-based authentication (detail display)

```
> show dot1x channel-group-number 11 detail
Date 2008/12/17 17:57:03 UTC
ChGr 11
AccessControl : Multiple-Auth
Status        : ---
Supplicants   : 2 / 2 / 256
TxTimer(s)    : 15 / 30
ReAuthSuccess : 4
SuppDetection : Shortcut
PortControl   : Auto
Last EAPOL    : 0012.e200.0011
ReAuthMode    : Enable
ReAuthTimer(s): 123 / 300
ReAuthFail    : 0

Supplicants MAC      Status      AuthState      BackEndState      ReAuthSuccess
```

```

                SessionTime(s) Date/Time
0012.e200.0011  Authorized      Authenticated Idle      0
                177            2008/12/17 17:55:00
0012.e200.0012  Authorized      Authenticated Idle      0
                5              2008/12/17 17:56:58
>

```

Figure 5-11: Displaying the status information about each VLAN for IEEE 802.1X VLAN-based authentication (static) (no display type is specified)

```

> show dot1x vlan 20
Date 2008/12/17 12:32:00 UTC
VLAN 20
AccessControl : Multiple-Auth          PortControl : Auto
Status        : ---                   Last EAPOL   : 0012.e200.0003
Supplicants   : 2 / 2 / 256           ReAuthMode   : Enable
TxTimer(s)    : --- / 30              ReAuthTimer(s): 123 / 300
ReAuthSuccess : 4                     ReAuthFail   : 0
SuppDetection : Disable
Port(s): 1/1-10, ChGr 1-5
Force-Authorized Port(s): 1/4,8-10, ChGr 1-5
>

```

Figure 5-12: Displaying status information about VLAN for IEEE 802.1X VLAN-based authentication (static) (details display)

```

> show dot1x vlan 20 detail
Date 2008/12/17 17:57:03 UTC
VLAN 20
AccessControl : Multiple-Auth          PortControl : Auto
Status        : ---                   Last EAPOL   : 0012.e200.0003
Supplicants   : 2 / 2 / 256           ReAuthMode   : Enable
TxTimer(s)    : --- / 30              ReAuthTimer(s): 123 / 300
ReAuthSuccess : 4                     ReAuthFail   : 0
SuppDetection : Disable
Port(s): 1/1-10, ChGr 1-5
Force-Authorized Port(s): 1/4,8-10, ChGr 1-5

Supplicants MAC      Status      AuthState      BackEndState      ReAuthSuccess
                SessionTime(s) Date/Time
[Port 1/1]
0012.e200.0003      Authorized      Authenticated Idle      0
                177            2008/12/17 17:55:00
0012.e200.0004      Authorized      Authenticated Idle      0
                5              2008/12/17 17:56:58
>

```

Figure 5-13: Displaying status information about IEEE 802.1X VLAN-based authentication (dynamic) (no display type is specified)

```

> show dot1x vlan dynamic
Date 2008/12/17 12:32:00 UTC
VLAN(Dynamic)
AccessControl : Multiple-Auth          PortControl : Auto
Status        : ---                   Last EAPOL   : 0012.e200.0005
Supplicants   : 2 / 2 / 1024          ReAuthMode   : Enable
TxTimer(s)    : --- / 30              ReAuthTimer(s): 123 / 300
ReAuthSuccess : 4                     ReAuthFail   : 0
SuppDetection : Disable
VLAN(s): 2-5

VLAN(Dynamic) Supplicants
VLAN 2      2          VLAN 3      0          VLAN 4      0          VLAN 5      0
>

```

Figure 5-14: Displaying status information about IEEE 802.1X VLAN-based authentication (dynamic) (detail display)

```

> show dot1x vlan dynamic detail

```

```

Date 2008/12/17 17:57:03 UTC
VLAN(Dynamic)
AccessControl : Multiple-Auth
Status        : ---
Supplicants   : 2 / 2 / 1024
TxTimer(s)    : --- / 30
ReAuthSuccess : 4
SuppDetection : Disable
VLAN(s): 2-5

PortControl    : Auto
Last EAPOL     : 0012.e200.0005
ReAuthMode     : Enable
ReAuthTimer(s) : 123 / 300
ReAuthFail     : 0

Supplicants MAC      Status      AuthState      BackEndState  ReAuthSuccess
                   SessionTime(s) Date/Time
[VLAN 2]
0012.e200.0005      Authorized  Authenticated  Idle          0
                   177
                   2008/12/17 17:55:00
0012.e200.0006      Authorized  Authenticated  Idle          0
                   5
                   2008/12/17 17:56:58
>

```

Figure 5-15: Displaying status information about each VLAN for IEEE 802.1X
VLAN-based authentication (dynamic) (no display type is specified)

```

> show dot1x vlan dynamic 2
Date 2008/12/17 12:32:00 UTC
VLAN(Dynamic)
AccessControl : Multiple-Auth
Status        : ---
Supplicants   : 2 / 2 / 1024
TxTimer(s)    : --- / 30
ReAuthSuccess : 4
SuppDetection : Disable
VLAN(s): 2-5

PortControl    : Auto
Last EAPOL     : 0012.e200.0005
ReAuthMode     : Enable
ReAuthTimer(s) : 123 / 300
ReAuthFail     : 0

VLAN(Dynamic) Supplicants
VLAN 2         2
>

```

Figure 5-16: Displaying status information about each VLAN for IEEE 802.1X
VLAN-based authentication (dynamic) (detail display)

```

> show dot1x vlan dynamic 2 detail
Date 2008/12/17 17:57:03 UTC
VLAN(Dynamic)
AccessControl : Multiple-Auth
Status        : ---
Supplicants   : 2 / 2 / 1024
TxTimer(s)    : --- / 30
ReAuthSuccess : 4
SuppDetection : Disable
VLAN(s): 2-5

PortControl    : Auto
Last EAPOL     : 0012.e200.0005
ReAuthMode     : Enable
ReAuthTimer(s) : 123 / 300
ReAuthFail     : 0

Supplicants MAC      Status      AuthState      BackEndState  ReAuthSuccess
                   SessionTime(s) Date/Time
[VLAN 2]
0012.e200.0005      Authorized  Authenticated  Idle          0
                   177
                   2008/12/17 17:55:00
0012.e200.0006      Authorized  Authenticated  Idle          0
                   5
                   2008/12/17 17:56:58
>

```

Figure 5-17: Displaying the status information for all types of IEEE 802.1X authentication

```

> show dot1x detail
Date 2008/12/17 17:57:03 UTC
System 802.1X : Enable
  AAA Authentication Dot1x : Enable
  Authorization Network    : Enable
  Accounting Dot1x         : Enable

```

```

Port 1/1
AccessControl : ---
Status        : Authorized
Supplicants   : 1 / 1
TxTimer(s)    : --- / 30
ReAuthSuccess : 4
KeepUnauth(s) : --- / 3600

PortControl    : Auto
Last EAPOL     : 0012.e200.0021
ReAuthMode     : Enable
ReAuthTimer(s) : 123 / 300
ReAuthFail     : 0

Supplicants MAC    Status      AuthState      BackEndState  ReAuthSuccess
                  SessionTime(s) Date/Time
0012.e200.0021     Authorized  Authenticated  Idle          0
                  177
                  2008/12/17 17:55:00

Port 1/2
AccessControl : Multiple-Auth
Status        : ---
Supplicants   : 2 / 2 / 256
TxTimer(s)    : 15 / 30
ReAuthSuccess : 4
SuppDetection : Shortcut

PortControl    : Auto
Last EAPOL     : 0012.e200.0001
ReAuthMode     : Enable
ReAuthTimer(s) : 123 / 300
ReAuthFail     : 0

Supplicants MAC    Status      AuthState      BackEndState  ReAuthSuccess
                  SessionTime(s) Date/Time
0012.e200.0001     Authorized  Authenticated  Idle          0
                  177
                  2008/12/17 17:55:00
0012.e200.0002     Authorized  Authenticated  Idle          0
                  5
                  2008/12/17 17:56:58

ChGr 11
AccessControl : Multiple-Auth
Status        : ---
Supplicants   : 2 / 2 / 256
TxTimer(s)    : 15 / 30
ReAuthSuccess : 4
SuppDetection : Shortcut

PortControl    : Auto
Last EAPOL     : 0012.e200.0011
ReAuthMode     : Enable
ReAuthTimer(s) : 123 / 300
ReAuthFail     : 0

Supplicants MAC    Status      AuthState      BackEndState  ReAuthSuccess
                  SessionTime(s) Date/Time
0012.e200.0011     Authorized  Authenticated  Idle          0
                  177
                  2008/12/17 17:55:00
0012.e200.0012     Authorized  Authenticated  Idle          0
                  5
                  2008/12/17 17:56:58

VLAN 20
AccessControl : Multiple-Auth
Status        : ---
Supplicants   : 2 / 2 / 256
TxTimer(s)    : --- / 30
ReAuthSuccess : 4
SuppDetection : Disable
Port(s): 1/3-15, ChGr 1-5
Force-Authorized Port(s): 1/4,8-15, ChGr 1-5

Supplicants MAC    Status      AuthState      BackEndState  ReAuthSuccess
                  SessionTime(s) Date/Time
[Port 1/3]
0012.e200.0003     Authorized  Authenticated  Idle          0
                  177
                  2008/12/17 17:55:00
0012.e200.0004     Authorized  Authenticated  Idle          0
                  5
                  2008/12/17 17:56:58

VLAN(Dynamic)
AccessControl : Multiple-Auth
Status        : ---
Supplicants   : 2 / 2 / 1024
TxTimer(s)    : --- / 30
ReAuthSuccess : 4

PortControl    : Auto
Last EAPOL     : 0012.e200.0005
ReAuthMode     : Enable
ReAuthTimer(s) : 123 / 300
ReAuthFail     : 0

```

```
SuppDetection : Disable
VLAN(s) : 2-5
```

Supplicants MAC	Status	AuthState	BackEndState	ReAuthSuccess
[VLAN 2]	SessionTime(s)	Date/Time		
0012.e200.0005	VLAN(Dynamic)	Supplicants : 2		
	Authorized	Authenticated	Idle	0
	177	2008/12/17 17:55:00		
0012.e200.0006	Authorized	Authenticated	Idle	0
	5	2008/12/17 17:56:58		

>

Display items

Table 5-3: Display items for the status information about IEEE 802.1X authentication

Item		Meaning	Displayed information
System 802.1X		Displays the operating status of IEEE 802.1X authentication.	<ol style="list-style-type: none"> 1. Enable (IEEE 802.1X authentication is operating.) 2. Disable (IEEE 802.1X authentication stops.)
AAA	Authentication Dot1x	Displays the operating status of authentication requests to RADIUS.	<ol style="list-style-type: none"> 1. Enable (Authentication request to RADIUS is enabled.) 2. Disable (Authentication request to RADIUS is disabled.)
	Authorization Network	Displays the operating status of VLAN allocation from RADIUS when VLAN-based authentication (dynamic) is used.	<ol style="list-style-type: none"> 1. Enable (VLAN allocation from RADIUS is enabled.) 2. Disable (VLAN allocation from RADIUS is disabled.)
	Accounting Dot1x	Displays the operating status of the accounting functionality.	<ol style="list-style-type: none"> 1. Enable (The accounting functionality is enabled.) 2. Disable (The accounting functionality is disabled.)
Port/ChGr/VLAN/ VLAN(Dynamic)		Indicates the type of authentication. Port <nif no.> / <port no.>: Indicates a port for port-based authentication ChGr<channel group number>: Indicates a channel group for port-based authentication VLAN <vlan id>: Indicates a VLAN ID for VLAN-based authentication (static). VLAN (Dynamic): Indicates VLAN-based authentication (dynamic).	
AccessControl		Displays the authentication submode set for the relevant type of authentication. ----: Indicates single mode. Multiple-Hosts: Indicates multi mode. Multiple-Auth: Indicates terminal authentication mode.	<ol style="list-style-type: none"> 1. --- 2. Multiple-Hosts 3. Multiple-Auth

Item	Meaning	Displayed information
PortControl	Displays the authentication control setting. Auto: Authentication control is applied. Force-Authorized: Communication is always authorized. Force-Unauthorized: Communication is never authorized.	1. Auto 2. Force-Authorized 3. Force-Unauthorized
Status	Displays the authentication status of the port. Authorized: Already authenticated. Unauthorized: Not authenticated. ---: Terminal authentication mode	1. Authorized 2. Unauthorized 3. ---
Last EAPOL	Displays the source MAC address of the last received EAPOL.	
Supplicants	Displays the number of supplicants that have already been authenticated or assigned for authentication. [For the entire Switch] The number of supplicants to be authenticated is displayed. [For each type of authentication] For single mode or multi mode: <i><number of authenticated supplicants> / <number of supplicants to be authenticated></i> For terminal authentication mode: <i><number of authenticated supplicants> / <number of supplicants to be authenticated> / <maximum number of supplicants within an authentication type></i>	
ReAuthMode	Displays the status of the self-issuance of EAPOL Request/ID re-authentication requests.	1. Enable 2. Disable
TxTimer(s)	Displays the timer for sending EAPOL Request/ID authentication requests prior to authentication. ---: The timer on a Switch is disabled because any of the following applies: - The number of supplicants to be authenticated reached the maximum value for the authentication type. - A supplicant was authenticated even though new terminal detection mode was disabled. - The following authentication types are disabled: Port-based authentication: For port or a channel group to be authenticated VLAN-based authentication (static or dynamic): For VLAN to be authenticated <i><current timer value> / <tx_period seconds></i>	
ReAuthTimer(s)	Displays the timer for sending EAPOL Request/ID re-authentication requests after a successful authentication. ---: The timer is disabled because authentication has not been successful. <i><current timer value> / <reauth_period seconds></i>	
ReAuthSuccess	The number of times that re-authentication has been successful	
ReAuthFail	The number of times that re-authentication has failed	

Item	Meaning	Displayed information
KeepUnauth	<p>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.</p> <p>---: The timer is disabled because the operation is normal.</p> <p><current timer value> / <keepunauth_period seconds></p>	
SuppDetection	<p>(For terminal authentication mode only)</p> <p>This item displays the mode for detecting a new terminal.</p> <p>Disable: The detection operation is stopped.</p> <p>Shortcut: Omission mode</p>	<ol style="list-style-type: none"> 1. Disable 2. Shortcut
Port(s)	(For VLAN-based authentication (static) only) This item displays the list for ports belonging to the VLAN to be authenticated.	
Force-Authorized Port(s)	(For VLAN-based authentication (static) only) This item displays the list of ports excluded from authentication.	
VLAN(s)	(For VLAN-based authentication (dynamic) only) This item displays the list of VLANs to be authenticated.	
VLAN(Dynamic) Supplicants	(For VLAN-based authentication (dynamic) only) This item displays the number of supplicants already authenticated.	
Supplicant MAC	The supplicant's MAC address.	
Status	<p>Displays the authentication status of the supplicants.</p> <p>Authorized: Already authenticated.</p> <p>Unauthorized: Not authenticated.</p>	<ol style="list-style-type: none"> 1. Authorized 2. Unauthorized
AuthState	<p>Displays the status of authentication processing for the supplicant.</p> <p>Connecting: The supplicant is connecting.</p> <p>Authenticating: Authentication is in progress.</p> <p>Authenticated: Authentication has been completed.</p> <p>Aborting: Authentication processing has stopped.</p> <p>Held: The authentication request has been rejected.</p>	<ol style="list-style-type: none"> 1. Connecting 2. Authenticating 3. Authenticated 4. Aborting 5. Held
BackEndState	<p>Displays the status of authentication processing for the supplicant by the RADIUS server.</p> <p>Idle: The supplicant is waiting for processing.</p> <p>Response: The supplicant is responding to the server.</p> <p>Request: A request is being sent to the supplicant.</p> <p>Success: Authentication processing has finished successfully.</p> <p>Fail: The authentication processing failed.</p> <p>Timeout: A timeout occurred during an attempt to connect to the server.</p>	<ol style="list-style-type: none"> 1. Idle 2. Response 3. Request 4. Success 5. Fail 6. Timeout

Item	Meaning	Displayed information
ReAuthSuccess	Displays the number of times re-authentication was successful.	
SessionTime	Displays the time (in seconds for each supplicant) required to establish a session after a successful authentication.	
Date/Time	Displays the time that authentication of the supplicant was successful.	

Impact on communication

None

Response messages

Table 5-4: List of response messages for the show dot1x command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Receive Error)	An attempt to receive data from the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Send Error)	An attempt to send data to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Dot1x doesn't seem to be running.	The IEEE 802.1X setting has not been enabled. Check the configuration.
No operational Channel Group.	There are no available channel groups. Check the authentication mode set by the configuration.
No operational Port.	There are no available ports. Check the authentication mode set by the configuration.
No operational VLAN(Dynamic).	VLAN-based authentication (dynamic) was not configured. Check the authentication mode set by the configuration.
No operational VLAN.	There are no available VLANs. Check the authentication mode set by the configuration.
Now another user is using dot1x command, please try again.	Another user is using the <code>dot1x</code> command. Wait a while, and then retry the operation.

Notes

Information about the supplicants for which VLAN dynamic assignment failed in VLAN-based authentication (dynamic) is not displayed. Execute the `show dot1x logging` and `show vlan mac-vlan` commands to make sure the information is not displayed.

clear dot1x statistics

Clears the IEEE 802.1X authentication statistics.

Syntax

```
clear dot1x statistics [{ port <port list> | channel-group-number <channel group list> | vlan {<vlan id list> | dynamic} }]
```

Input mode

User mode and administrator mode

Parameters

{ port <port list> | channel-group-number <channel group list> | vlan {<vlan id list> | dynamic} }

port <port list>

Clears statistics for port-based authentication of the specified physical port in list format. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Clears statistics for port-based authentication of the specified channel group in list format. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

vlan <vlan id list>

Clears statistics for VLAN-based authentication (static) of the specified VLAN in list format.

For details about how to specify <vlan id list>, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

vlan dynamic

Clears statistics for VLAN-based authentication (dynamic).

Operation when this parameter is omitted:

Clears statistics for all types of authentication.

Example

Figure 5-18: Clearing IEEE 802.1X authentication statistics

```
> clear dot1x statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 5-5: List of response messages for the clear dot1x statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Receive Error)	An attempt to receive data from the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Send Error)	An attempt to send data to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Dot1x doesn't seem to be running.	The IEEE 802.1X setting has not been enabled. Check the configuration.
No operational Channel Group.	There are no available channel groups. Check the authentication mode set by the configuration.
No operational Port.	There are no available ports. Check the authentication mode set by the configuration.
No operational VLAN(Dynamic).	VLAN-based authentication (dynamic) was not configured. Check the authentication mode set by the configuration.
No operational VLAN.	There are no available VLANs. Check the authentication mode set by the configuration.
Now another user is using dot1x command, please try again.	Another user is using the <code>dot1x</code> command. Wait a while, and then retry the operation.

Notes

If this command is executed, MIB information of the IEEE 802.1X MIB group is also cleared.

clear dot1x auth-state

Initializes the IEEE 802.1X authentication status.

Syntax

```
clear dot1x auth-state [{ port <port list> | channel-group-number <channel group list> | vlan {<vlan id list> | dynamic [<vlan id list>]} | supplicant-mac <mac address>}] [-f]
```

Input mode

User mode and administrator mode

Parameters

```
{ port <port list> | channel-group-number <channel group list> | vlan {<vlan id list> | dynamic [<vlan id list>]} | supplicant-mac <mac address> }
```

port <port list>

Initializes the authentication status for the ports specified in list format for port-based authentication. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Initializes the authentication status for the channel groups specified in list format for port-based authentication. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

vlan <vlan id list>

Initializes the authentication status of the VLANs specified in list format for VLAN-based authentication (static).

For details about how to specify <vlan id list>, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

vlan dynamic <vlan id list>

Initializes the authentication status of the VLANs specified in list format for VLAN-based authentication (dynamic).

For details about how to specify <vlan id list>, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

If <vlan id list> is omitted, the authentication status of all VLANs in VLAN-based authentication (dynamic) is initialized.

supplicant-mac <mac address>

Initializes the authentication status for the specified MAC address.

-f

Initializes the authentication status without displaying a confirmation message.

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 5-19: Initializing all IEEE 802.1X authentication statuses on a Switch

```
> clear dot1x auth-state
Initialize all 802.1X Authentication Information. Are you sure? (y/n) :y
>
```

Display items

None

Impact on communication

If initialization is performed, the IEEE 802.1X authentication status on the relevant ports or VLANs is initialized, and communication is lost. To restore communication, re-authentication is necessary.

Response messages

Table 5-6: List of response messages for the clear dot1x auth-state command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Receive Error)	An attempt to receive data from the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Send Error)	An attempt to send data to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Dot1x doesn't seem to be running.	The IEEE 802.1X setting has not been enabled. Check the configuration.
No operational Channel Group.	There are no available channel groups. Check the authentication mode set by the configuration.
No operational Port.	There are no available ports. Check the authentication mode set by the configuration.
No operational VLAN(Dynamic).	VLAN-based authentication (dynamic) was not configured. Check the authentication mode set by the configuration.
No operational VLAN.	There are no available VLANs. Check the authentication mode set by the configuration.
Now another user is using dot1x command, please try again.	Another user is using the <code>dot1x</code> command. Wait a while, and then retry the operation.

Notes

When authentication status is initialized, EAP-Failure or EAP-Req/Id might be sent according to the specified parameter.

- If the parameter is omitted, EAP-Failure and EAP-Req/Id are multicasted once to all types of IEEE 802.1X authentication in a Switch.
- If the parameter is `port <port list>`, `channel-group-number <channel group list>`, `vlan <vlan id list>`, or `vlan dynamic`, EAP-Failure and EAP-Req/Id are multicasted once to the specified type of IEEE 802.1X authentication.

- If the parameter is `vlan dynamic <vlan id list>` and there is an authentication terminal, EAP-Failure is unicasted once to the authentication terminal, and EAP-Req/Id is multicasted once to the specified type of IEEE 802.1X authentication.
- If the parameter is `supplicant-mac <mac address>`, EAP-Failure is unicasted to the specified authentication terminal. If there is no authentication terminal under the IEEE 802.1X authentication to which the specified authentication terminal belongs, EAP-Req/Id is multicasted once to the type of IEEE 802.1X authentication to which the specified authentication terminal belongs.

reauthenticate dot1x

Re-authenticates the status of IEEE 802.1X authentication. Even if re-authentication timer (reauth-period) is 0 (disabled), re-authentication is forcibly performed.

Syntax

```
reauthenticate dot1x [{ port <port list> | channel-group-number <channel group list>
| vlan {<vlan id list> | dynamic [<vlan id list>]} | supplicant-mac <mac address> }]
[-f]
```

Input mode

User mode and administrator mode

Parameters

```
{ port <port list> | channel-group-number <channel group list> | vlan {<vlan id list> | dynamic
[<vlan id list>]} | supplicant-mac <mac address> }
```

port <port list>

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*.

vlan <vlan id list>

Re-authenticates the authentication status of the VLANs specified in list format for VLAN-based authentication (static).

For details about how to specify <vlan id list>, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

vlan dynamic <vlan id list>

Re-authenticates the authentication status of the VLANs specified in list format for VLAN-based authentication (dynamic).

For details about how to specify <vlan id list>, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

If <vlan id list> is omitted, re-authentication for all VLANs for VLAN-based authentication (dynamic) is initiated.

supplicant-mac <mac address>

Re-authenticates the authentication status of the specified MAC address.

-f

Initiates re-authentication without displaying a confirmation message.

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 5-20: Re-authentication for all IEEE 802.1X-authenticated ports and VLANs on a Switch

```
> reauthenticate dot1x
Reauthenticate all 802.1X ports and vlans. Are you sure? (y/n) :y
>
```

Display items

None

Impact on communication

When re-authentication is initiated, no problems with communication arise if re-authentication is successful. If re-authentication fails, however, communication will be lost.

Response messages

Table 5-7: List of response messages for the reauthenticate dot1x command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Receive Error)	An attempt to receive data from the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Send Error)	An attempt to send data to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Dot1x doesn't seem to be running.	The IEEE 802.1X setting has not been enabled. Check the configuration.
No operational Channel Group.	There are no available channel groups. Check the authentication mode set by the configuration.
No operational Port.	There are no available ports. Check the authentication mode set by the configuration.
No operational VLAN(Dynamic).	VLAN-based authentication (dynamic) was not configured. Check the authentication mode set by the configuration.
No operational VLAN.	There are no available VLANs. Check the authentication mode set by the configuration.
Now another user is using dot1x command, please try again.	Another user is using the <code>dot1x</code> command. Wait a while, and then retry the operation.

Notes

None

restart dot1x

Restarts the IEEE 802.1X program.

Syntax

```
restart dot1x [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the IEEE 802.1X program without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

core-file

When the IEEE 802.1X program is restarted, the core file of the program is output.

Operation when this parameter is omitted:

A core file is not output.

Operation when all parameters are omitted:

Restarts the IEEE 802.1X program after displaying a confirmation message.

Example

Figure 5-21: Restarting the IEEE 802.1X program

```
> restart dot1x
802.1X restart OK? (y/n) : y
>
```

Figure 5-22: Restarting IEEE 802.1X program (when the -f parameter is specified)

```
> restart dot1x -f
>
```

Display items

None

Impact on communication

All the IEEE 802.1X authentication statuses on a Switch are initialized and communication is lost.
To restore communication, re-authentication is necessary.

Response messages

Table 5-8: List of response messages for the restart dot1x command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Dot1x doesn't seem to be running.	The IEEE 802.1X setting has not been enabled. Check the configuration.
Now another user is using dot1x command, please try again.	Another user is using the dot1x command. Wait a while, and then retry the operation.

Notes

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

Storage directory: `/usr/var/core`

Core file: `dot1xd.core`

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

dump protocols dot1x

Outputs control table information and statistics collected by the IEEE 802.1X program to a file.

Syntax

```
dump protocols dot1x
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 5-23: Acquiring IEEE 802.1X program online dump

```
> dump protocols dot1x
>
```

Display items

None

Impact on communication

None

Response messages

Table 5-9: List of response messages for the dump protocols dot1x command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Receive Error)	An attempt to receive data from the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Send Error)	An attempt to send data to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Dot1x doesn't seem to be running.	The IEEE 802.1X setting has not been enabled. Check the configuration.
Now another user is using dot1x command, please try again.	Another user is using the <code>dot1x</code> command. Wait a while, and then retry the operation.

Notes

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

Storage directory: `/usr/var/dot1x`

Dump file: `dot1x_dump.gz`

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

show dot1x logging

Displays the operation log messages collected by the IEEE 802.1X program.

Syntax

```
show dot1x logging [{ error | warning | notice | info }]
```

Input mode

User mode and administrator mode

Parameters

{ error | warning | notice | info }

Specify the level of operation log message to be displayed. Of the output messages, only logs whose priority level is higher than the level specified by the `dot1x loglevel` configuration command are displayed.

Note, however, that if `notice` is specified, NORMAL level log messages are also displayed.

If `info` is specified, all log messages are displayed.

Operation when this parameter is omitted:

Displays the same operation log messages as those displayed when `info` is specified is displayed.

Example

Figure 5-24: Displaying IEEE 802.1X operation log messages

```
> show dot1x logging
Date 2009/01/23 13:32:00 UTC
No=1:Jan 23 13:31:43:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=1/1 VLAN=10 Login
succeeded. ; New Supplicant Auth Success.
No=16:Jan 23 13:16:55:NORMAL:LOGOUT: MAC=0012.e200.0001 PORT=1/1 VLAN=10 Force
Logout. ; Port link down.
No=2:Jan 23 13:16:10:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=1/1 VLAN=10 Login
succeeded. ; Supplicant Re-Auth Success.
No=1:Jan 23 13:15:10:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=1/1 VLAN=10 Login
succeeded. ; New Supplicant Auth Success.
No=30:Jan 23 13:10:34:NOTICE:LOGIN: MAC=0012.e200.0001 PORT=1/1 VLAN=10 Login
failed. ; RADIUS authentication failed.
```

Display items

The following table shows the items displayed when an IEEE 802.1X operation log message is displayed.

Table 5-10: Items displayed for IEEE 802.1X operation log messages

Item	Meaning	Displayed information
Level	Levels of operation log messages	Severity of a log message
<log>	Operation log message	Contents of a registered operation log message

The following shows the display format of a message.

```
No=10:Dec 1 10:09:50:NORMAL:LOGOUT: MAC=0012.e200.0001 PORT=1/1 VLAN=3 Logout succeeded.
(1) (2) (3) (4) (5) (6) (7)
```

(1) Message number: Indicates the number assigned to each message shown in *Table 5-13: List of operation log messages*.

- (2) Date: Indicates the date recorded in the IEEE 802.1X program.
- (3) Time: Indicates the time recorded in the IEEE 802.1X program.
- (4) Log ID: Indicates the level of the operation log message.
- (5) Log type: Indicates the type of operation that outputs the log message.
- (6) Additional information: Indicates supplementary information provided in the message.
- (7) Message body

Operation log messages show the following information:

- Log ID: See *Table 5-11: Log ID and type in operation log messages*.
- Log type: See *Table 5-11: Log ID and type in operation log messages*.
- Additional information: See *Table 5-12: Additional information*.
- List of messages: See *Table 5-13: List of operation log messages*.

Table 5-11: Log ID and type in operation log messages

Log ID	Log type	Meaning
NORMAL	LOGIN	Indicates that login was successful.
	LOGOUT	Indicates that logout was successful.
	SYSTEM	Indicates a runtime notification.
NOTICE	LOGIN	Indicates that authentication failed.
	LOGOUT	Indicates that logout failed.
WARNING	SYSTEM	Indicates a communication failure.
ERROR	SYSTEM	Indicates an operation failure of the IEEE 802.1X program.

Table 5-12: Additional information

Display format	Meaning
MAC=xxxx.xxxx.xxxx	Indicates the MAC address.
VLAN=xxxx	Indicates the VLAN ID. Note, however, that this is not displayed if VLAN ID information could not be acquired.
PORT=xx/xx CHGR=xx	Indicates the port number or channel group number. Note, however, that this information is not displayed if port information could not be acquired.
ServerIP=xxx.xxx.xxx.xxx	Indicates the server IP address.
ServerIPv6=xxxx:xxxx:xxxx	Indicates the server IPv6 address.
ServerName=ccccc	Indicates the server name.

Table 5-13: List of operation log messages

#	Log ID	Log type	Message text	Meaning and action	Additional information
1	NORMAL	LOGIN	Login succeeded. ; New Supplicant Auth Success.	[Meaning] A new supplicant was authenticated successfully. [Action] None	MAC address port number or channel group number VLAN ID

#	Log ID	Log type	Message text	Meaning and action	Additional information
2	NORMAL	LOGIN	Login succeeded. ; Supplicant Re-Auth Success.	[Meaning] A supplicant was re-authenticated successfully. [Action] None	MAC address port number or channel group number VLAN ID
10	NORMAL	LOGOUT	Logout succeeded.	[Meaning] Authentication has been canceled by a request from the supplicant or because the terminal was moved. [Action] None	MAC address port number or channel group number VLAN ID
11	NORMAL	LOGOUT	Force logout. ; "clear dot1x auth-state" command succeeded.	[Meaning] Authentication has been canceled by a command. [Action] None	MAC address port number or channel group number VLAN ID
12	NORMAL	LOGOUT	Force logout. ; The supplicant was cleared, because it was registered to MAC VLAN with the configuration.	[Meaning] An attempt to authenticate the relevant supplicant was canceled because the MAC address was configured for the MAC VLAN. [Action] None	MAC address port number or channel group number VLAN ID
13	NORMAL	LOGOUT	Force logout. ; The supplicant was cleared, because it was registered to mac-address-table with the configuration.	[Meaning] An attempt to authenticate the relevant supplicant was canceled because a MAC address was configured for mac-address-table. [Action] None	MAC address port number or channel group number VLAN ID
14	NORMAL	LOGOUT	Force logout. ; The status of port was changed to Unauthorized, because another supplicant was detected in single mode.	[Meaning] The authentication status has been changed to Unauthorized because multiple supplicants were detected on a single-mode port. [Action] None	MAC address port number or channel group number VLAN ID
15	NORMAL	LOGOUT	Force logout. ; Dot1x configuration deleted.	[Meaning] Authentication has been canceled because the IEEE 802.1X authentication configuration was deleted. [Action] If you want to use IEEE 802.1X authentication, set the configuration.	MAC address port number or channel group number VLAN ID
16	NORMAL	LOGOUT	Force logout. ; Port link down.	[Meaning] Authentication has been canceled because the port is in the link-down state. [Action] None	MAC address port number or channel group number VLAN ID

#	Log ID	Log type	Message text	Meaning and action	Additional information
17	NORMAL	LOGOUT	Force logout. ; VLAN status down.	[Meaning] Authentication has been canceled because the VLAN has gone down or the VLAN was deleted from the configuration of the port. [Action] None	MAC address port number or channel group number VLAN ID
18	NORMAL	LOGOUT	Force logout. ; Re-Auth failed.	[Meaning] Re-authentication processing failed. [Action] None	MAC address port number or channel group number VLAN ID
19	NORMAL	LOGOUT	Force logout. ; Could not be registered to hardware.	[Meaning] Authentication has been canceled because registration of a supplicant in the hardware failed. [Action] If this message appears frequently, use the <code>restart dot1x</code> command to restart the IEEE 802.1X program.	MAC address port number or channel group number VLAN ID
30	NOTICE	LOGIN	Login failed. ; RADIUS authentication failed.	[Meaning] Authentication of a new supplicant failed. [Action] Correctly set the user name and password sent from the supplicant and the user settings of the RADIUS server.	MAC address port number or channel group number VLAN ID
31	NOTICE	LOGIN	Login failed. ; RADIUS authentication failed. (Re-Auth)	[Meaning] Re-authentication of a supplicant failed. [Action] Correctly set the user name and password sent from the supplicant and the user settings of the RADIUS server.	MAC address port number or channel group number VLAN ID
32	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: "aaa authorization network default" is not configured.)	[Meaning] VLAN dynamic assignment failed because the <code>aaa authorization network default</code> configuration command was not configured [Action] Set the <code>aaa authorization network default</code> configuration command.	MAC address port number or channel group number
33	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: No Tunnel-Type Attribute.)	[Meaning] VLAN dynamic assignment failed because there was no Tunnel-Type attribute. [Action] Set the Tunnel-Type attribute in the Accept packet to be sent by the RADIUS server.	MAC address port number or channel group number

#	Log ID	Log type	Message text	Meaning and action	Additional information
34	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Tunnel-Type Attribute is not VLAN(13).)	[Meaning] VLAN dynamic assignment failed because the value of the Tunnel-Type attribute was not VLAN(13). [Action] Set the Tunnel-Type attribute in the Accept packet to be sent by the RADIUS server to VLAN(13).	MAC address port number or channel group number
35	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: No Tunnel-Medium-Type Attribute.)	[Meaning] VLAN dynamic assignment failed because there was no Tunnel-Medium-Type attribute. [Action] Set the Tunnel-Medium-Type attribute in the Accept packet to be sent by the RADIUS server.	MAC address port number or channel group number
36	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Tunnel-Medium-Type Attribute is not IEEE802(6).)	[Meaning] VLAN dynamic assignment failed because the value of the Tunnel-Medium-Type attribute was not IEEE 802(6). [Action] Set the Tunnel-Medium-Type attribute in the Accept packet to be sent by the RADIUS server to IEEE 802(6).	MAC address port number or channel group number
37	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: No Tunnel-Private-Group-ID Attribute.)	[Meaning] VLAN dynamic assignment failed because there was no Tunnel-Private-Group-ID attribute. [Action] Set the Tunnel-Private-Group-ID attribute in the Accept packet to be sent by the RADIUS server.	MAC address port number or channel group number
38	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Invalid Tunnel-Private-Group-ID Attribute.)	[Meaning] VLAN dynamic assignment failed because an invalid value was set for the Tunnel-Private-Group-ID attribute. [Action] Check the setting of the Tunnel-Private-Group-ID attribute in the Accept packet to be sent by the RADIUS server.	MAC address port number or channel group number
39	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The VLAN ID is out of range.)	[Meaning] VLAN dynamic assignment failed because the VLAN ID was not in the normal range. [Action] Check the range of the VLAN IDs set for the Tunnel-Private-Group-ID attribute in the Accept packet to be sent by the RADIUS server.	MAC address port number or channel group number VLAN ID

#	Log ID	Log type	Message text	Meaning and action	Additional information
40	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The Port doesn't belong to VLAN.)	<p>[Meaning] VLAN dynamic assignment failed because the authentication port did not belong to the VLAN ID.</p> <p>[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 <code>switchport mac</code> configuration command with the <code>vlan</code> parameter specified.</p>	MAC address port number or channel group number VLAN ID
41	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The VLAN ID is not set to radius-vlan.)	<p>[Meaning] VLAN dynamic assignment failed because the VLAN ID was not subject to VLAN-based authentication (dynamic).</p> <p>[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 by the <code>dot1x vlan dynamic radius-vlan</code> configuration command.</p>	MAC address port number or channel group number VLAN ID
42	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The VLAN status is disabled.)	<p>[Meaning] VLAN dynamic assignment failed because the VLAN is disabled for VLAN-based authentication (dynamic).</p> <p>[Action] Execute the <code>state</code> configuration command to set the status of the VLAN to be assigned to <code>active</code>.</p>	MAC address port number or channel group number VLAN ID
43	NOTICE	LOGIN	Login failed. ; The number of supplicants on the switch is full.	<p>[Meaning] Authentication was not available because there were too many supplicants for the Switch.</p> <p>[Action] Attempt authentication again when the total number of authenticated supplicants falls below the capacity limit.</p>	MAC address port number or channel group number VLAN ID
44	NOTICE	LOGIN	Login failed. ; The number of supplicants on the interface is full.	<p>[Meaning] Authentication was not available because there were too many supplicants on the interface.</p> <p>[Action] Attempt authentication again when the number of authenticated supplicants on the interface falls below the capacity limit.</p>	MAC address port number or channel group number VLAN ID

#	Log ID	Log type	Message text	Meaning and action	Additional information
45	NOTICE	LOGIN	Login failed. ; Failed to authenticate the supplicant because it could not be registered to mac-address-table.(code=x)	<p>[Meaning] Authentication failed because registration of a supplicant in mac-address-table failed.</p> <p>[Action] If the total number of supplicants to be authenticated including other types of authentication exceeds the capacity limit of a Switch, perform authentication again when the number of authenticated supplicants goes below the capacity limit.</p>	MAC address port number or channel group number VLAN ID
46	NOTICE	LOGIN	Login failed. ; Failed to authenticate the supplicant because it could not be registered to MAC VLAN.(code=x)	<p>[Meaning] Authentication failed because the registration of a supplicant in the MAC VLAN failed.</p> <p>[Action] If the total number of supplicants to be authenticated including other types of authentication exceeds the capacity limit of a Switch, perform authentication again when the number of authenticated supplicants goes below the capacity limit.</p>	MAC address port number or channel group number VLAN ID
47	NOTICE	LOGIN	Login failed. ; Failed to connect to RADIUS server.	<p>[Meaning] Authentication failed because an attempt to connect to the RADIUS server failed.</p> <p>[Action] Check the following:</p> <ul style="list-style-type: none"> • Communication between the Switch and the RADIUS server is available. • The RADIUS server functionality is enabled. 	MAC address port number or channel group number VLAN ID
48	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Could not be registered to hardware.)	<p>[Meaning] Authentication failed because registration of a supplicant in the hardware failed.</p> <p>[Action] If this message appears frequently, use the <code>restart dot1x</code> command to restart the IEEE 802.1X program.</p>	MAC address port number or channel group number VLAN ID
80	WARNING	SYSTEM	Invalid EAPOL frame received.	<p>[Meaning] An invalid EAPOL frame has been received.</p> <p>[Action] Check whether there is any problem with the following:</p> <ul style="list-style-type: none"> • The contents of EAPOL frames sent by the supplicant • Transmission line quality 	n/a

#	Log ID	Log type	Message text	Meaning and action	Additional information
81	WARNING	SYSTEM	Invalid EAP over RADIUS frame received.	<p>[Meaning] An invalid EAP over RADIUS frame has been received.</p> <p>[Action] Check whether there is any problem with the following:</p> <ul style="list-style-type: none"> • The contents of packets sent by the RADIUS server • Transmission line quality 	n/a
82	WARNING	SYSTEM	Failed to connect to RADIUS server.	<p>[Meaning] An attempt to connect to the RADIUS server failed.</p> <p>[Action] Check the following:</p> <ul style="list-style-type: none"> • Communication between the Switch and the RADIUS server is available. • The RADIUS server functionality is enabled. 	Server IP address
83	WARNING	SYSTEM	Failed to connect to RADIUS server.	<p>[Meaning] An attempt to connect to the RADIUS server failed.</p> <p>[Action] Check the following:</p> <ul style="list-style-type: none"> • Communication between the Switch and the RADIUS server is available. • The RADIUS server functionality is enabled. 	Server IPv6 address
84	WARNING	SYSTEM	Failed to connect to Accounting server.	<p>[Meaning] An attempt to connect to the accounting server failed.</p> <p>[Action] Check the following:</p> <ul style="list-style-type: none"> • Communication between the Switch and the accounting server is available. • The accounting server functionality is enabled. 	Server IP address
85	WARNING	SYSTEM	Failed to connect to Accounting server.	<p>[Meaning] An attempt to connect to the accounting server failed.</p> <p>[Action] Check the following:</p> <ul style="list-style-type: none"> • Communication between the Switch and the accounting server is available. • The accounting server functionality is enabled. 	Server IPv6 address

#	Log ID	Log type	Message text	Meaning and action	Additional information
86	WARNING	SYSTEM	Failed in the name resolution with the DNS server.	[Meaning] Name resolution by the DNS server failed. [Action] Change the server set by the <code>radius-server host</code> configuration command to IPv4 or IPv6 address.	Server name
90	ERROR	SYSTEM	Failed to open socket.	[Meaning] An attempt to open a socket has failed. [Action] If this message appears frequently, use the <code>restart dot1x</code> command to restart the IEEE 802.1X program.	n/a

Legend n/a: Not applicable

Impact on communication

None

Response messages

Table 5-14: List of response messages for the show dot1x logging command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Receive Error)	An attempt to receive data from the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Send Error)	An attempt to send data to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Dot1x doesn't seem to be running.	The IEEE 802.1X setting has not been enabled. Check the configuration.
Now another user is using dot1x command, please try again.	Another user is using the <code>dot1x</code> command. Wait a while, and then retry the operation.

Notes

None

clear dot1x logging

Clears the operation log messages collected by IEEE 802.1X program.

Syntax

```
clear dot1x logging
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 5-25: Clearing IEEE 802.1X operation log messages

```
> clear dot1x logging
>
```

Display items

None

Impact on communication

None

Response messages

Table 5-15: List of response messages for the clear dot1x logging command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Receive Error)	An attempt to receive data from the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Connection failed to 802.1X program.(Reason:Send Error)	An attempt to send data to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart dot1x</code> command to restart IEEE 802.1X.
Dot1x doesn't seem to be running.	The IEEE 802.1X setting has not been enabled. Check the configuration.
Now another user is using dot1x command, please try again.	Another user is using the <code>dot1x</code> command. Wait a while, and then retry the operation.

Notes

None

Chapter

6. 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 logging
show web-authentication
show web-authentication statistics
clear web-authentication logging
clear web-authentication statistics
commit web-authentication
store web-authentication
load web-authentication
clear web-authentication auth-state
restart web-authentication
dump protocols web-authentication
set web-authentication html-files
clear web-authentication html-files
show web-authentication html-files
```

set web-authentication user

Adds a user for Web authentication. At this time, specify the VLAN to which the user belongs.

To apply the change to the authentication information, execute the `commit web-authentication` command.

Syntax

```
set web-authentication user <user name> <password> <vlan id>
```

Input mode

Administrator mode

Parameters

<user name>

Specify a user name to be registered.

Only alphanumeric characters can be used, and the characters are case sensitive. Specify a name with 1 to 16 characters.

<password>

Specify a password.

Only alphanumeric characters can be used, and the characters are case sensitive. Specify a name with 1 to 16 characters.

<vlan id>

For details about the specifiable range of values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

- When dynamic VLAN mode or legacy 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 a VLAN ID.

Example

When `USER01` is added as the user name, `user0101` as the password, and `10` as the VLAN ID:

```
# set web-authentication user USER01 user0101 10
```

Display items

None

Impact on communication

None

Response messages

Table 6-1: List of response messages for the set web-authentication user command

Message	Description
Already user '<user name>' exists.	The specified user has already been registered.
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
Now another user is using WA command, please try again.	Another user is using a command for the Web authentication functionality. Wait a while, and then retry the operation.
The number of users exceeds 300.	The number of users to be registered exceeds 300.
WA is not configured.	The Web authentication 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 <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.

Only alphanumeric characters can be used, and the characters are case sensitive. Specify a name with 1 to 16 characters.

<old password>

Specify the password before the change.

Only alphanumeric characters can be used, and the characters are case sensitive. Specify a name with 1 to 16 characters.

<new password>

Specify the password after the change.

Only alphanumeric characters can be used, and the characters are case sensitive. Specify a name with 1 to 16 characters.

Example

Changing the password for user USER01:

```
# set web-authentication passwd USER01 user0101 user1111
```

Display items

None

Impact on communication

None

Response messages

Table 6-2: List of response messages for the set web-authentication passwd command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Now another user is using WA command, please try again.	Another user is using a command for the Web authentication functionality. Wait a while, and then retry the operation.
The old-password is different.	The old password for the specified user is incorrect.
Unknown user '<user name>'.	The specified user has not been registered.

Message	Description
WA 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 <user name> <vlan id>
```

Input mode

Administrator mode

Parameters

<user name>

Specify the name of the user for which the VLAN is being changed.

Only alphanumeric characters can be used, and the characters are case sensitive. Specify a name with 1 to 16 characters.

<vlan id>

Specify the VLAN ID of the VLAN to be changed.

For details about the specifiable range of values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

Example

When changing the VLAN to which user USER01 belongs to 30

```
# set web-authentication vlan USER01 30
```

Display items

None

Impact on communication

None

Response messages

Table 6-3: List of response messages for the set web-authentication vlan command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Now another user is using WA command, please try again.	Another user is using a command for the Web authentication functionality. Wait a while, and then retry the operation.
Unknown user '<user name>'.	The specified user has not been registered.
WA is not configured.	The Web authentication 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 {<user name> | -all} [-f]
```

Input mode

Administrator mode

Parameters

<user name>

Deletes the specified user.

Only alphanumeric characters can be used, and the characters are case sensitive. Specify a name with 1 to 16 characters.

-all

Deletes all users.

-f

Deletes a user unconditionally.

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 6-4: List of response messages for the remove web-authentication user command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Now another user is using WA command, please try again.	Another user is using a command for the Web authentication functionality. Wait a while, and then retry the operation.
Unknown user '<user name>'.	The specified user has not been registered.

Message	Description
WA 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 authentication passwd command
- set 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

Displays user information being edited.

commit

Displays information about the user who is executing the command.

Example

- When displaying the user information being edited:

```
# show web-authentication user edit
Date 2006/10/14 10:52:49 UTC
Total user counts:2
username          VLAN
0123456789012345  3
USER01            4094
```
- When displaying information of the user who is performing operation:

```
# show web-authentication user commit
Date 2006/10/14 10:52:49 UTC
Total user counts:3
username          VLAN
0123456789012345  4
USER02            4094
USER03            2
```

Display items

Table 6-5: Information displayed for registered users of Web authentication

Item	Meaning	Displayed information
Total user counts	Total number of registered users	The number of registered users
username	User name	A registered user name
VLAN	VLAN	The VLAN set for the registered user

Impact on communication

None

Response messages*Table 6-6:* List of response messages for the show web-authentication user command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Now another user is using WA command, please try again.	Another user is using a command for the Web authentication functionality. Wait a while, and then retry the operation.
WA 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

The following shows an example of displaying authenticated users:

- When the authentication mode is dynamic VLAN mode or legacy mode:

```
# show web-authentication login
Date 2010/04/15 10:52:49 UTC
Total user counts:2
Username
VLAN      MAC address      Login time              Limit time
0123456789012345
  3      0012.e2e3.9166   2010/04/15 09:58:04 UTC  00:10:20
USER01
4094      0012.e268.7527   2010/04/15 10:10:23 UTC  00:20:35
```

- When the authentication mode is fixed VLAN mode:

```
# show web-authentication login
Date 2010/04/15 10:52:49 UTC
Total user counts:2
Username
VLAN      MAC address      Port  IP address
Login time      Limit time
0123456789012345
  3      0012.e2e3.9166   1/5   192.168.0.1
2010/04/15 09:58:04 UTC  00:10:20
USER01
4094      0012.e268.7527   1/6   192.168.1.10
2010/04/15 10:10:23 UTC  00:20:35
```

Display items

Table 6-7: Information displayed for authenticated users

Item	Meaning	Displayed information
Total user counts	Total number of users	The number of the authenticated, currently logged-in users
Username	User name	The name of the authenticated, currently logged-in user.
Port	Port number	The number of the physical port accommodating the authenticated, currently logged-in users (displayed for fixed VLAN mode)
IP address	IP address	The IP address of the authenticated, currently logged-in users (displayed for fixed VLAN mode)
VLAN	VLAN	The VLAN set for the authenticated, currently logged-in users

Item	Meaning	Displayed information
MAC address	MAC address	The MAC address of the authenticated, currently logged-in user
Login time	Login date and time	The time when the authenticated, currently logged-in user logged in
Limit time	Remaining login time	<p>The remaining login time of the authenticated, currently logged-in user.</p> <p>When a user is logged in, the remaining time might be displayed as <code>00:00:00</code> immediately before the user is logged out due to a timeout.</p> <p>When the maximum connection time is 10 to 1440 minutes: <code>hh:mm:ss</code> hour:minute:second</p> <p>When the maximum connection time is set to unlimited: infinity</p>

Impact on communication

None

Response messages

Table 6-8: List of response messages for the show web-authentication login command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart web-authentication</code> command to restart the Web authentication program.
WA is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

None

show web-authentication logging

Displays the operation log messages collected by Web authentication program.

Syntax

```
show web-authentication logging [user]
```

Input mode

Administrator mode

Parameters

user

Specify the type of operation log message to be displayed.

If this parameter is specified, user authentication information is displayed.

Operation when this parameter is omitted:

Displays the operation log of the Web authentication program and the user authentication information in chronological order.

Example

■ When the parameter is omitted:

```
# show web-authentication logging
Date 2007/11/15 10:52:49 UTC
No=1:Nov 15 00:09:50:NORMAL:LOGIN:MAC=0012.e200.0001 USER=testdata1 Login
succeeded.
No=2:Nov 15 00:10:10:NORMAL:LOGOUT: MAC=0012.e200.0001 USER=testdata1
Logout succeeded.
No=90:Nov 15 00:09:55:NORMAL:SYSTEM: connection failed ; L2MacManager.
```

■ When user is specified for the parameter:

```
# show web-authentication logging user
Date 2007/11/15 11:13:15 UTC
No=1:Nov 15 00:09:50:NORMAL:LOGIN: MAC=0012.e200.0001 USER=testdata1 Login
succeeded.
No=2:Nov 15 00:10:10:NORMAL:LOGOUT: MAC=0012.e200.0001 USER=testdata1
Logout succeeded.
```

Display items

Table 6-9: Information displayed for Web authentication operation log messages

Item	Meaning	Displayed information
Level	Levels of operation log messages	Severity of a log message
<log>	Operation log message	Contents of a registered operation log message

The following shows the display format of a message.

```
No=1:Nov 15 00:09:50:NORMAL:LOGIN: MAC=0012.e200.0001 USER=testdata1 Login succeeded.
(1) (2) (3) (4) (5) (6) (7)
```

(1) Message number: Indicates the number assigned to each message shown in Table 6-12: List of operation log messages.

(2) Date: Indicates the date recorded in the Web authentication program.

(3) Time: Indicates the time recorded in the Web authentication program.

(4) Log ID: Indicates the level of the operation log message.

(5) Log type: Indicates the type of operation that outputs the log message.

(6) Additional information: Indicates supplementary information provided in the message.

(7) Message body

Operation log messages show the following information:

- Log ID: See *Table 6-10: Log ID and type in operation log messages*.
- Log type: See *Table 6-10: Log ID and type in operation log messages*.
- Additional information: See *Table 6-11: Additional information*.
- List of messages: See *Table 6-12: List of operation log messages*.

Table 6-10: Log ID and type in operation log messages

Log ID	Log type	Meaning
NORMAL	LOGIN	Indicates that login was successful.
	LOGOUT	Indicates that logout was successful.
	SYSTEM	Indicates a runtime notification.
NOTICE	LOGIN	Indicates that authentication failed.
	LOGOUT	Indicates that logout failed.
ERROR	SYSTEM	Indicates a communication failure or an operation failure in the Web authentication program.

Table 6-11: Additional information

Display format	Meaning
MAC=xxxx.xxxx.xxxx	Indicates the MAC address.
USER=xxxxxxxxxx	Indicates the user ID.
IP=xxx.xxx.xxx	Indicates the IP address.
VLAN=xxxx	Indicates the VLAN ID. Note, however, that this is not displayed if VLAN ID information could not be acquired.
PORT=xx/xx	Indicates the port number.

Table 6-12: List of operation log messages

#	Log ID	Log type	Message text	Meaning and action	Additional information
1	NORMAL	LOGIN	Login succeeded.	[Meaning] The client was successfully authenticated. [Action] None	MAC address User name IP address ^{#1} VLAN ID ^{#1} Port number ^{#1}
2	NORMAL	LOGOUT	Logout succeeded.	[Meaning] Client successfully canceled authentication. [Action] None	MAC address User name IP address ^{#1} VLAN ID ^{#1} Port number ^{#1}

#	Log ID	Log type	Message text	Meaning and action	Additional information
3	NORMAL	LOGIN	Login update succeeded.	[Meaning] The user's login time was successfully updated. [Action] None	MAC address User name IP address ^{#1} VLAN ID ^{#1} Port number ^{#1}
4	NORMAL	LOGOUT	Force logout ; clear web-authentication command succeeded.	[Meaning] Authentication has been canceled by a command. [Action] None	MAC address User name IP address ^{#1} VLAN ID ^{#1} Port number ^{#1}
5	NORMAL	LOGOUT	Force logout ; Connection time was beyond a limit.	[Meaning] Authentication was canceled because the maximum connection time was exceeded. [Action] None	MAC address User name IP address ^{#1} VLAN ID ^{#1} Port number ^{#1}
6	NORMAL	LOGOUT	Force logout ; mac-address-table aging.	[Meaning] Authentication was canceled because a MAC address was deleted due to mac-address-table aging. [Action] The terminal is not in use. Check the terminal.	MAC address User name IP address ^{#1} VLAN ID ^{#1} Port number ^{#1}
7	NORMAL	LOGOUT	Force logout ; VLAN deleted.	[Meaning] Authentication was canceled because a VLAN for Web authentication was deleted. [Action] Check the VLAN configuration settings.	MAC address User name VLAN ID
8	NORMAL	LOGOUT	Force logout ; Authentic method changed (RADIUS <-> Local).	[Meaning] Authentication was canceled because the authentication method was switched between the RADIUS authentication and local authentication. [Action] None	MAC address User name IP address ^{#1} VLAN ID Port number ^{#1}
10	NOTICE	LOGIN	Login failed ; User name not found to web authentication DB.	[Meaning] Authentication failed because the specified user ID was not registered in the internal DB, or the number of characters for the user ID was out of range. [Action] Use the correct user ID to log in.	User name

#	Log ID	Log type	Message text	Meaning and action	Additional information
11	NOTICE	LOGIN	Login failed ; Password not found to web authentication DB. [Password=[password]]	[Meaning] Authentication failed because a password was not entered or the entered password was incorrect. [Action] Use the correct password to log in.	User name Password
12	NOTICE	LOGIN	Login failed ; ARP resolution.	[Meaning] Authentication failed because ARP resolution of the client PC's IP address failed. [Action] Log in again.	User name IP address
13	NOTICE	LOGOUT	Logout failed ; ARP resolution.	[Meaning] Authentication could not be canceled because ARP resolution of the client PC's IP address failed. [Action] Log out again.	User name ^{#1} IP address
14	NOTICE	LOGIN	Login failed ; Double login.	[Meaning] Authentication failed because duplicated login operation was performed. The cause is either of the following: <ul style="list-style-type: none"> The user has already logged in the same client PC using a different user ID. In dynamic VLAN mode, the user has already logged in the same client PC in a different VLAN [Action] Log in from another PC. Alternatively, log out from the same client PC, and then log in again.	MAC address User name

#	Log ID	Log type	Message text	Meaning and action	Additional information
15	NOTICE	LOGIN	Login failed ; Number of login was beyond limit.	<p>[Meaning] Authentication cannot be performed because the number of logins exceeded the maximum allowable number. The cause is either of the following:</p> <ul style="list-style-type: none"> • The capacity limit for Web authentication has already been exceeded. • The total number of IEEE 802.1X authentications, Web authentications, and MAC-based authentications exceeded the capacity limit. <p>[Action] Log in again when the number of authenticated users drops low enough.</p>	MAC address User name
17	NOTICE	LOGIN	Login failed ; VLAN not specified.	<p>[Meaning] Authentication could not be performed because the VLAN ID did not match the VLAN ID set for Web authentication.</p> <p>[Action] Set the correct VLAN ID in the configuration.</p>	MAC address User name VLAN ID
18	NOTICE	LOGIN	Login failed ; MAC address could not register.	<p>[Meaning] Authentication could not be performed because registration of the MAC address failed.</p> <p>[Action] Log in again.</p>	MAC address User name
19	NOTICE	LOGOUT	Logout failed ; MAC address could not delete.	<p>[Meaning] Authentication could not be performed because deletion of the MAC address failed.</p> <p>[Action] Log out again.</p>	MAC address ^{#2} User name ^{#1, #2} VLAN ID ^{#1, #2} Port number ^{#1, #2}
20	NOTICE	LOGIN	Login failed ; RADIUS authentication failed.	<p>[Meaning] Authentication could not be performed because RADIUS authentication failed.</p> <p>[Action] Use the correct user ID to log in.</p>	MAC address User name IP address ^{#1} VLAN ID ^{#1} Port number ^{#1}

#	Log ID	Log type	Message text	Meaning and action	Additional information
21	NOTICE	LOGIN	Login failed ; Failed to connection to RADIUS server.	<p>[Meaning] Authentication failed because an attempt to communicate with the RADIUS server failed.</p> <p>[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.</p>	MAC address User name IP address ^{#1} VLAN ID ^{#1} Port number ^{#1}
22	NOTICE	LOGIN	Login failed ; Connection failed L2MacManager.	<p>[Meaning] Authentication failed because an attempt to communicate with the VLAN program failed.</p> <p>[Action] Log in again. If this message appears frequently, specify the <code>mac-manager</code> parameter for the <code>restart vlan</code> command and execute it.</p>	MAC address User name
23	NOTICE	LOGIN	Login failed ; L2MacManager failed.	<p>[Meaning] Authentication failed because notification from the VLAN program was received indicating that authentication could not be performed.</p> <p>[Action] Log in again. If this message appears frequently, specify the <code>mac-manager</code> parameter for the <code>restart vlan</code> command and execute it.</p>	MAC address User name

#	Log ID	Log type	Message text	Meaning and action	Additional information
24	NOTICE	LOGOUT	Logout failed ; L2MacManager failed.	<p>[Meaning] Canceling authentication failed because a notification from the VLAN program indicating that de-authentication could not be performed was received. The cause is either of the following:</p> <ul style="list-style-type: none"> • IEEE 802.1X authentication performed on the same PC after Web authentication. • After Web authentication, the same MAC address as the authenticated terminal is registered by using the <code>mac-address</code> configuration command. <p>[Action] Analyze the cause and log in again.</p>	MAC address
25	NOTICE	LOGIN	Login failed ; Double login. (L2MacManager)	<p>[Meaning] Authentication failed because notification from the VLAN program was received indicating that authentication could not be performed. The cause is either of the following:</p> <ul style="list-style-type: none"> • The terminal for which Web authentication was performed had already been authenticated by IEEE 802.1X or MAC-based authentication. • The MAC address for the terminal to be authenticated had already been registered by the <code>mac-address</code> configuration command. <p>[Action] Use another terminal to log in.</p>	MAC address User name VLAN ID

#	Log ID	Log type	Message text	Meaning and action	Additional information
26	NORMAL	LOGOUT	Force logout ; VLAN deleted.	<p>[Meaning] When the mode is legacy mode, authentication of the user logged in to a VLAN was deleted because the VLAN set for the interface was deleted.</p> <p>[Action] Configure the VLAN (MAC VLAN) again.</p>	<p>[Legacy mode] MAC address User name VLAN ID</p>
				<p>[Meaning] When the mode is fixed VLAN mode or dynamic VLAN mode, authentication of a user who logged in to a VLAN was canceled because the VLAN set for the interface was deleted or the mode of the VLAN was changed.</p> <p>[Action] Configure the VLAN again.</p>	<p>[Fixed VLAN mode or Dynamic VLAN mode] MAC address User name IP address VLAN ID Port number</p>
27	NOTICE	LOGIN	Login failed ; VLAN not specified.	<p>[Meaning] In legacy mode, authentication cannot be performed because the authentication request was sent from a VLAN that was not set for the interface.</p> <p>[Action] Correctly configure the VLAN again.</p>	<p>MAC address User name VLAN ID</p>
28	NORMAL	LOGOUT	Force logout ; Polling time out.	<p>[Meaning] Authentication was canceled because disconnection of an authenticated terminal was detected.</p> <p>[Action] None</p>	<p>MAC address User name IP address VLAN ID Port number</p>
29	NORMAL	LOGOUT	Force logout ; Client moved.	<p>[Meaning] Authentication was canceled because it was detected that the port of an authenticated terminal was moved.</p> <p>[Action] Log in again.</p>	<p>MAC address User name IP address VLAN ID Port number</p>
31	NORMAL	LOGOUT	Force logout ; Port not specified.	<p>[Meaning] Authentication has been canceled because the setting for the port was deleted.</p> <p>[Action] Check the configuration.</p>	<p>MAC address User name IP address VLAN ID Port number</p>

#	Log ID	Log type	Message text	Meaning and action	Additional information
32	NOTICE	LOGIN	Login update failed.	<p>[Meaning] The login time could not be updated because re-authentication of the user failed.</p> <p>[Action] Log in again using the correct user ID and password.</p>	MAC address User name IP address
33	NORMAL	LOGOUT	Force logout ; Port link down.	<p>[Meaning] Authentication of all users logged in for the port was canceled because the link for the applicable port was down.</p> <p>[Action] After confirming that the port status is link-up, log in again.</p>	MAC address User name IP address VLAN ID Port number
34	NOTICE	LOGIN	Login failed ; Port not specified.	<p>[Meaning] Authentication cannot be performed because the request was not issued from the port set for fixed VLAN mode or dynamic VLAN mode.</p> <p>[Action] Connect the terminal to the port to be authenticated, and then log in again.</p>	MAC address User name Port number
39	NOTICE	LOGIN	Login failed ; VLAN not specified.	<p>[Meaning] When the mode is fixed VLAN mode or dynamic VLAN mode, authentication cannot be performed because the authentication request was issued by a VLAN which is not set for the interface.</p> <p>[Action] Set a correct configuration, and log in again.</p>	MAC address User name IP address VLAN ID Port number
40	NORMAL	LOGOUT	Force logout ; Ping packet accepted.	<p>[Meaning] Authentication of the user was canceled because a logout ping was received.</p> <p>[Action] None</p>	MAC address User name IP address VLAN ID Port number

#	Log ID	Log type	Message text	Meaning and action	Additional information
41	NORMAL	LOGOUT	Force logout ; Other authentication program.	[Meaning] Authentication was canceled because it was overwritten by another authentication operation. [Action] Make sure other authentication methods are not used for login from the same terminal.	MAC address User name IP address VLAN ID Port number
48	NORMAL	LOGOUT	Force logout ; Program stopped.	[Meaning] Authentication of all users was canceled because the Web authentication program has stopped. [Action] To use Web authentication uninterruptedly for authentication, set the configuration.	MAC address User name IP address VLAN ID Port number
49	NORMAL	LOGOUT	Force logout ; Authentic mode had changed (dynamic vlan -> static vlan).	[Meaning] Authentication of all users was canceled because the authentication method was switched from legacy mode or dynamic VLAN mode to fixed VLAN mode. [Action] None	MAC address User name IP address ^{#1} VLAN ID Port number ^{#1}
50	NORMAL	LOGOUT	Force logout ; Authentic mode had changed (static vlan -> dynamic vlan).	[Meaning] Authentication of all users was canceled because the authentication method was switched from fixed VLAN mode to legacy mode or dynamic VLAN mode. [Action] None	MAC address User name IP address VLAN ID Port number
51	NOTICE	LOGIN	Login failed ; IP address is not right.	[Meaning] In fixed VLAN mode or dynamic VLAN mode, login operation was performed by using an IP address other than Web authentication IP address. [Action] Log in by using the Web authentication IP address.	User name IP address
52	NORMAL	LOGOUT	Force logout ; Authentic mode had changed (Legacy -> dynamic vlan).	[Meaning] All authentications were canceled because the authentication method was changed from legacy mode to dynamic VLAN mode. [Action] None	MAC address User name VLAN ID

#	Log ID	Log type	Message text	Meaning and action	Additional information
53	NORMAL	LOGOUT	Force logout ; Authentic mode had changed (dynamic vlan -> Legacy).	[Meaning] All authentications were canceled because authentication method was changed from dynamic VLAN mode to legacy mode. [Action] None	MAC address User name IP address VLAN ID Port number
82	NORMAL	SYSTEM	Accepted clear auth-state command.	[Meaning] A request issued by the clear web-authentication auth-state command to cancel authentication was received. [Action] None	n/a
83	NORMAL	SYSTEM	Accepted clear statistics command.	[Meaning] A request issued by the clear web-authentication statistics command to clear statistics was received. [Action] None	n/a
84	NORMAL	SYSTEM	Accepted commit command.	[Meaning] A commit notification issued by the commit web-authentication command for the internal DB was received. [Action] None	n/a
85	NORMAL	SYSTEM	Accepted dump command.	[Meaning] A dump output request issued by the dump protocols web-authentication command was received. [Action] None	n/a
86	NORMAL	LOGOUT	Force logout ; MAC address not found L2MacManager.	[Meaning] A MAC address is available for Web authentication, but it is not available for the VLAN program. Therefore, an attempt was made to register a MAC address in the VLAN program, but it failed and authentication is canceled. [Action] Log in again.	MAC address User name

#	Log ID	Log type	Message text	Meaning and action	Additional information
87	NORMAL	SYSTEM	MAC address existed in the L2MacManager.	<p>[Meaning] A MAC address, which is available for the VLAN program, but it is not available for Web authentication, was detected.</p> <p>[Action] No action is available because Web authentication falls in the unauthenticated state.</p>	MAC address User name
88	ERROR	SYSTEM	WAD could not initialize.[error code]	<p>[Meaning] Initializing the Web authentication program failed.</p> <p>[Action] Reconfigure the configuration for Web authentication. If this message appears frequently, use the <code>restart web-authentication</code> command to restart the Web authentication program.</p>	error code
89	ERROR	SYSTEM	Connection failed ; Operation command. error=[error-code]	<p>[Meaning] Outputting the response message for the command failed.</p> <p>[Action] Wait a while, and then re-execute the command.</p>	error code
90	ERROR	SYSTEM	Connection failed ; L2MacManager.	<p>[Meaning] An attempt to communicate with the VLAN program was made, but failed.</p> <p>[Action] If this message appears frequently, specify the <code>mac-manager</code> parameter for the <code>restart vlan</code> command and execute it.</p>	n/a
92	ERROR	SYSTEM	Disconnection failed ; L2MacManager.	<p>[Meaning] Communication with the VLAN program was interrupted.</p> <p>[Action] If this message appears frequently, specify the <code>mac-manager</code> parameter for the <code>restart vlan</code> command and execute it.</p>	n/a

#	Log ID	Log type	Message text	Meaning and action	Additional information
96	ERROR	SYSTEM	Program failed ; Login information could not delete.	[Meaning] An attempt to delete the login information failed. [Action] If this message appears frequently, use the <code>restart web-authentication</code> command to restart the Web authentication program.	n/a
97	ERROR	SYSTEM	Connection failed ; Driver. [error code]	[Meaning] Connection with the driver failed. [Action] Reconfigure the configuration for Web authentication. If this message appears frequently, use the <code>restart web-authentication</code> command to restart the Web authentication program.	error code
98	NOTICE	LOGOUT	Logout failed ; User is not authenticating.	[Meaning] Logout failed because the user is not being authenticated by Web authentication. [Action] Use the <code>show web-authentication login</code> command to check the authentication status.	MAC address
99	ERROR	SYSTEM	Accounting failed ; RADIUS accounting.	[Meaning] A response to an accounting request was not received from the RADIUS server. [Action] Check whether communication is possible between the Switch and the RADIUS server.	MAC address User name
100	NORMAL	SYSTEM	Accepted clear logging command.	[Meaning] A request to delete the operation log by the <code>clear web-authentication logging</code> command was received. [Action] None	n/a
101	NOTICE	SYSTEM	Change to redundancy mode (SBY -> ACT).	[Meaning] The Web authentication program was switched from standby mode to active mode. [Action] None	n/a

#	Log ID	Log type	Message text	Meaning and action	Additional information
102	NOTICE	SYSTEM	Change to redundancy mode (ACT -> SBY).	[Meaning] The Web authentication program was switched from active mode to standby mode. [Action] None	n/a
103	NORMAL	SYSTEM	Synchronized ; Wad -> L2MacManager.	[Meaning] The authentication status was registered in the hardware because a difference with the hardware was found. [Action] No action is required because the authentication status and the hardware status can be synchronized by Web authentication.	MAC address User name
104	NORMAL	LOGOUT	Force logout ; L2MacManager synchronize.	[Meaning] The authentication status was cleared because a difference with the hardware was found. [Action] No action is required because the authentication status and the hardware status can be synchronized by Web authentication.	MAC address User name
105	NOTICE	LOGIN	Login failed ; VLAN suspended.	[Meaning] An authentication error occurred because the VLAN used by the login user to be switched after authentication was in the <code>disable</code> status. [Action] Enable the VLAN after authentication, and then log in again.	MAC address User name VLAN ID
106	NORMAL	LOGOUT	Force logout ; VLAN suspended.	[Meaning] Authentication was canceled because the status of the VLAN for the login user changed to <code>disable</code> . [Action] Enable the VLAN after authentication, and then log in again.	MAC address User name IP address ^{#1} VLAN ID Port number ^{#1}

#	Log ID	Log type	Message text	Meaning and action	Additional information
255	ERROR	SYSTEM	The other error. [error-code]	<p>[Meaning] An internal Web authentication error occurred. Communication failed with an internal functionality indicated by the error code in [] after The other error..</p> <p>[Action] An internal Web authentication error occurred. Use the <code>dump protocols web-authentication command</code> to collect information, and then use the <code>restart web-authentication command</code> to restart Web authentication.</p>	error code

Legend n/a: Not applicable

#1: Displayed when the mode is fixed VLAN mode or dynamic VLAN mode.

#2: Displayed if logout failed during logout processing caused by port down, VLAN suspend, or specification by a user using an operation command.

Impact on communication

None

Response messages

Table 6-13: List of response messages for the show web-authentication logging command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart web-authentication command</code> to restart the Web authentication program.
WA is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

- Web authentication operation log messages are displayed starting from the newer messages.
- For duplex configuration, operation log information is deleted on transfer between active and standby, rather than being inherited.

show web-authentication

Displays the configuration for Web authentication.

Syntax

```
show web-authentication
```

Input mode

Administrator mode

Parameters

None

Example

- When the authentication mode is legacy mode and the authentication method is local authentication with no registered VLANs:

```
# show web-authentication
Date 2010/04/16 10:52:49 UTC
web-authentication Information:
  Authentic-mode   : Legacy
  Authentic-method : Local           Accounting-state : disable
    Max-timer     : 60               Max-user       : 4096
    VLAN Count    : 0               Auto-logout    : enable
  Syslog-send      : enable
  Jump-URL          : http://www.example.com/
  Web-port          : http   : 80      https   : 443
```

- When the authentication mode is legacy mode and the authentication method is local authentication with registered VLANs:

```
# show web-authentication
Date 2010/04/16 10:52:49 UTC
web-authentication Information:
  Authentic-mode   : Legacy
  Authentic-method : Local           Accounting-state : disable
    Max-timer     : 60               Max-user       : 4096
    VLAN Count    : 16              Auto-logout    : disable
  Syslog-send      : enable
  Jump-URL          : http://www.example.com/
  Web-port          : http   : 80      https   : 443
```

```
VLAN Information:
  VLAN ID :      5,10,15,20,25,30,35,40,1000-1007
```

- When the authentication mode is fixed VLAN mode and the authentication method is RADIUS authentication:

```
# show web-authentication
Date 2010/04/15 10:52:49 UTC
web-authentication Information:
  Authentic-mode   : Static-VLAN
  Authentic-method : RADIUS           Accounting-state : disable
    Max-timer     : 60               Max-user       : 4096
    VLAN Count    : -               Auto-logout    : -
  Syslog-send      : enable
  Alive-detection  : enable
    timer         : 60               interval-timer : 3       count   : 3
  Jump-URL          : http://www.example.com/
  Web-IP-address    : 192.168.1.1
  FQDN              : aaa.example.com
  Web-port          : http   : 80, 8080      https   : 443, 8443
  Access-list-No    : 100
```

```

Port      : 1/1
VLAN ID   : 5,10,15

```

```

Port      : 1/2
VLAN ID   : 15-16

```

- When the authentication mode is dynamic VLAN mode and the authentication method is local authentication:

```

# show web-authentication
Date 2010/04/15 10:52:49 UTC
web-authentication Information:
Authentic-mode   : Dynamic-VLAN
Authentic-method : Local           Accounting-state : disable
Max-timer       : 60               Max-user       : 4096
VLAN Count      : -               Auto-logout    : disable
Syslog-send     : enable
URL-redirect    : enable          Protocol : http
Jump-URL        : http://www.example.com/
Web-IP-address  : 192.168.1.1
FQDN            : aaa.example.com
Web-port        : http : 80, 8080   https : 443, 8443
Redirect-vlan   : 10
Access-list-No  : 100

Port      : 1/10
VLAN ID   : 1000,1500
Native VLAN : 10

Port      : 1/12
VLAN ID   : 1000,1500
Native VLAN : 10

```

- When the authentication mode is dynamic VLAN mode and the authentication method is RADIUS authentication:

```

# show web-authentication
Date 2010/04/15 10:52:49 UTC
web-authentication Information:
Authentic-mode   : Dynamic-VLAN
Authentic-method : RADIUS          Accounting-state : enable
Max-timer       : 60               Max-user       : 4096
VLAN Count      : -               Auto-logout    : disable
Syslog-send     : enable
URL-redirect    : enable          Protocol : http
Jump-URL        : http://www.example.com/
Web-IP-address  : 192.168.1.1
FQDN            : aaa.example.com
Web-port        : http : 80, 8080   https : 443, 8443
Redirect-vlan   : 10
Access-list-No  : 100

Port      : 1/10
VLAN ID   : 1000,1500
Native VLAN : 10

Port      : 1/12
VLAN ID   : 1000,1500
Native VLAN : 10

```

Display items

Table 6-14: Items displayed for the Web authentication configuration

Item	Meaning	Displayed information
Authentic-mode	Authentication mode	Authentication mode for the Web authentication functionality. Legacy: Indicates legacy mode. Dynamic-VLAN: Indicates dynamic VLAN mode Static-VLAN: Indicates fixed VLAN mode
Authentic-method	Authentication method	Authentication method for the Web authentication functionality. Local: Indicates local authentication RADIUS: Indicates RADIUS authentication
Accounting-state	Whether the accounting server is available	Whether the accounting server is available for the Web authentication functionality. enable: The accounting server is available. disable: An accounting server is not available.
Max-timer	Maximum connection time	Maximum connection time (in minutes) for a login user
Max-user	Maximum number of authenticated users	The maximum number of authenticated users who can log in to the Web authentication functionality.
VLAN Count	Total number of VLANs	The total number of VLANs registered in legacy mode for Web authentication. Note that - is displayed in mode other than legacy mode.
Auto-logout	Whether forced logout by MAC address aging is available	Whether forced logout by MAC address aging in legacy mode and dynamic VLAN mode for the Web authentication functionality is available. enable: Forced logout can be used. disable: Forced logout cannot be used. - is displayed when the mode is fixed VLAN mode.
Syslog-send	The usage state of the syslog server output functionality	The usage state of the functionality that outputs the Web authentication operation log to the syslog server. enable: Used disable: Not used
Alive-detection	Usage state	The usage state of the functionality that cancels authentication when disconnection of a terminal authenticated in fixed VLAN mode of Web authentication is detected. enable: Used disable: Not used
timer	Monitoring packet sending interval	Displays the monitoring packet sending interval for detecting disconnection of terminals authenticated through Web authentication in seconds.
interval-timer	The interval for retransmitting monitoring packets	The interval for retransmitting monitoring packets if no monitoring packets are returned from a terminal (in seconds)
count	The number of monitoring packet retransmissions	The number of monitoring packet retransmissions used for detecting disconnection of a terminal authenticated through Web authentication
URL-redirect	Usage state	The usage state of URL redirection in Web authentication dynamic VLAN mode. enable: Used disable: Not used

Item	Meaning	Displayed information
Protocol	http/https type	Login page type to be displayed on a terminal. http: Login page is displayed in http. https: Login page is displayed in https.
Jump-URL	URL to jump to after authentication	URL to jump to after Web authentication is successful
Web-IP-address	IP address	Web authentication IP address
FQDN	FQDN setting	Specified FQDN (Fully Qualified Domain Name). - is displayed if no FQDNs have been configured.
Web-port	Communication port	The number of the communication port for the Web server
http	http port	The number of the communication port for http protocols
https	https port	The number of the communication port for https protocols
Redirect-vlan	VLAN information	The ID of the VLAN for which URL redirection is configured.
Access-list-No.	Access Lists	The access list number or the access list name. - is displayed if neither is specified. ²
VLAN Information	VLAN information	Detailed information about a VLAN registered in Web authentication
Port	Port information	The number of the port embedded in a VLAN
VLAN ID	VLAN information	VLAN ID registered in Web authentication.
Native VLAN	VLAN ID of a native VLAN	The VLAN ID of the native VLAN set for the port for dynamic VLAN mode

Impact on communication

None

Response messages

Table 6-15: List of response messages for the show web-authentication command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart web-authentication</code> command to restart the Web authentication program.
WA 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

- When the authentication mode is fixed VLAN mode or dynamic VLAN mode, and the authentication method is local authentication:

```
# show web-authentication statistics
Date 2010/04/15 11:10:49 UTC
web-authentication Information:
  Authentication Request Total :      100
  Authentication Current Count :       10
  Authentication Error Total   :       30
```

- When the authentication mode is fixed VLAN mode or dynamic VLAN mode, and the authentication method is RADIUS authentication:

```
# show web-authentication statistics
Date 2010/04/15 11:10:49 UTC
web-authentication Information:
  Authentication Request Total :      100
  Authentication Current Count :       10
  Authentication Error Total   :       30
RADIUS web-authentication Information:
[RADIUS frames]
  TxTotal   :      10  TxAccReq  :      10  TxError   :       0
  RxTotal   :      30  RxAccAccpt:      10  RxAccRejct:      10
                        RxAccChllg:      10  RxInvalid :       0
Account web-authentication Information:
[Account frames]
  TxTotal   :      10  TxAccReq  :      10  TxError   :       0
  RxTotal   :      20  RxAccResp :      10  RxInvalid :       0
```

- When the authentication mode is legacy mode and the authentication method is local authentication:

```
# show web-authentication statistics
Date 2010/04/12 11:10:49 UTC
web-authentication Information:
  Authentication Request Total :      100
  Authentication Current Count :       10
  Authentication Error Total   :       30
```

- When the authentication mode is legacy mode and the authentication method is RADIUS authentication:

```
# show web-authentication statistics
Date 2010/04/12 11:10:49 UTC
web-authentication Information:
  Authentication Request Total :      100
  Authentication Current Count :       10
  Authentication Error Total   :       30
RADIUS web-authentication Information:
```



```

[RADIUS frames]
    TxTotal    :      10  TxAccReq  :      10  TxError   :      0
    RxTotal    :      30  RxAccAcpt :      10  RxAccRejt :     10
                        RxAccChllg:      10  RxInvalid :      0
Account web-authentication Information:
[Account frames]
    TxTotal    :      10  TxAccReq  :      10  TxError   :      0
    RxTotal    :      20  RxAccResp :      10  RxInvalid :      0

```

Display items

Table 6-16: Items displayed for Web authentication statistics

Item	Meaning
Authentication Request Total	The total number of authentication requests
Authentication Current Count	The number of users currently authenticated
Authentication Error Total	The total number of authentication request errors
RADIUS frames	RADIUS information
TxTotal	The total number of packets transmitted to the RADIUS server
TxAccReq	The total number of Access-Request packets sent to the RADIUS server
TxError	The number of errors occurring during transmission to the RADIUS server
RxTotal	The total number of received packets from the RADIUS server
RxAccAcpt	The total number of Access-Accept packets received from the RADIUS server
RxAccRejt	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 6-17: List of response messages for the show web-authentication statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart web-authentication</code> command to restart the Web authentication program.
WA is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

Information is deleted because statistics are not inherited for duplex configuration.

clear web-authentication logging

Clears log information for Web authentication.

Syntax

```
clear web-authentication logging
```

Input mode

Administrator mode

Parameters

None

Example

The following shows an example of clearing log information for Web authentication.

```
# clear web-authentication logging
```

Display items

None

Impact on communication

None

Response messages

Table 6-18: List of response messages for the clear web-authentication logging command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart web-authentication</code> command to restart the Web authentication program.
WA 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 6-19: List of response messages for the clear web-authentication statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart web-authentication</code> command to restart the Web authentication program.
WA is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

None

commit web-authentication

Stores local authentication user data for Web authentication in internal flash memory.

Syntax

```
commit web-authentication [-f]
```

Input mode

Administrator mode

Parameters

-f

Stores local authentication data for Web authentication in internal flash memory without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

The following shows an example of storing local authentication data for Web authentication:

```
# commit web-authentication
Commitment web-authentication user data. Are you sure? (y/n): y
Commit complete.
```

Display items

None

Impact on communication

None

Response messages

Table 6-20: List of response messages for the commit web-authentication command

Message	Description
Can not commit.	An attempt to update the authentication information failed. Execute the <code>restart web-authentication</code> command to update the authentication information again.
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Command information was damaged.	Information was discarded because the execution information is corrupted.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart web-authentication</code> command to restart the Web authentication program.
Now another user is using WA command, please try again.	Another user is using a command for the Web authentication functionality. Wait a while, and then retry the operation.
WA is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

- Information about the Web authentication DB which is being operated is not overwritten unless this command is executed after the following commands are executed to add, change, or delete users:
 - set web-authentication user
 - set web-authentication passwd
 - set web-authentication vlan
 - remove web-authentication user
- If execution of this command is interrupted before completion, the Web authentication database is not updated. In such a case, re-execute the command to update the Web authentication database.

store web-authentication

Backs up Web authentication user information to a file.

Syntax

```
store web-authentication <file name> [-f]
```

Input mode

Administrator mode

Parameters

<file name>

Specify the name of the file to which Web authentication user information is to be backed up.

-f

Backs up Web authentication user information to a file without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

When the authdata backup file for Web authentication user information is created:

```
# store web-authentication authdata
Backup web-authentication user data. Are You sure? (y/n): y
Backup complete.
```

Display items

None

Impact on communication

None

Response messages

Table 6-21: List of response messages for the store web-authentication command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Now another user is using WA command, please try again.	Another user is using a command for the Web authentication functionality. Wait a while, and then retry the operation.
Store operation failed.	Restoration from the backup file failed.
WA is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

If Web authentication user information is backed up to a file when the available space in the flash memory is insufficient, incomplete backup files might be created. When creating backup files, use the `show flash` command to make sure there is enough free capacity in the flash memory.

The following shows an example of executing the `show flash` command:

```
> show flash
```

Date 2007/04/01 19:46:29 JST

Flash :

	user area	config area	dump area	area total
used	37,063kB	65kB	16kB	37,144kB
free	<u>616kB</u>	7,199kB	8,152kB	15,967kB
total	37,679kB	7,265kB	8,168kB	53,112kB

Note: The underlined part (the value for `free` indicating the free capacity of the user area) must be at least 20 KB.

If the free capacity in flash memory is insufficient, use the `rm` command to delete unnecessary files before creating the backup files.

load web-authentication

Restores Web authentication user information from a backup file for Web authentication user information. Note that information registered or changed by using the following commands will be replaced by the information that is being restored:

- set web-authentication user
- set web-authentication passwd
- set web-authentication vlan
- remove web-authentication user
- commit web-authentication

Syntax

```
load web-authentication <file name> [-f]
```

Input mode

Administrator mode

Parameters

<file name>

Specify the name of the backup file from which Web authentication user information is restored.

-f

Restores Web authentication user information without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

When Web authentication user information is restored from the authdata backup file:

```
# load web-authentication authdata
Restore web-authentication user data. Are you sure? (y/n): y
Restore complete.
```

Display items

None

Impact on communication

None

Response messages

Table 6-22: List of response messages for the load web-authentication command

Message	Description
Can not load.	An attempt to apply Web authentication information failed. Execute the <code>restart web-authentication</code> command, and then execute the <code>load web-authentication</code> command again to restore the Web authentication user information.
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart web-authentication</code> command to restart the Web authentication program.
File format error.	Registration is not possible because the file is not a backup file.
Load operation failed.	Restoration from the backup file failed.
Now another user is using WA command, please try again.	Another user is using a command for the Web authentication functionality. Wait a while, and then retry the operation.
WA is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

- 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`
- If execution of this command is interrupted before completion, the Web authentication database is not updated. In such a case, re-execute the command to update the Web authentication database.

clear web-authentication auth-state

Forcibly logs out an authenticated, currently logged-in user.

When multiple logins are performed using the same user ID, if a user logs out by using this command, all users who have the same user ID are forcibly logged out. Alternatively, a specific login can be canceled by specifying a MAC address.

Syntax

```
clear web-authentication auth-state { user {<user name> | -all } | mac-address
<mac> } [-f]
```

Input mode

Administrator mode

Parameters

user { <user name> | -all }

<user name>

Forces user logout by specifying an authenticated, currently logged-in user.

Specify a user name with 1 to 16 characters. You can use alphanumeric characters and some symbols. However, you cannot use the following characters:

!!, space, two-byte characters, double-quotation mark ("), ampersand (&), left curly bracket ({), right curly bracket (}), bracket ((and)), single-quotation mark ('), semicolon (;), dollar sign (\$), grave accent mark (`), backslash (\), sharp sign (#) at the beginning, and percent sign (%).

-all

Forcibly logs out the authenticated, currently logged-in users.

mac-address <mac>

<mac>

Forces user logout by specifying the MAC address that is used by the authenticated, currently logged-in user.

Specify the MAC address in the range from 0000.0000.0000 to feff.ffff.ffff. Note that you cannot specify a multicast MAC address (address in which the lowest bit of the first byte is 1).

-f

Forces user logout without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

- When forcing logout of authenticated, currently logged-in user USER01:

```
# clear web-authentication auth-state user USER01
Logout user web-authentication. Are you sure? (y/n): y
```
- Forces logout of all authenticated, currently logged-in users:

```
# 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 6-23: List of response messages for the clear web-authentication auth-state command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart web-authentication</code> command to restart the Web authentication program.
Delete Error.	An attempt to delete a user failed.
The specified user is not login user.	The specified user is not a logged-in user.
WA is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

None

restart web-authentication

Restarts the Web authentication program and the Web server.

Syntax

```
restart web-authentication [-f] [{core-file | web-server}]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

{core-file | web-server}

core-file

Outputs the Web authentication core file and the Web server core file at restart.

web-server

Restart the Web server only.

Operation when this parameter is omitted:

Restarts the Web authentication program and the Web server. The core files are not output.

Example

The following shows an example of restarting the Web authentication program:

```
> restart web-authentication
WA restart OK? (y/n): y
```

Display items

None

Impact on communication

If `web-server` is specified for a parameter, only the Web server is restarted and authentication is not canceled. There is no impact on communication.

Note that if `web-server` is not specified, communication with the post-authentication VLAN is no longer possible because the Web authentication program is restarted, all authentications are canceled, and the MAC address is deleted from the post-authentication VLAN (MAC-VLAN).

Response messages

Table 6-24: List of response messages for the restart web-authentication command

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

Message	Description
WA is not configured.	<p>If Web authentication functionality has not been set, check the configuration.</p> <p>If the <code>web-authentication system-auth-control</code> configuration command has been set, perform the following operation:</p> <ul style="list-style-type: none">• Use the <code>no web-authentication system-auth-control</code> configuration command to stop Web authentication. Wait at least 10 seconds, and then use the <code>web-authentication system-auth-control</code> configuration command to restart Web authentication.

Notes

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

Storage directory: `/usr/var/core/`

Web authentication core file: `wad.core`

Web server core file: `httpd.core`

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

dump protocols web-authentication

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

Syntax

```
dump protocols web-authentication
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following shows an example of collecting Web authentication dump information:

```
> dump protocols web-authentication
```

Display items

None

Impact on communication

None

Response messages

Table 6-25: List of response messages for the dump protocols web-authentication command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart web-authentication</code> command to restart the Web authentication program.
WA is not configured.	The Web authentication functionality is not enabled. Check the configuration.

Notes

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

Storage directory: `/usr/var/wa/`

File: `wad_dump.gz`

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

set web-authentication html-files

Replaces the images for Web authentication pages (such as login and logout pages), the messages output for authentication errors, and the icons displayed in the **Favorites** menu of the Web browser.

When you execute this command, specify the name of the directory in which the page images, messages, or icons to be registered are stored. Page images (such as HTML or GIF files), messages, and icons to be registered must have been created and stored in any directory (such as the current directory) beforehand. Note that if you execute this command with the directory in which a new file is stored specified, all registered information will be cleared and overwritten with the new information.

Syntax

```
set web-authentication html-files <directory> [-f]
```

Input mode

Administrator mode

Parameters

<directory>

Specify the directory that stores 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 a directory according to the following conditions:

- Stores the above in a directory other than /config/wa/htdocs.
- There must be no subdirectories in the specified directory.
- There must be a login.html file in the specified directory.
- Specify the file names of the page images, messages, and icons to be registered as follows:

Login page: login.html

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.

-f

Replaces pages, messages, and icons without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

The following shows an example of registering Web authentication page images, messages, and

icons (when page images, messages, and icons to be registered are stored in the `k-html` directory):

```
# ls -l k-html
-rwxr-xr-x operator users 1108 Dec 6 09:59 login.html
-rwxr-xr-x operator users 1302 Dec 6 09:59 loginNG.html
-rwxr-xr-x operator users 1300 Dec 6 09:59 loginOK.html
-rwxr-xr-x operator users 843 Dec 6 09:59 logout.html
-rwxr-xr-x operator users 869 Dec 6 09:59 logoutNG.html
-rwxr-xr-x operator users 992 Dec 6 09:59 logoutOK.html
-rwxr-xr-x operator users 109 Dec 6 09:59 webauth.msg
-rwxr-xr-x operator users 199 Dec 6 09:59 favicon.ico
-rwxr-xr-x operator users 20045 Dec 6 09:59 aaa.gif

# set web-authentication html-files k-html
Would you wish to install new html-files ? (y/n):y
executing...
Install complete.
```

Display items

None

Impact on communication

None

Response messages

Table 6-26: List of response messages for the `set web-authentication html-files` command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't put a sub directory in the directory.	The specified directory contains a subdirectory.
Can't specify "/config/wa/htdocs" in this command.	The <code>/config/wa/htdocs</code> directory cannot be specified.
Directory size over.	The capacity of the specified directory exceeds the limit (1024 KB).
Installation on standby system failed (active system succeeded).	Although registration on the active system succeeded, registration on the standby system failed.
Install operation failed.	An attempt to register the file failed.
No login.html file in the directory.	There is no <code>login.html</code> file in the specified directory.
No such directory.	The specified directory does not exist.
Too many files.	The number of files exceeds the limit of 100.

Notes

- This command does not check the contents of the HTML files. If the contents of the specified file are incorrect, login and logout operations for Web authentication might not be possible.
- This command can be executed regardless of whether or not the configuration command for Web authentication has been set.
- If this command is executed during dual operation, page images, messages, and icons are registered automatically in the standby system. If you use the `synchronize` command to synchronize the information between the active and standby systems, the information will also be applied to the standby system.
- Page images, messages, and icons registered by using this command are retained when Web authentication is performed, the Web server is restarted, the Switch is restarted, and a switch

between the active and standby systems is performed.

- The total capacity of a file that can be registered is 1024 KB. If the capacity exceeds 1024 KB, the file cannot be registered.
- A maximum of 100 files can be registered. If there are too many files, command execution might take time.
- If this command is interrupted while it is being executed, the registered page is not displayed, but the default page is displayed. In addition, the result might not be displayed correctly by using the `show web-authentication html-files` command. If this happens, re-execute this command to register page images and messages.
- In dynamic VLAN mode or legacy mode, if the `loginOK.html` file contains a reference to another file, the login success window might not be displayed correctly.

clear web-authentication html-files

Deletes the Web authentication pages, messages, and icons registered by the `set web-authentication html-files` command, and reverts to the default settings.

Syntax

```
clear web-authentication html-files [-f]
```

Input mode

Administrator mode

Parameters

`-f`

Deletes the pages, messages, and icons without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

The following shows an example of deleting the registered html file:

```
# clear web-authentication html-files
Would you wish to clear registered html-files and initialize? (y/n):y
Clear complete.
```

Display items

None

Impact on communication

None

Response messages

Table 6-27: 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.
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Clear operation failed.	An attempt to delete the file failed.
Clear operation on standby system failed (active system succeeded).	Although deletion from the active system succeeded, deletion from the standby system failed.

Notes

- This command can be executed regardless of whether or not the configuration command for Web authentication has been set.
- If this command is executed during duplex operation, the file registered by using the `set web-authentication html-files` command is also deleted in the standby system. If you use the `synchronize` command to synchronize the information between the active and standby systems, the information will also be applied to the standby system.

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 registered by the `set web-authentication html-files` command and the date and time the file was registered.

■ When the file is registered:

```
# show web-authentication html-files
Date 2007/04/01 10:07:04 UTC
TOTAL SIZE      :      60775
-----
                SIZE      DATE
login.html      :      2049  2007/03/30 14:05
loginOK.html    :      1046  2007/03/30 14:05
loginNG.html    :       985  2007/03/30 14:05
logout.html     :       843  2007/03/30 14:05
logoutOK.html   :       856  2007/03/30 14:05
logoutNG.html   :       892  2007/03/30 14:05
webauth.msg     :        104  2007/03/30 14:05
favicon.ico     :          0  default now
the other files :     54000  2007/03/30 14:05
```

■ When the file is not registered (the default information is displayed):

```
# show web-authentication html-files
Date 2007/04/01 10:07:04 UTC
TOTAL SIZE      :      5730
-----
                SIZE      DATE
login.html      :      1108  default now
loginOK.html    :      1046  default now
loginNG.html    :       985  default now
logout.html     :       843  default now
logoutOK.html   :       856  default now
logoutNG.html   :       892  default now
webauth.msg     :          0  default now
favicon.ico     :          0  default now
the other files :          0  default now
```

■ When the file is registered (information about individual files that are not the HTML file, msg

file, or ico file is displayed):

```
# show web-authentication html-files detail
```

```
Date 2007/04/01 10:07:04 UTC
```

```
TOTAL SIZE      :      60775
```

```
-----
              SIZE      DATE
login.html    :      2049    2007/03/30 14:05
loginOK.html  :      1046    2007/03/30 14:05
loginNG.html  :       985    2007/03/30 14:05
logout.html   :       843    2007/03/30 14:05
logoutOK.html :       856    2007/03/30 14:05
logoutNG.html :       892    2007/03/30 14:05
webauth.msg   :       104    2007/03/30 14:05
favicon.ico   :         0    default now
aaa.gif       :     20000    2007/03/30 14:05
bbb.gif       :     15000    2007/03/30 14:05
ccc.gif       :     10000    2007/03/30 14:05
ddd.gif       :       9000    2007/03/30 14:05
```

Display items

None

Impact on communication

None

Response messages

Table 6-28: 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.
Can't execute this command in standby system.	This command cannot be executed on a standby system.

Notes

This command can be executed regardless of whether or not the configuration command for Web authentication has been set.

Chapter

7. MAC-based Authentication

```
show mac-authentication login
show mac-authentication logging
show mac-authentication
show mac-authentication statistics
clear mac-authentication auth-state
clear mac-authentication logging
clear mac-authentication statistics
set mac-authentication mac-address
remove mac-authentication mac-address
commit mac-authentication
show mac-authentication mac-address
store mac-authentication
load mac-authentication
restart mac-authentication
dump protocols mac-authentication
```

show mac-authentication login

Displays the authenticated, currently logged-in terminals in ascending order by login date and time.

Syntax

```
show mac-authentication login
```

Input mode

Administrator mode

Parameters

None

Example

The following shows an example of displaying authenticated MAC addresses:

```
# show mac-authentication login
Date 2010/04/01 10:52:49 UTC
Total client counts:2
MAC address      Port      VLAN      Login time      Limit time      Mode
0012.e200.0001   1/1       3          2010/04/01 09:58:04 UTC  00:10:20       Static
0012.e200.0002   1/10      4094       2010/04/01 10:10:23 UTC  00:20:35       Dynamic
```

Display items

The following table describes the items displayed for authenticated MAC addresses.

Table 7-1: Items displayed for authenticated MAC addresses

Item	Meaning	Displayed information
Total client counts	Total number of terminals	The number of authenticated, currently logged-in terminals
MAC address	MAC address	The MAC addresses of authenticated, currently logged-in terminals
Port	Port number	The physical port numbers of the ports where the authenticated, currently logged-in terminal is located
VLAN	VLAN	VLANs set for the authenticated, currently logged-in terminals. VLANs that were switched after authentication in dynamic VLAN mode.
Login time	Login date and time	Login times of the authenticated, currently logged-in terminals
Limit time	Remaining login time	Remaining login time of the authenticated, currently logged-in terminals. When a user is logged in, the remaining time might be displayed as 00:00:00 immediately before the user is logged out due to a timeout. When the maximum connection time is from 10 to 1440 (minutes): hh:mm:ss hour:minute:second When the maximum connection time is set to unlimited: infinity

Item	Meaning	Displayed information
Mode	Operating mode	Authenticated mode. Static: Authenticated in fixed VLAN mode Dynamic: Authenticated in dynamic VLAN mode

Impact on communication

None

Response messages

Table 7-2: List of response messages for the show mac-authentication login command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed.
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.
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 program.

Syntax

```
show mac-authentication logging [client]
```

Input mode

Administrator mode

Parameters

client

Specify the type of operation log message to be displayed.

If this parameter is specified, terminal authentication information is displayed.

Operation when this parameter is omitted:

Displays the operation log of the MAC-based authentication program and the terminal authentication information in chronological order.

Example

The following examples show operation log messages displayed for MAC-based authentication.

■ When the parameter is omitted:

```
# show mac-authentication logging
Date 2007/12/01 10:52:49 UTC
No=1:Dec 1 10:09:50:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=1/1 VLAN=3 Login
succeeded.
No=2:Dec 1 10:10:10:NORMAL:LOGOUT: MAC=0012.e212.0001 PORT=1/1 VLAN=3
Logout succeeded.
No=82:Dec 1 10:10:55:NORMAL:SYSTEM: accepted clear auth-state command.
```

■ When client is specified for the parameter:

```
# show mac-authentication logging client
Date 2007/12/01 11:13:15 UTC
No=1:Dec 1 10:09:50:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=1/1 VLAN=3 Login
succeeded.
No=2:Dec 1 10:10:10:NORMAL:LOGOUT: MAC=0012.e212.0001 PORT=1/1 VLAN=3
Logout succeeded.
```

Display items

The following table describes the items displayed for MAC-based authentication operation log messages.

Table 7-3: Items displayed for MAC-based authentication operation log messages

Item	Meaning	Displayed information
Level	Levels of operation log messages	Severity of a log message
<log>	Operation log message	Contents of a registered operation log message

The following shows the display format of a message.

```
No=1:Dec 1 10:09:50:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=1/1 VLAN=3 Login succeeded.
(1) (2) (3) (4) (5) (6) (7)
```

(1) Message number: Indicates the number assigned to each message shown in

Table 7-6: List of operation log messages.

- (2) Date: Indicates the date recorded in the MAC-based authentication program.
- (3) Time: Indicates the time recorded in the MAC-based authentication program.
- (4) Log ID: Indicates the level of the operation log message.
- (5) Log type: Indicates the type of operation that outputs the log message.
- (6) Additional information: Indicates supplementary information provided in the message.
- (7) Message body

Operation log messages show the following information:

- Log ID: See *Table 7-4: Log ID and type in operation log messages*.
- Log type: See *Table 7-4: Log ID and type in operation log messages*.
- Additional information: See *Table 7-5: Additional information*.
- List of messages: See *Table 7-6: List of operation log messages*.

Table 7-4: Log ID and type in operation log messages

Log ID	Log type	Meaning
NORMAL	LOGIN	Indicates that authentication was successful.
	LOGOUT	Indicates that authentication was canceled.
	SYSTEM	Indicates a runtime notification.
NOTICE	LOGIN	Indicates that authentication failed.
	LOGOUT	Indicates that cancelation of authentication was failed.
ERROR	SYSTEM	Indicates a communication failure or an operation failure in the MAC-based authentication program.

Table 7-5: Additional information

Display format	Meaning
MAC=xxx.xxxx.xxxx	Indicates the MAC address.
VLAN=xxx	Indicates the VLAN ID. Note, however, that this is not displayed if VLAN ID information could not be acquired.
PORT=xx/xx	Indicates the port number.

Table 7-6: List of operation log messages

#	Log ID	Log type	Message text	Meaning and action	Additional information
1	NORMAL	LOGIN	Login succeeded.	[Meaning] The terminal was successfully authenticated. [Action] None	MAC address VLAN ID Port number

7. MAC-based Authentication

#	Log ID	Log type	Message text	Meaning and action	Additional information
2	NORMAL	LOGOUT	Force logout ; Port link down.	[Meaning] Authentication was canceled because the link for the relevant port went down. [Action] Make sure the status of relevant port is link-up.	MAC address VLAN ID Port number
3	NORMAL	LOGOUT	Force logout ; Authentic method changed (RADIUS <-> Local).	[Meaning] Authentication was canceled because of a switch between the RADIUS authentication and local authentication methods. [Action] None	MAC address VLAN ID Port number
4	NORMAL	LOGOUT	Force logout ; Clear mac-authentication command succeeded.	[Meaning] Authentication was canceled by an operation command. [Action] None	MAC address VLAN ID Port number
5	NORMAL	LOGOUT	Force logout ; Connection time was beyond a limit.	[Meaning] Authentication was canceled because the maximum connection time was exceeded. [Action] None If the terminal is connected, authentication is attempted again.	MAC address VLAN ID Port number
6	NOTICE	LOGIN	Login failed ; Port link down.	[Meaning] An authentication error occurred because the port was down. [Action] Make sure the status of relevant port is link-up.	MAC address VLAN ID Port number
7	NOTICE	LOGIN	Login failed ; Port not specified.	[Meaning] An authentication error occurred because the authentication request was sent from a port that was not set as a MAC-based authentication port. [Action] Make sure the terminal is connected to the correct port. If there are no problems with the connection, check the configuration.	MAC address VLAN ID Port number

#	Log ID	Log type	Message text	Meaning and action	Additional information
8	NOTICE	LOGIN	Login failed ; VLAN not specified.	<p>[Meaning] An authentication error occurred because the authentication request was sent from a VLAN that does not exist on the port.</p> <p>[Action] Make sure the terminal is connected to the correct port. If there are no problems with the connection, check the configuration.</p>	MAC address VLAN ID Port number
9	NORMAL	LOGOUT	Force logout ; Program stopped.	<p>[Meaning] Authentication of all users was canceled because the MAC-based authentication program stopped.</p> <p>[Action] To subsequently perform MAC-based authentication, set the configuration.</p>	MAC address VLAN ID Port number
10	NORMAL	LOGOUT	Force logout ; Other authentication program.	<p>[Meaning] Authentication was canceled because it was overwritten by another authentication operation.</p> <p>[Action] Check whether another authentication operation was performed on the same terminal.</p>	MAC address VLAN ID Port number
11	NORMAL	LOGOUT	Force logout ; VLAN deleted.	<p>[Meaning] Authentication was canceled because the VLAN for the authentication port was changed.</p> <p>[Action] Check the VLAN configuration.</p>	MAC address VLAN ID Port number
12	NORMAL	LOGOUT	Force logout ; Client moved.	<p>[Meaning] The old authenticated state was canceled because the authenticated terminal was connected to another port.</p> <p>[Action] None Authentication is performed again.</p>	MAC address VLAN ID Port number

#	Log ID	Log type	Message text	Meaning and action	Additional information
13	NOTICE	LOGIN	Login failed ; Double login. (L2MacManager)	<p>[Meaning] The VLAN program reported that authentication was not possible (because duplicate MAC addresses were registered).</p> <p>[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.</p>	MAC address VLAN ID Port number
14	NOTICE	LOGIN	Login failed ; Double login.	<p>[Meaning] Authentication could not be performed because of duplicate registration.</p> <p>[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.</p>	MAC address
15	NOTICE	LOGIN	Login failed ; Number of login was beyond limit.	<p>[Meaning] Authentication could not be performed because the maximum login limit was exceeded. The cause is either of the following:</p> <ul style="list-style-type: none"> • The capacity limit for MAC-based authentication has already been exceeded. • The total number of IEEE 802.1X authentications, Web authentications, and MAC-based authentications exceeded the capacity limit. <p>[Action] Attempt authentication again when the number of authentications drops low enough.</p>	MAC address

#	Log ID	Log type	Message text	Meaning and action	Additional information
17	NOTICE	LOGOUT	Logout failed ; L2MacManager failed.	[Meaning] Deletion failed because the user was not being authenticated by MAC-based authentication. [Action] Check whether the MAC address has already been authenticated.	MAC address VLAN ID Port number
18	NOTICE	LOGIN	Login failed ; MAC address could not register. [error-code]	[Meaning] Authentication could not be performed because registration of the MAC address failed. [Action] Attempt authentication again.	MAC address error code
19	NOTICE	LOGOUT	Logout failed ; MAC address could not delete. [error-code]	[Meaning] An attempt to delete MAC address failed. [Action] Attempt de-authentication again.	MAC address ^{#1} VLAN ID ^{#1} Port number ^{#1} error code
20	NOTICE	LOGIN	Login failed ; RADIUS authentication failed.	[Meaning] Authentication could not be performed because RADIUS authentication failed. [Action] Make sure the terminal to be authenticated is correct. Also make sure the RADIUS definition is correct.	MAC address VLAN ID Port number
21	NOTICE	LOGIN	Login failed ; Failed to connection to RADIUS server.	[Meaning] Authentication failed because an attempt to communicate with the RADIUS server failed. [Action] Check whether communication is possible between the Switch and the RADIUS server. After the Switch can communicate with the RADIUS server, attempt authentication again.	MAC address VLAN ID Port number

#	Log ID	Log type	Message text	Meaning and action	Additional information
22	NOTICE	LOGIN	Login failed ; Connection failed L2MacManager.	[Meaning] Authentication failed because an attempt to communicate with the VLAN program failed. [Action] Attempt authentication again. If this message appears frequently, specify the <code>mac-manager</code> parameter for the <code>restart vlan</code> command and execute it.	MAC address
28	NORMAL	LOGOUT	Force logout ; Port not specified.	[Meaning] Authentication was canceled because the setting was deleted from the port. [Action] Check the configuration.	MAC address VLAN ID Port number
29	NOTICE	LOGIN	Login failed ; Port number failed.	[Meaning] Authentication is impossible because port number acquisition failed. [Action] Attempt authentication again.	MAC address Port number
30	NORMAL	LOGOUT	Force logout ; mac-address-table aging.	[Meaning] Authentication was canceled because a MAC address was deleted due to MAC address table aging. [Action] The terminal is not in use. Check the terminal.	MAC address VLAN ID Port number
31	NORMAL	LOGOUT	Force logout ; Authentic mode had changed (dynamic vlan -> static vlan).	[Meaning] All authentications were canceled because authentication mode changed from dynamic VLAN mode to fixed VLAN mode. [Action] None	MAC address VLAN ID Port number
32	NORMAL	LOGOUT	Force logout ; Authentic mode had changed (static vlan -> dynamic vlan).	[Meaning] All authentications were canceled because authentication mode changed from fixed VLAN mode to dynamic VLAN mode. [Action] None	MAC address VLAN ID Port number

#	Log ID	Log type	Message text	Meaning and action	Additional information
34	NORMAL	LOGIN	Un-authorized Port Accepted.	[Meaning] Communication with an unauthorized terminal was detected. [Action] None	MAC address VLAN ID Port number
82	NORMAL	SYSTEM	Accepted clear auth-state command.	[Meaning] A notification issued by the <code>clear mac-authentication auth-state</code> command for forced logout was received. [Action] None	n/a
83	NORMAL	SYSTEM	Accepted clear statistics command.	[Meaning] A request issued by the <code>clear mac-authentication statistics</code> command for deleting statistics was received. [Action] None	n/a
84	NORMAL	SYSTEM	Accepted commit command.	[Meaning] A notification issued by the <code>commit mac-authentication</code> command for re-configuring the authentication information was received. [Action] None	n/a
85	NORMAL	SYSTEM	Accepted dump command.	[Meaning] A dump output request issued by the <code>dump protocols mac-authentication</code> command was received. [Action] None	n/a
86	NORMAL	LOGOUT	Force logout ; MAC address not found L2MacManager.	[Meaning] An attempt to register a MAC address in the VLAN program was made because the MAC address exists on MAC-based authentication but not in the VLAN program. However, authentication was canceled because the registration attempt failed. [Action] Attempt authentication again.	MAC address VLAN ID Port number

#	Log ID	Log type	Message text	Meaning and action	Additional information
88	ERROR	SYSTEM	Macauthd could not initialize.[error-code]	<p>[Meaning] Initializing the MAC-based authentication program failed.</p> <p>[Action] Check the configurations of MAC-based authentication. If this message appears frequently, use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.</p>	error code
89	ERROR	SYSTEM	Connection failed ; Operation command. error=[error-code]	<p>[Meaning] Outputting the response message for the command failed.</p> <p>[Action] Wait a while, and then re-execute the command.</p>	error code
90	ERROR	SYSTEM	Connection failed ; L2MacManager.	<p>[Meaning] An attempt to communicate with the VLAN program was made, but failed.</p> <p>[Action] If this message appears frequently, specify the <code>mac-manager</code> parameter for the <code>restart vlan</code> command and execute it.</p>	n/a
92	ERROR	SYSTEM	Disconnection failed ; L2MacManager.	<p>[Meaning] Communication with the VLAN program was interrupted.</p> <p>[Action] If this message appears frequently, specify the <code>mac-manager</code> parameter for the <code>restart vlan</code> command and execute it.</p>	n/a
93	ERROR	SYSTEM	Program failed ; Configuration command. [error-code]	<p>[Meaning] An attempt to read the configuration failed.</p> <p>[Action] Use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.</p>	error code

#	Log ID	Log type	Message text	Meaning and action	Additional information
94	ERROR	SYSTEM	Program failed ; Internal data update. [error-code]	[Meaning] An attempt to update the internal table for the configuration failed. [Action] Use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.	error code
95	ERROR	SYSTEM	Program failed ; Login information could not create. [error-code]	[Meaning] Creation of login information failed. [Action] Use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.	error code
96	ERROR	SYSTEM	Program failed ; Login information could not delete.	[Meaning] An attempt to delete the login information failed. [Action] Use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.	n/a
99	ERROR	SYSTEM	Accounting failed ; RADIUS accounting.	[Meaning] A response to an accounting request was not received from the RADIUS server. [Action] Check whether communication is possible between the Switch and the RADIUS server. After the Switch can communicate with the RADIUS server, attempt authentication again.	MAC address
100	NORMAL	SYSTEM	Accepted clear logging command.	[Meaning] A request to delete the operation log by the <code>clear mac-authentication logging</code> command was received. [Action] None	n/a
101	NOTICE	SYSTEM	Change to redundancy mode (SBY -> ACT).	[Meaning] The MAC-based authentication program was switched from standby mode to active mode. [Action] None	n/a

7. MAC-based Authentication

#	Log ID	Log type	Message text	Meaning and action	Additional information
102	NOTICE	SYSTEM	Change to redundancy mode (ACT -> SBY).	[Meaning] The MAC-based authentication program was switched from active mode to standby mode. [Action] None	n/a
103	NORMAL	SYSTEM	Synchronized ; Macauthd -> L2MacManager.	[Meaning] The authentication status was registered in the hardware because a difference with the hardware was found. [Action] No action is required because the authentication status and the hardware status can be synchronized by MAC-based authentication.	MAC address
105	NOTICE	LOGIN	Login failed ; VLAN suspended.	[Meaning] An authentication error occurred because the VLAN was disabled. [Action] Enable the VLAN, and then attempt authentication again.	MAC address VLAN ID Port number
106	NORMAL	LOGOUT	Force logout ; VLAN suspended.	[Meaning] Authentication was canceled because the status of the VLAN changed to disable. [Action] Enable the VLAN, and then attempt authentication again.	MAC address VLAN ID Port number
107	NOTICE	LOGIN	Login failed ; MAC address not found to MAC authentication DB.	[Meaning] Authentication failed because the MAC address to be authenticated was not registered in the internal MAC-based authentication DB. [Action] Make sure the MAC address registered in the internal MAC-based authentication DB is correct.	MAC address VLAN ID ^{#2}

#	Log ID	Log type	Message text	Meaning and action	Additional information
108	NOTICE	LOGIN	Login failed ; VLAN ID not found to MAC authentication DB.	<p>[Meaning] Authentication failed because the VLAN ID to be authenticated was not registered in the internal MAC-based authentication DB.</p> <p>[Action] Make sure the VLAN ID registered in the internal MAC-based authentication DB is correct.</p>	MAC address VLAN ID
255	ERROR	SYSTEM	The other error. [error-code]	<p>[Meaning] An internal MAC-based authentication error occurred. Communication failed with an internal functionality indicated by the error code in [] after The other error..</p> <p>[Action] An internal error of the MAC-based authentication program occurred. Use the <code>dump protocols mac-authentication</code> command to collect information, and then use the <code>restart mac-authentication</code> command to restart MAC-based authentication.</p>	error code

Legend n/a: Not applicable

#1: Displayed if logout failed during logout processing caused by port down, VLAN suspend, or specification by a user using an operation command.

#2: Displayed for fixed VLAN mode only.

Impact on communication

None

Response messages

Table 7-7: List of response messages for the show mac-authentication logging command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed.
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.
Mac-authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

Notes

- MAC-based authentication operation log messages are displayed with newer messages displayed first.
- For duplex configuration, operation log information is deleted on transfer between active and standby, rather than being inherited.

show mac-authentication

Displays the configuration for MAC-based authentication.

Syntax

```
show mac-authentication
```

Input mode

Administrator mode

Parameters

None

Example

The following examples show configuration information displayed for MAC-based authentication.

- When a port for MAC-based authentication is not registered:

```
# show mac-authentication
Date 2010/04/15 10:52:49 UTC
mac-authentication Information:
  Authentic-method : RADIUS           Accounting-state : disable
  Syslog-send      : enable

  Authentic-mode   : Static-VLAN
    Max-timer      : 60                Max-terminal   : 4096
    Port Count     : 0                Auto-logout    : enable
  VLAN-check       : enable
  Vid-key          : %VLAN

  Authentic-mode   : Dynamic-VLAN
    Max-timer      : 60                Max-terminal   : 4096
    Port Count     : 0                Auto-logout    : enable
```

- When a port for MAC-based authentication is registered:

```
# show mac-authentication
Date 2010/04/15 10:52:49 UTC
mac-authentication Information:
  Authentic-method : RADIUS           Accounting-state : disable
  Syslog-send      : enable

  Authentic-mode   : Static-VLAN
    Max-timer      : 60                Max-terminal   : 4096
    Port Count     : 1                Auto-logout    : enable
  VLAN-check       : enable
  Vid-key          : %VLAN
  Access-list-No   : 100

  Authentic-mode   : Dynamic-VLAN
    Max-timer      : 60                Max-terminal   : 4096
    Port Count     : 1                Auto-logout    : enable
  Access-list-No   : 100

Port Information:
  Port              :      1/2
    Dynamic-VLAN
      VLAN ID       :    1300-1310
      Native VLAN    :    1000

  Port              :      1/10
    Static-VLAN
      VLAN ID       :    300,305
```

Display items

Table 7-8: Items displayed for the configuration of MAC-based authentication

Item	Meaning	Displayed information
Authentic-method	Authentication method	Authentication method for the MAC-based authentication functionality. Local: Indicates local authentication RADIUS: Indicates RADIUS authentication
Accounting-state	Whether the accounting server is available	Whether the accounting server is available for the MAC-based authentication functionality. enable: An accounting server is available. disable: An accounting server is not available.
Syslog-send	The usage state of the syslog server output functionality	The usage state of the functionality for outputting the MAC-based authentication operation log to the syslog server. enable: Used disable: Not used
Authentic-mode	Authentication mode	Authentication mode for the MAC-based authentication functionality. Static-VLAN: Indicates fixed VLAN mode Dynamic-VLAN: Indicates dynamic VLAN mode
Max-timer	Maximum connection time	Maximum connection time (in minutes) for a login terminal
Max-terminal	Maximum number of authenticated terminals	Maximum number of authentication terminals that can simultaneously login to the MAC-based authentication functionality.
Port Count	Total number of ports	Total number of ports registered for MAC-based authentication
Auto-logout	Auto-logout setting for when no accesses detected status continues	The status of the auto-logout functionality when continuing no access status is detected for a MAC address. enable: The auto-logout functionality is enabled when the no access status is detected. disable: The auto-logout functionality is disabled even if the no access status is detected.
VLAN-check	Whether VLAN ID matching is required for authentication.	Whether VLAN ID matching is required or not when authentication is performed by MAC-based authentication functionality. enable: The VLAN ID is checked. disable: The VLAN ID is not checked.
Vid-key	Character string to be added to the account name when RADIUS authentication is performed.	Character strings to be added to the account name when authentication request is sent to the RADIUS server.
Access-list-No	Access Lists	The access list number or the access list name. - is displayed if neither is specified.
Port	Port information	The number of the port registered for MAC-based authentication
VLAN ID	VLAN information	The ID of the VLAN to which a port, which is registered for MAC-based authentication, belongs.

Item	Meaning	Displayed information
Native VLAN	VLAN ID of a native VLAN	The VLAN ID of the native VLAN set for the port for dynamic VLAN mode

Impact on communication

None

Response messages

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

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed.
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.
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 2010/04/01 11:10:49 UTC
mac-authentication Information:
  Authentication Request Total :      100
  Authentication Current Count :       10
  Authentication Error Total   :       30
RADIUS mac-authentication Information:
[RADIUS frames]
  TxTotal   :      10  TxAccReq :      10  TxError   :      0
  RxTotal   :      30  RxAccAccpt:     10  RxAccRejct:    10
                        RxAccChllg:     10  RxInvalid :      0
Account mac-authentication Information:
[Account frames]
  TxTotal   :      10  TxAccReq :      10  TxError   :      0
  RxTotal   :      20  RxAccResp :     10  RxInvalid :      0
```

Display items

Table 7-10: Items displayed for MAC-based authentication statistics

Item	Meaning
Authentication Request Total	The total number of authentication requests
Authentication Current Count	The number of currently authenticated terminals
Authentication Error Total	The total number of authentication request errors
RADIUS frames	RADIUS information
TxTotal	The total number of packets transmitted to the RADIUS server
TxAccReq	The total number of Access-Request packets sent to the RADIUS server
TxError	The number of errors occurring during transmission to the RADIUS server
RxTotal	The total number of received packets from the RADIUS server
RxAccAccpt	The total number of Access-Accept packets received from the RADIUS server
RxAccRejct	The total number of Access-Reject packets received from the RADIUS server
RxAccChllg	The total number of Access-Challenge packets received from the RADIUS server

Item	Meaning
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 7-11: List of response messages for the show mac-authentication statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed.
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.
Mac-authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

Notes

None

clear mac-authentication auth-state

Specify the MAC address to forcibly log out the specific authentication terminal.

In addition, you can forcibly log out all the authenticated, currently logged-in terminals.

Syntax

```
clear mac-authentication auth-state mac-address {<mac> | -all} [-f]
```

Input mode

Administrator mode

Parameters

mac-address {<mac> | -all}

<mac>

Forcibly logs out the authenticated terminal that has the MAC address specified by <mac>.

Specify the MAC address in the range from 0000.0000.0000 to feff.ffff.ffff. Note that you cannot specify a multicast MAC address (address in which the lowest bit of the first byte is 1).

-all

Forcibly logs out all the authenticated, currently logged-in terminals.

-f

Forcibly logs out terminals without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

The following show examples of forcibly logging out all the authenticated, currently logged in terminals.

- When forcibly logging out the authenticated, currently logged in terminals by specifying the MAC address (0012.e200.0001):

```
# clear mac-authentication auth-state mac-address 0012.e200.0001
Logout client mac-authentication of specified MAC address. Are you sure? (y/n): y
```
- When forcibly logging out all the authenticated, currently logged in terminals:

```
# clear mac-authentication auth-state mac-address -all
Logout all client mac-authentication. Are you sure? (y/n): y
```

Display items

None

Impact on communication

Authentication for the specified terminal will be canceled.

Response messages

Table 7-12: List of response messages for the clear mac-authentication auth-state command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed.
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.
Delete Error.	An attempt to delete the terminal failed.
Mac-authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

Notes

None

clear mac-authentication logging

Clears the 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 log information for MAC-based authentication:

```
# clear mac-authentication logging
```

Display items

None

Impact on communication

None

Response messages

Table 7-13: List of response messages for the clear mac-authentication logging command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed.
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.
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 7-14: List of response messages for the clear mac-authentication statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed.
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.
Mac-authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

Notes

None

set mac-authentication mac-address

Adds a MAC address for MAC-based authentication to the internal MAC-based authentication DB. Specify the VLAN ID to which the user belongs. You can add a MAC address that has already been registered if its VLAN ID is different from that already registered.

At least one VLAN ID must be specified if you use this command in dynamic VLAN mode because a VLAN ID is changed to the specified VLAN ID by using this command after authentication in dynamic VLAN mode.

To apply the setting to the internal MAC-based authentication DB, execute the `commit mac-authentication` command.

Syntax

```
set mac-authentication mac-address <mac> [<vlan id>]
```

Input mode

Administrator mode

Parameters

<mac>

Specify the MAC address to be registered.

Specify the MAC address in the range from 0000.0000.0000 to feff.ffff.ffff. Note that you cannot specify a multicast MAC address (address in which the lowest bit of the first byte is 1).

<vlan id>

Specify the VLAN ID of the VLAN to which the user will communicate after authentication.

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

In dynamic VLAN mode, you must specify at least one VLAN ID for each MAC address. Also, in dynamic VLAN mode, if you specify 1 as the VLAN ID, an authentication error occurs because that VLAN cannot be used as the post-authentication VLAN.

Operation when this parameter is omitted:

The VLAN ID is not checked at authentication time.

In dynamic VLAN mode, an authentication error occurs during authentication for the specified MAC address.

Example

To add 0012.e200.1234 as the MAC address and 10 as the VLAN ID:

```
# set mac-authentication mac-address 0012.e200.1234 10
```

Display items

None

Impact on communication

None

Response messages

Table 7-15: List of response messages for the set mac-authentication mac-address command

Message	Description
Already mac address "<mac>","<vlan id>" exists.	The specified MAC address has already been registered.
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Mac-authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.
Now another user is using mac-authentication command, please try again.	Another user is using a command related to the MAC-based authentication functionality. Wait a while, and then retry the operation.
The number of client exceeds 1024.	The number of registered MAC addresses exceeds the capacity limit.

Notes

- This command cannot be used concurrently by multiple users.
- The setting is applied to the internal MAC-based authentication DB only when the `commit mac-authentication` command is executed.
- When using the command in dynamic VLAN mode, note the following and specify <vlan id>:
 - When the same MAC address is registered to multiple VLAN IDs, the VLAN ID that has the smallest number is used for matching.
 - When the VLAN ID is omitted, an authentication error occurs at terminal authentication time because the VLAN ID after switching cannot be determined.
 - For a given MAC address, if it is registered both with no associated VLAN ID and with an associated VLAN ID, then this is taken to be no VLAN ID specified, and an authentication error occurs at terminal authentication time.
 - When 1 is specified as the VLAN ID, an authentication error occurs at terminal authentication time.

remove mac-authentication mac-address

Deletes MAC addresses, for MAC-based authentication, from the internal MAC-based authentication DB. Regardless of any associated VLAN ID, as long as the MAC address is the same as the specified MAC address, the MAC address is deleted.

To apply the setting to the authentication information, execute the `commit mac-authentication` command.

Syntax

```
remove mac-authentication mac-address {<mac> | -all} [-f]
```

Input mode

Administrator mode

Parameters

<mac>

Deletes the specified MAC address.

Specify the MAC address in the range from 0000.0000.0000 to feff.ffff.ffff. Note that you cannot specify a multicast MAC address (address in which the lowest bit of the first byte is 1).

-all

Deletes all MAC addresses.

-f

Deletes 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
```
- When deleting all MAC addresses registered in the local authentication data:

```
# remove mac-authentication mac-address -all
Remove all mac-authentication mac-address. Are you sure? (y/n): y
```

Display items

None

Impact on communication

None

Response messages

Table 7-16: List of response messages for the `remove mac-authentication mac-address` command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Mac-authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.
Now another user is using mac-authentication command, please try again.	Another user is using a command related to the MAC-based authentication functionality. Wait a while, and then retry the operation.
Unknown mac-address '<mac>'.	The specified MAC address has not been registered.

Notes

The setting is applied to the internal MAC-based authentication DB only when the `commit mac-authentication` command is executed.

commit mac-authentication

Saves the internal MAC-based authentication DB for MAC-based authentication to the internal flash memory.

The contents of the internal MAC-based authentication DB which is being used is not overwritten unless this command is executed after the following commands are executed to add or delete MAC addresses:

- set mac-authentication mac-address
- remove mac-authentication mac-address

Syntax

commit mac-authentication [-f]

Input mode

Administrator mode

Parameters

-f

Stores the internal MAC-based authentication DB for MAC-based authentication to internal flash memory without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

The following shows an example of saving the internal MAC-based authentication DB for MAC-based authentication:

```
# commit mac-authentication
Commitment mac-authentication mac-address data. Are you sure? (y/n): y
Commit complete.
```

Display items

None

Impact on communication

None

Response messages

Table 7-17: List of response messages for the commit mac-authentication command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can not commit.	An attempt to update the authentication information failed. Execute the <code>restart mac-authentication</code> command to update the authentication information again.
Can't execute.	The command could not be executed. Re-execute the command.
Command information was damaged.	Information was discarded because the execution information is corrupted.

Message	Description
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.
Mac-authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.
Now another user is using mac-authentication command, please try again.	Another user is using a command related to the MAC-based authentication functionality. Wait a while, and then retry the operation.

Notes

- The information in the internal MAC-based authentication DB which is being used is modified only when this command is executed.
- If execution of this command is interrupted before completion, the MAC-based authentication database is not updated. In such a case, re-execute the command to update the MAC-based authentication database.

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 of MAC addresses.

Syntax

```
show mac-authentication mac-address {edit | commit}
```

Input mode

Administrator mode

Parameters

{edit | commit}

edit

Displays information that is being edited.

commit

Displays information about the current internal MAC-based authentication DB.

Example

- When displaying information that is being edited:

```
# show mac-authentication mac-address edit
Date 2007/12/01 10:52:49 UTC
Total mac-address counts:2
mac-address          VLAN
0012.e200.1234       3
0012.e201.abcd       4094
```

- When displaying information about the current internal MAC-based authentication DB:

```
# show mac-authentication mac-address commit
Date 2007/12/01 10:52:49 UTC
Total mac-address counts:3
mac-address          VLAN
0012.e200.1234       4
0012.e201.abcd       4094
0012.e202.6789       2
```

Display items

Table 7-18: Items displayed for MAC-based authentication registration information

Item	Meaning	Displayed information
Total mac-address counts	The total number of registered MAC addresses	The number of registered MAC addresses
mac-address	MAC address	Registered MAC address
VLAN	VLAN	The VLAN set for a registered MAC address.

Impact on communication

None

Response messages*Table 7-19:* List of response messages for the show mac-authentication mac-address command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Mac-authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.
Now another user is using mac-authentication command, please try again.	Another user is using a command related to the MAC-based authentication functionality. Wait a while, and then retry the operation.

Notes

None

store mac-authentication

Backs up the internal MAC-based authentication DB to files.

Syntax

```
store mac-authentication <file name> [-f]
```

Input mode

Administrator mode

Parameters

<file name>

Specify the name of a file to which the internal MAC-based authentication DB is to be backed up.

-f

Backs up the internal MAC-based authentication DB to files without displaying confirmation messages.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

When creating the authdata backup file for the internal MAC-based authentication DB:

```
# store mac-authentication authdata
Backup mac-authentication MAC address data. Are you sure? (y/n): y
Backup complete.
```

Display items

None

Impact on communication

None

Response messages

Table 7-20: List of response messages for the store mac-authentication command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Mac-authentication command is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.
Now another user is using mac-authentication command, please try again.	Another user is using a command related to the MAC-based authentication functionality. Wait a while, and then retry the operation.
Store operation failed.	Restoration from the backup file failed.

Notes

If the internal MAC-based authentication DB is backed up when the flash memory capacity is insufficient, incomplete backup files might be created. When creating backup files, use the `show flash` command to make sure there is enough free capacity in the flash memory.

The following shows an example of executing the `show flash` command:

```
> show flash
Date 2007/12/01 19:46:29 JST
Flash :
      user area   config area   dump area   area total
used   37,063kB      65kB        16kB      37,144kB
free    616kB       7,199kB      8,152kB     15,967kB
total  37,679kB      7,265kB      8,168kB     53,112kB
```

Note: The underlined part (the value for `free` indicating the free capacity of the user area) must be at least 100 KB.

If the free capacity in flash memory is insufficient, use the `rm` command to delete unnecessary files before creating the backup files.

load mac-authentication

Restores the internal MAC-based authentication DB from a backup file to the internal MAC-based authentication DB. Note that the contents registered or changed by the following commands will be replaced by the contents of the restored backup:

- set mac-authentication mac-address
- remove mac-authentication mac-address
- commit mac-authentication

Syntax

```
load mac-authentication <file name> [-f]
```

Input mode

Administrator mode

Parameters

<file name>

Specify the name of the backup file from which the internal MAC-based authentication DB is to be restored.

-f

Restores the internal MAC-based authentication DB without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

When restoring the internal MAC-based authentication DB from the `authdata` backup file:

```
# load mac-authentication authdata
Restore mac-authentication MAC address data. Are you sure? (y/n): y
Restore complete.
```

Display items

None

Impact on communication

None

Response messages

Table 7-21: List of response messages for the load mac-authentication command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can not load.	An attempt to update the internal MAC-based authentication DB failed. Execute the <code>restart mac-authentication</code> command, and then execute the <code>load mac-authentication</code> command again to restore the internal MAC-based authentication DB.
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.
File format error.	Registration is not possible because the file is not a backup file.
Load operation failed.	Restoration from the backup file failed.
Mac-authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.
Now another user is using mac-authentication command, please try again.	Another user is using a command related to the MAC-based authentication functionality. Wait a while, and then retry the operation.

Notes

- Note that the contents registered or changed by the following commands will be replaced by the contents of the restored backup:
 - `set mac-authentication mac-address`
 - `remove mac-authentication mac-address`
 - `commit mac-authentication`
- If execution of this command is interrupted before completion, the MAC-based authentication database is not updated. In such a case, re-execute the command to update the MAC-based authentication database.

restart mac-authentication

Restarts the MAC-based authentication program.

Syntax

```
restart mac-authentication [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs a core file for MAC-based authentication when the MAC-based authentication program is restarted.

Operation when this parameter is omitted:

A core file is not output.

Example

The following shows an example of restarting the MAC-based authentication program:

```
> restart mac-authentication
macauth restart OK? (y/n): y
```

Display items

None

Impact on communication

All authentications for authenticated, currently logged-in terminals are canceled and communication will be impossible.

After the MAC-based authentication program is restarted, you must perform authentication again.

Response messages

Table 7-22: List of response messages for the restart mac-authentication command

Message	Description
Can't execute.	The command could not be executed.
Mac-authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

Notes

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

- Storage directory: `/usr/var/core/`
- Core file for MAC-based authentication: `macauthd.core`

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

dump protocols mac-authentication

Outputs to a file detailed event trace information and control table information collected by the MAC-based authentication program.

Syntax

```
dump protocols mac-authentication
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following shows an example of dumping the MAC-based authentication information:

```
> dump protocols mac-authentication
```

Display items

None

Impact on communication

None

Response messages

Table 7-23: List of response messages for the dump protocols mac-authentication command

Message	Description
Can't execute.	The command could not be executed.
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.
Mac-authentication is not configured.	The MAC-based authentication functionality is not configured. Check the configuration.

Notes

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

- Storage directory: `/usr/var/macauth/`
- File: `macauthd_dump.gz`

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

Chapter

8. Authentication VLANs [OP-VAA]

```
show fense server [OP-VAA]
show fense statistics [OP-VAA]
show fense logging [OP-VAA]
clear fense statistics [OP-VAA]
clear fense logging [OP-VAA]
restart vaa [OP-VAA]
dump protocols vaa [OP-VAA]
```

show fense server [OP-VAA]

Displays information set for an authentication VLAN, and the operating status of the current VLANaccessAgent.

Syntax

```
show fense server [id <id no list>] [detail [<vlan id list>]]
```

Input mode

User mode and administrator mode

Parameters

id <id no list>

Displays information about connection of the specified authentication server (VLANaccessController).

[Specification using numeric values]

Specify a unique VAA ID.

[Specifying a range by using "-" or ","]

All VAA IDs in the range are specified.

Operation when this parameter is omitted:

Displays all information about configured connections.

detail

Displays the detailed connection information of the specified authentication server (VLANaccessController).

<vlan id list>

Specifies multiple VLAN IDs which have been set as authenticated VLANs.

For details about how to specify <vlan id list>, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

Operation when this parameter is omitted:

Displays all information about configured VLANs.

Operation when all parameters are omitted:

Displays all information about configured VAA IDs and VLAN IDs.

Example

- The following shows an example of displaying all configured VLANaccessAgent information:

```
>show fense server
Date 2007/01/26 10:50:49 UTC
VAA NAME: switch01
VAA Sync Mode: Sync
Current Registered MAC: 20
Server Information:
ID:1      Status: enable      Agent Status: CONNECTED
      Server Address: 192.168.2.100      Port: 52153
      Retry Timer: 10      Retry Count: 25920      Current Count: 0
      Alive Timer: 20
      Target-VLAN Count: 4
ID:2      Status: enable      Agent Status: DISCONNECTED
      Server Address: 192.168.3.200      Port: 52153
```



```

Retry Timer:      3  Retry Count: infinity  Current Count:      20
Alive Timer:      20
Target-VLAN Count: 2

```

- An example of displaying detailed information about all configured VLANaccessAgent is shown below. Information about the server and the fence VLAN for all VLAN IDs is displayed.

```

>show fense server detail
Date 2007/01/26 10:50:49 UTC
VAA NAME: switch01
VAA Sync Mode: NoSync
Current Registered MAC: 20
Server Information:
ID:1          Status: enable          Agent Status: CONNECTED
  Server Address: 192.168.2.100      Port: 52153
    Retry Timer: 10  Retry Count: 25920  Current Count: 0
    Alive Timer: 20
  Target-VLAN Count: 4
  Target-VLAN Information:
    VLAN ID:2  1P Subnet Address: 192.168.2.0  mask 255.255.255.0
    VLAN ID:3  1P Subnet Address: 192.168.3.0  mask 255.255.255.0
    VLAN ID:4  1P Subnet Address: 192.168.4.0  mask 255.255.255.0
    VLAN ID:10 1P Subnet Address: 192.168.10.0 mask 255.255.255.0
ID:2          Status: enable          Agent Status: DISCONNECTED
  Server Address: 192.168.3.200      Port: 52153
    Retry Timer: 3  Retry Count: infinity  Current Count: 20
    Alive Timer: 20
  Target-VLAN Count: 2
  Target-VLAN Information:
    VLAN ID:10 1P Subnet Address: 192.168.10.0 mask 255.255.255.0
    VLAN ID:11 1P Subnet Address: 192.168.11.0 mask 255.255.255.0

```

Display items

The following table shows the items displayed for VLANaccessAgent information.

Table 8-1: Items displayed for VLANaccessAgent information

Item	Meaning	Displayed information
VAA NAME	VLANaccessAgent name	Displays the name set for VLANaccessAgent of a Switch. switch-name: Indicates the device name. -: Not set
VAA Sync Mode	Whether the functionality for registering authentication information exceeding the authentication capacity limit is available	Indicates whether the functionality for registering authentication information exceeding the authentication capacity limit is enabled or disabled. NoSync: Indicates that inter-switch asynchronous mode is enabled. Sync: Indicates normal mode.
Current Registered MAC [#]	The number of registered dynamic MACs	Displays the number of MAC addresses registered for MAC VLANs. To view the registered MAC addresses, use the <code>show vlan mac-vlan <vlan id list> dynamic</code> command.
Server Information	Authentication server information	Lists information about the authentication server.
ID	VLANaccessAgent ID	Displays the ID for VLANaccessAgent connection information. 1 to 10: Indicates the ID.
Status	Startup status	Indicates the startup and termination settings for VLANaccessAgent. enable: Running. disable: Disabled

Item	Meaning	Displayed information
Agent Status [#]	Server status	Indicates the authentication server status from the following categories. CONNECTED: Indicates the status that connection with the authentication server is established. DISCONNECTED: Indicates the status that connection with the authentication server is disconnected. SUSPENDED: Indicates the status that the VLANAccessAgent functionality is disabled. INVALID: Indicates that the versions of VLANAccessAgent and the authentication server do not match.
Server Address	Authentication server IP address	Indicates the value set for as the authentication server IP address. IP-address: Indicates the server IP address. -: Not set
Port	TCP port number for the authentication server	Indicates the setting value for the TCP port number of the authentication server. 1024 to 65535: Indicates the port number.
Retry Timer	Interval for retrying connection to the authentication server	Indicates the setting value for the retry interval (in seconds) when connection to the authentication server fails. 1 to 65535: Indicates the retry interval.
Retry Count	The number of retries to the authentication server until a dynamic MAC address is deleted	Indicates the setting value as the number of retries before the dynamic MAC address for the authentication VLAN is deleted if connection to the authentication server fails. infinity: Indicates an unlimited number of retries. 0 to 32767: Indicates the number of retries.
Current Count [#]	Current number of retries	Indicates the current number of retries for connecting to the authentication server. The value is cleared if connection to the authentication server is established successfully. Unsigned 32-bit value: Indicates the number of retries.
Alive Timer	Timeout interval for monitoring unreachable Keep Alive packets	Indicates setting value for the timeout interval (in seconds) until an attempt to reconnect to the authentication server is made if no Keep Alive packets are received. 20 to 7200: Indicates the timeout interval.
Target-VLAN Count	Number of authenticated VLANs	Indicates the number of VLANs which were set as authenticated VLANs for VLANAccessAgent. 0 to 4094: Indicates the number of VLANs.

[#]: A parameter value which is changed dynamically according to the operating status of VLANAccessAgent. For other parameters, information is displayed according to the configuration.

Table 8-2: Items displayed for detailed information about VLANAccessAgent

Item	Meaning	Displayed information
VAA NAME	VLANAccessAgent name	Displays the name set for VLANAccessAgent of a Switch. switch-name: Indicates the device name. -: Not set
VAA Sync Mode	Whether the functionality for registering authentication information exceeding the authentication capacity limit is available	Indicates whether the functionality for registering authentication information exceeding the authentication capacity limit is enabled or disabled. NoSync: Indicates that inter-switch asynchronous mode is enabled. Sync: Indicates normal mode.

Item	Meaning	Displayed information
Current Registered MAC [#]	The number of registered dynamic MACs	Displays the number of MAC addresses registered for MAC VLANs. To view the registered MAC addresses, use the <code>show vlan mac-vlan <vlan id list> dynamic</code> command.
Server Information	Authentication server information	Lists information about the authentication server.
ID	VLANaccessAgent ID	Indicates <code>vaa_id</code> in the connection information set for VLANaccessAgent. 1 to 10: Indicates <code>vaa_id</code> .
Status	Startup status	Indicates the running or stopped settings for VLANaccessAgent. enable: Running. disabled: Disabled
Agent Status [#]	Server status	Indicates the authentication server status from the following categories. CONNECTED: Indicates the status that connection with the authentication server is established. DISCONNECTED: Indicates the status that connection with the authentication server is disconnected. SUSPENDED: Indicates the status that the VLANaccessAgent functionality is disabled. INVALID: Indicates that the versions of VLANaccessAgent and the authentication server do not match.
Server Address	Authentication server IP address	Indicates the value set for as the authentication server IP address. IP-address: Indicates the server IP address. -: Not set
Port	TCP port number for the authentication server	Indicates the setting value for the TCP port number of the authentication server. 1024 to 65535: Indicates the port number.
Retry Timer	Interval for retrying connection to the authentication server	Indicates the setting value for the retry interval (in seconds) when connection to the authentication server fails. 1 to 65535: Indicates the retry interval.
Retry Count	The number of retries to the authentication server until a dynamic MAC address is deleted	Indicates the setting value as the number of retries before the dynamic MAC address for the authentication VLAN is deleted if connection to the authentication server fails. infinity: Indicates an unlimited number of retries. 0 to 32767: Indicates the number of retries.
Current Count [#]	Current number of retries	Indicates the current number of retries for connecting to the authentication server. The value is cleared if connection to the authentication server is established successfully. Unsigned 32-bit value: Indicates the number of retries.
Alive Timer	Timeout interval for monitoring unreachable Keep Alive packets	Indicates setting value for the timeout interval (in seconds) until an attempt to reconnect to the authentication server is made if no Keep Alive packets are received. 20 to 7200: Indicates the timeout interval.
Target-VLAN Count	Number of authenticated VLANs	Indicates the number of VLANs which were set as authenticated VLANs for VLANaccessAgent. 0 to 4094: Indicates the number of VLANs.
Target-VLAN Information	Authenticated MAC VLAN information	Lists the information registered as authenticated MAC VLANs.

Item	Meaning	Displayed information
VLAN ID	VLAN ID	Indicates the ID of a VLAN set as an authenticated VLAN. 2 to 4095: Indicates a VLAN ID.
IP Subnet Address	Subnet address of an authenticated VLAN	Indicates the setting value for the subnet address of the authenticated VLAN corresponding to the VLAN ID.

#: A parameter value which is changed dynamically according to the operating status of VLANaccessAgent. For other parameters, information is displayed according to the configuration.

Impact on communication

None

Response messages

Table 8-3: List of response messages for the show fense server command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to VAA program.	Communication with the VLANaccessAgent program failed. Re-execute the command. If this error occurs frequently, use the <code>show fense logging</code> command and the <code>dump protocols vaa</code> command to acquire the vaa status and the FENSE server logs (see the manual for the FENSE server for details), and then check the FENSE server status. After that, use the <code>restart vaa</code> command to restart VLANaccessAgent.
Now another user is using this command, please try again.	Another user is using the <code>show fense server detail</code> command. Wait a while, and then retry the operation.
VAA is not configured.	VLANaccessAgent has not been configured. Check the configuration.

Notes

The `show fense server detail` command cannot be used concurrently by multiple users.

show fense statistics [OP-VAA]

Displays statistics for VLANAccessAgent.

Syntax

```
show fense statistics [id <id no list>]
```

Input mode

User mode and administrator mode

Parameters

id <id no list>

Displays statistics for connection of the specified authentication server (VLANAccessController).

[Specification using numeric values]

Specify a unique VAA ID.

[Specifying a range by using "-" or ","]

All VAA IDs in the range are specified.

Operation when this parameter is omitted:

Displays all statistics you have set.

Example

The following shows an example of displaying statistics for all VLANAccessAgent you have set:

```
>show fense statistics
Date 2007/01/26 10:50:49 UTC
ID:1
VLANAccessController Connection:
  Connect Count      :      1
  Connect Failure Count :      0
  Timeout Disconnect Count:      0
VLANAccessAgent Recv Message:
      ADDMAC      DELMAC      LSTMAC      CLRMAC      DELMACALL
Request      11020      11000      100          0          0
Error          0          0          0          0          0
  FORMERROR      0          0          0          0          0
  INVSTATE      0          0          0          0          0
  NOMEMORY      0          0          0          0          0
  INVPARAM      0          0          0          0          0
  NOCLIENT      0          -          -          -          -
Target-VLAN Registration:
      MACReg      MACDel      AllMACDel      MACList
Request      11020      11000          0          100
Error          0          0          -          -
  INVVLAN      0          -          -          -
  MACOVFLW      0          -          -          -
  DUPMAC      0          -          -          -
  NOMAC      -          0          -          -
  HASHFULL      0          -          -          -
  OTHERERR      0          -          -          -
ID:2
VLANAccessController Connection:
  Connect Count      :      1
  Connect Failure Count :      0
  Timeout Disconnect Count:      0
VLANAccessAgent Recv Message:
      ADDMAC      DELMAC      LSTMAC      CLRMAC      DELMACALL
Request      1100      1000          15          0          0
```

Error	0	0	0	0	0
FORMERROR	0	0	0	0	0
INVSTATE	0	0	0	0	0
NOMEMORY	0	0	0	0	0
INVPARAM	0	0	0	0	0
NOCLIENT	0	-	-	-	-
Target-VLAN Registration:					
	MACReg	MACDel	AllMACDel	MACList	
Request	1100	1000	0	15	
Error	0	0	-	-	
INVLAN	0	-	-	-	
MACOVFLW	0	-	-	-	
DUPMAC	0	-	-	-	
NOMAC	-	0	-	-	
HASHFULL	0	-	-	-	
OTHERERR	0	-	-	-	

Display items

Table 8-4: Items displayed for VLANAccessAgent statistics

Item	Meaning	Displayed information
ID	VLANAccessAgentID	Displays vaa_id for information about connection to VLANAccessAgent. 1 to 10: Indicates vaa_id.
VLANAccessController Connection	Authentication server (VLANAccessController) connection information	Displays statistics for connection to the authentication server (VLANAccessController).
Connect Count	Number of connections	Indicates the number of connections to the authentication server. Unsigned 32-bit value: Indicates the number of connections.
Connect Failure Count	Number of failed connections	Indicates the number of failed connections to the authentication server. Unsigned 32-bit value: Indicates the number of failed connections.
Timeout Disconnect Count	Number of timeouts	Indicates the number of disconnections when the Switch did not receive the Keep Alive message from the authentication server within the interval set by the fense alive-timer command. Unsigned 32-bit value: Indicates the number of timeouts.
VLANAccessAgent Recv Message	Statistics for received messages from the authentication server	Lists the number of messages that VLANAccessAgent has received from the authentication server.
ADDMAC	MAC address registration request	Indicates statistics for MAC address registration requests.
Request	Number of times that MAC address registration requests was been received	Indicates the number of times that MAC address registration requests have been received from the authentication server. Unsigned 32-bit value: Indicates the number of registration requests.
Error	Number of failed MAC address registration requests	Indicates the total number of times that responses to MAC address registration requests from the authentication server failed. Unsigned 32-bit value: Indicates the number of failed registration requests.

Item	Meaning	Displayed information
FORMERROR	Number of times that FORMERROR has been sent as the cause of the error	Indicates the number of FORMERROR error responses to MAC address registration messages. Unsigned 32-bit value: Indicates the number of FORMERROR errors.
INVSTATE	Number of times that INVALIDSTATE has been sent as the cause of the error.	Indicates the number of INVALIDSTATE error responses to MAC address registration messages. Unsigned 32-bit value: Indicates the number of INVALIDSTATE errors.
NOMEMORY	Number of times that NOMEMORY has been sent as the cause of the error	Indicates the number of NOMEMORY error responses to MAC address registration messages. Unsigned 32-bit value: Indicates the number of NOMEMORY errors.
INVPARAM	Number of times that INVALIDPARAM has been sent as the cause of the error.	Indicates the number of INVALIDPARAM error responses to MAC address registration messages. Unsigned 32-bit value: Indicates the number of INVALIDPARAM errors.
NOCLIENT	Number of times that NOCLIENT has been sent as the cause of the error.	Indicates the number of NOCLIENT error responses to MAC address registration messages. Unsigned 32-bit value: Indicates the number of NOCLIENT errors.
DELMAC	MAC address deletion request	Indicates statistics for MAC address deletion requests.
Request	Number of times that a MAC address deletion request has been received	Indicates the number of MAC address deletion requests that have been received from the authentication server. Unsigned 32-bit value: Indicates the number of deletion requests.
Error	Number of failed MAC address deletion requests	Indicates the total number of times that MAC address deletion requests, received from the authentication server, failed. Unsigned 32-bit value: Indicates the number of failed deletion requests.
FORMERROR	Number of times that FORMERROR has been sent as the cause of the error	Indicates the number of FORMERROR error responses to MAC address deletion messages. Unsigned 32-bit value: Indicates the number of FORMERROR errors.
INVSTATE	Number of times that INVALIDSTATE has been sent as the cause of the error.	Indicates the number of INVALIDSTATE error responses to MAC address deletion messages. Unsigned 32-bit value: Indicates the number of INVALIDSTATE errors.
NOMEMORY	Number of times that NOMEMORY has been sent as the cause of the error	Indicates the number of NOMEMORY error responses to MAC address deletion messages. Unsigned 32-bit value: Indicates the number of NOMEMORY errors.
INVPARAM	Number of times that INVALIDPARAM has been sent as the cause of the error.	Indicates the number of INVALIDPARAM error responses to MAC address deletion messages. Unsigned 32-bit value: Indicates the number of INVALIDPARAM errors.
LSTMAC	Request for acquiring a list	Indicates statistics for requests to acquire a list.
Request	Number of times that a request for acquiring the list has been received	Indicates the number of requests to acquire a list of MAC addresses that have been received from the authentication server. Unsigned 32-bit value: Indicates the number of times that the list was requested.

Item	Meaning	Displayed information
Error	Number of failed requests for acquiring the list	Indicates the total number of times that requests to acquire a list of MAC addresses, received from the authentication server, failed. Unsigned 32-bit value: Indicates the number of times that a request for acquiring the list failed.
FORMERROR	Number of times that FORMERROR has been sent as the cause of the error	Indicates the number of FORMERROR error responses to MAC address list request messages. Unsigned 32-bit value: Indicates the number of FORMERROR errors.
INVSTATE	Number of times that INVALIDSTATE has been sent as the cause of the error.	Indicates the number of INVALIDSTATE error responses to MAC address list request messages. Unsigned 32-bit value: Indicates the number of INVALIDSTATE errors.
NOMEMORY	Number of times that NOMEMORY has been sent as the cause of the error	Indicates the number of NOMEMORY error responses to MAC address list request messages. Unsigned 32-bit value: Indicates the number of NOMEMORY errors.
INVPARAM	Number of times that INVALIDPARAM has been sent as the cause of the error.	Indicates the number of INVALIDPARAM error responses to MAC address list request messages. Unsigned 32-bit value: Indicates the number of INVALIDPARAM errors.
CLRMAC	Batch deletion request	Indicates statistics for batch deletion requests.
Request	Number of times that batch deletion requests were received	Indicates the number of times that batch deletion requests were received from the authentication server. Unsigned 32-bit value: Indicates the number of times that batch deletion requests were issued.
Error	Number of failed batch deletion requests	Indicates the total number of times that batch deletion requests from the authentication server failed. Unsigned 32-bit value: Indicates the number of failed batch deletion requests.
FORMERROR	Number of times that FORMERROR has been sent as the cause of the error	Indicates the number of FORMERROR error responses that have been sent as MAC address batch deletion messages. Unsigned 32-bit value: Indicates the number of FORMERROR errors.
INVSTATE	Number of times that INVALIDSTATE has been sent as the cause of the error.	Indicates the number of INVALIDSTATE error responses to MAC address batch deletion messages. Unsigned 32-bit value: Indicates the number of INVALIDSTATE errors.
NOMEMORY	Number of times that NOMEMORY has been sent as the cause of the error	Indicates the number of NOMEMORY error responses to MAC address batch deletion messages. Unsigned 32-bit value: Indicates the number of NOMEMORY errors.
INVPARAM	Number of times that INVALIDPARAM has been sent as the cause of the error.	Indicates the number of INVALIDPARAM error responses to MAC address batch deletion messages. Unsigned 32-bit value: Indicates the number of INVALIDPARAM errors.
DELMACALL	Request for deleting all specified MAC addresses	Indicates statistics for requests to delete all specified MAC addresses.

Item	Meaning	Displayed information
Request	Number of times that a request for deleting all specified MAC addresses has been received	Indicates the number of requests to delete all specified MAC addresses, received from the authentication server. Unsigned 32-bit value: Indicates the number of requests to delete all specified MAC addresses that have been received.
Error	Number of times that a request for deleting all specified MAC addresses was failed	Indicates the total number of times that requests to delete all specified MAC addresses, received from the authentication server, failed. Unsigned 32-bit value: Indicates the number of times that requests to delete all specified MAC addresses failed.
FORMERROR	Number of times that FORMERROR has been sent as the cause of the error	Indicates the number of FORMERROR error message responses to requests to delete all MAC addresses. Unsigned 32-bit value: Indicates the number of FORMERROR errors.
INVSTATE	Number of times that INVALIDSTATE has been sent as the cause of the error.	Indicates the number of INVALIDSTATE error responses to request to delete all MAC addresses. Unsigned 32-bit value: Indicates the number of INVALIDSTATE errors.
NOMEMORY	Number of times that NOMEMORY has been sent as the cause of the error	Indicates the number of NOMEMORY error responses to requests to delete all MAC addresses. Unsigned 32-bit value: Indicates the number of NOMEMORY errors.
INVPARAM	Number of times that INVALIDPARAM has been sent as the cause of the error.	Indicates the number of INVALIDPARAM error responses to requests to delete all MAC addresses. Unsigned 32-bit value: Indicates the number of INVALIDPARAM errors.
Target-VLAN Registration	Statistics for registering MAC in a MAC VLAN	Indicates statistics for requests to register a MAC address to a MAC VLAN.
MAC Reg	Request to register a MAC address	Indicates statistics for requests to register a MAC address.
Request	Number of registration requests of a MAC address	Indicates the number of requests to register an authenticated MAC address to a MAC VLAN. Unsigned 32-bit value: Indicates the number of registration requests.
Error	Number of failed registration requests of a MAC address	Indicates the number of times that requests to register an authenticated MAC address to a MAC VLAN failed. Unsigned 32-bit value: Indicates the number of failed registration requests.
INVVLAN	Number of times that invalid VLAN ID has been returned as the cause of the error	Indicates the number of times that invalid VLAN ID has been returned to a MAC address registration request. Unsigned 32-bit value: Indicates the number of invalid VLAN ID errors.
MACOVFLW	Number of times that an excessive number of MAC entries has been returned as the cause of the error	Indicates the number of times that an excessive number of MAC entries has been returned as the cause of the error to a MAC address registration request. Unsigned 32-bit value: Indicates the number of MAC OVER FLOW errors.

Item	Meaning	Displayed information
DUPMAC	Number of times that duplicated registration has been returned as the cause of the error	Indicates the number of times that a duplicated registration error has been returned to a MAC address registration request. Unsigned 32-bit value: Indicates the number of DUPLICATE MAC errors.
HASHFULL	Number of times that a MAC address hardware registration error has been returned as the cause of the error	Indicates the number of times that a registration error caused by hardware specifications has been returned to a MAC address registration request. Unsigned 32-bit value: Indicates the number of errors.
OTHERERR	Number of times that other errors have been returned	Indicates the number of other error responses to MAC address registration requests. Unsigned 32-bit value: Indicates the number of OTHER ERROR errors.
MACDel	MAC address deletion request	Indicates statistics for MAC address deletion requests.
Request	Number of MAC address deletion requests	Indicates the number of MAC address deletion requests. Unsigned 32-bit value: Indicates the number of deletion requests.
Error	Number of failed MAC address deletion requests	Indicates the number of times that requests to delete an authenticated MAC address from a MAC VLAN failed. Unsigned 32-bit value: Indicates the number of failed deletion requests.
NOMAC	Number of times that an invalid MAC address error has been returned as the cause of the error	Indicates the number of times that an invalid MAC address error has been returned. Unsigned 32-bit value: Indicates the number of NOMAC errors.
AllMACDel	Request to delete all MAC addresses	Indicates statistics for requests to delete all MAC addresses.
Request	Number of requests to delete all MAC addresses	Indicates the number of requests to delete all MAC addresses. Unsigned 32-bit value: Indicates the number of deletion requests.
MACList	Request for acquiring the list of MAC addresses	Indicates statistics for requests to acquire lists of MAC addresses.
Request	Number of requests for acquiring the list of MAC addresses	Indicates the number of requests to acquire lists of dynamic MAC addresses. Unsigned 32-bit value: Indicates the number of times that the list was requested.

Impact on communication

None

Response messages

Table 8-5: List of response messages for the show fense statistics command

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

Message	Description
Connection failed to VAA program.	Communication with the VLANaccessAgent program failed. Re-execute the command. If this error occurs frequently, use the <code>show fense logging</code> command and the <code>dump protocols vaa</code> command to acquire the vaa status and the FENSE server logs (see the manual for the FENSE server for details), and then check the FENSE server status. After that, use the <code>restart vaa</code> command to restart VLANaccessAgent.
VAA is not configured.	VLANaccessAgent has not been configured. Check the configuration.

Notes

None

show fense logging [OP-VAA]

Displays the log messages for internal operations collected by the VLANAccessAgent program. Displayed information is used for analysis of authentication VLAN failures.

Syntax

```
show fense logging [{error | warning | notice}]
```

Input mode

User mode and administrator mode

Parameters

{error | warning | notice}

Specify the level of operation log message to be displayed. Logs with severity exceeding the specified level are displayed.

Operation when this parameter is omitted:

Displays operation log messages for which severity is the NOTICE level or higher.

Example

The following shows an example of displaying VLANAccessAgent operation log messages:

```
> show fense logging
Date 2006/03/01 10:50:49 UTC
1:Jul  2 14:47:34:NOTICE:DELMAC message was received from the authentication
server. id=1 Subnet=192.168.1.0 MAC=0012.e201.0204
2:Jul  2 14:32:45:NOTICE:ADDMAC message was received from the authentication
server. id=1 Subnet=192.168.1.0 MAC=0012.e201.0203
3:Jul  2 10:49:23:NOTICE:WELCOME message was received from the authentication
server. id=1
SrvVer=1.0 SrvIP=192.168.2.10
4:Jul  2 10:49:23:NOTICE:The connection with the authentication server succeeded.
id=1
```

Display items

Outputs operation log messages by severity level. The following table shows the levels of operation log messages and *Table 8-7: List of operation log messages* shows the list of operation log messages.

Table 8-6: Levels of operation log messages

Level	Description
ERROR	Indicates that a failure status has occurred, and indicates the action, such as restarting a daemon, that must be taken to resolve it.
WARNING	Indicates a warning message, such as received an invalid frame.
NOTICE	Indicates a communication message, such as information as to whether authentication is successful.

Table 8-7: List of operation log messages

#	Level	Message text	Meaning	Additional information
1	NOTICE	ADDMAC message was received from the authentication server. id=<vaa_id> Subnet=<subnet-address> MAC=<MAC-address>	Received an address registration request from the authentication server	<ul style="list-style-type: none"> vaa_id Subnet address MAC address

#	Level	Message text	Meaning	Additional information
2	WARNING	The error response for the ADDMAC message was transmitted to the authentication server. id=<vaa_id> MAC=<MAC-address> Code=<error-code>	Error response to an address registration request from the authentication server	<ul style="list-style-type: none"> vaa_id MAC address error code
3	NOTICE	DELMAC message was received from the authentication server. id=<vaa_id> Subnet=<subnet-address> MAC=<MAC-address>	Address deletion request received from the authentication server	<ul style="list-style-type: none"> vaa_id Subnet address MAC address
4	WARNING	The error response for the DELMAC message was transmitted to the authentication server. id=<vaa_id> MAC=<MAC-address> Code=<error-code>	Error response to an address deletion request from the authentication server	<ul style="list-style-type: none"> vaa_id MAC address error code
5	NOTICE	CLRMAC message was received from the authentication server. id=<vaa_id> Subnet=<subnet-address>	Address batch deletion request received from the authentication server	<ul style="list-style-type: none"> vaa_id Subnet address
6	WARNING	The error response for the CLRMAC message was transmitted to the authentication server. id=<vaa_id> subnet=<subnet-address> Code=<error-code>	Error response to a batch deletion request of MAC addresses from the authentication server.	<ul style="list-style-type: none"> vaa_id Subnet address error code
7	NOTICE	DELMACALLVLAN message was received from the authentication server. id=<vaa_id> MAC=<MAC-address>	Received a request from the authentication server to delete all specified MAC addresses	<ul style="list-style-type: none"> vaa_id MAC address
8	NOTICE	WELCOME message was received from the authentication server. id=<vaa_id> SrvVer=<authentication-server-version> SrvIP=<authentication-server-IP-address>	Received a Welcome message from the authentication server	<ul style="list-style-type: none"> vaa_id Version of the authentication server Authentication server IP address
9	WARNING	Illegal frame was received from the authentication server. id=<vaa_id> "<received-data>"	Received an invalid frame from the authentication server	<ul style="list-style-type: none"> vaa_id Received data
10	NOTICE	The connection with the authentication server succeeded. id=<vaa_id>	Successfully connected to the authentication server.	<ul style="list-style-type: none"> vaa_id
11	NOTICE	The connection with the authentication server failed. id=<vaa_id> RetryCount=<number-of-retries>	Connection to the authentication server failed.	<ul style="list-style-type: none"> vaa_id The number of retries
12	WARNING	The registration of the MAC address failed. id=<vaa_id> VLAN ID=<vlan_no> MAC=<MAC-address> Code=<error-code>	Registration of a MAC address to a MAC VLAN failed.	<ul style="list-style-type: none"> vaa_id vlan_no MAC address error code
13	WARNING	The number of registration of MAC addresses is full. id=<vaa_id> MAC=<MAC-address>	The number of MAC address registrations exceeds the limit because the resources are insufficient.	<ul style="list-style-type: none"> vaa_id MAC address
14	ERROR	Failed to open socket . Code=<error-code>	An attempt to open a socket failed.	<ul style="list-style-type: none"> error code

#	Level	Message text	Meaning	Additional information
15	WARNING	The socket with L2MacManager was closed. Code=<error-code>	The socket connection to L2MacManager was closed.	• error code
16	ERROR	Configuration data setting failed. Code=<error-code>	An attempt to set the Vlan-Port information failed.	• error code
17	WARNING	Device open error. Code=<error-code>	An attempt to acquire a MAC address table entry failed.	• error code

Impact on communication

None

Response messages

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

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to VAA program.	Communication with the VLANaccessAgent program failed. Re-execute the command. If this error occurs frequently, use the <code>show fense logging</code> command and the <code>dump protocols vaa</code> command to acquire the vaa status and the FENSE server logs (see the manual for the FENSE server for details), and then check the FENSE server status. After that, use the <code>restart vaa</code> command to restart VLANaccessAgent.
Now another user is using this command, please try again.	Another user is using this command. Wait a while, and then retry the operation.
VAA is not configured.	VLANaccessAgent has not been configured. Check the configuration.

Notes

This command cannot be used concurrently by multiple users.

clear fense statistics [OP-VAA]

Clears statistics for VLANaccessAgent.

Syntax

```
clear fense statistics [id <id no list>]
```

Input mode

User mode and administrator mode

Parameters

id <id no list>

Clears statistics for VLANaccessAgent corresponding to the VAA ID in the specified range.

[Specification using numeric values]

Specify a unique VAA ID.

[Specifying a range by using "-" or ","]

All VAA IDs in the range are specified.

Operation when this parameter is omitted:

Clears all statistics for configured connections.

Example

The following shows an example of clearing statistics for VLANaccessAgent.

```
> clear fense statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 8-9: List of response messages for the clear fense statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to VAA program.	Communication with the VLANaccessAgent program failed. Re-execute the command. If this error occurs frequently, use the <code>show fense logging</code> command and the <code>dump protocols vaa</code> command to acquire the vaa status and the FENSE server logs (see the manual for the FENSE server for details), and then check the FENSE server status. After that, use the <code>restart vaa</code> command to restart VLANaccessAgent.
VAA is not configured.	VLANaccessAgent has not been configured. Check the configuration.

Notes

None

clear fense logging [OP-VAA]

Clears the operation log messages collected by the VLANaccessAgent program.

Syntax

```
clear fense logging
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following shows an example of clearing an operation log message:

```
> clear fense logging
>
```

Display items

None

Impact on communication

None

Response messages

Table 8-10: List of response messages for the clear fense logging command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to VAA program.	Communication with the VLANaccessAgent program failed. Re-execute the command. If this error occurs frequently, use the <code>show fense logging</code> command and the <code>dump protocols vaa</code> command to acquire the vaa status and the FENSE server logs (see the manual for the FENSE server for details), and then check the FENSE server status. After that, use the <code>restart vaa</code> command to restart VLANaccessAgent.
VAA is not configured.	VLANaccessAgent has not been configured. Check the configuration.

Notes

None

restart vaa [OP-VAA]

Restarts VLANaccessAgent.

Syntax

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

Input mode

User mode and administrator mode

Parameters

-f

Restarts VLANaccessAgent without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file for VLANaccessAgent when VLANaccessAgent is restarted.

Operation when this parameter is omitted:

A core file is not output.

Operation when all parameters are omitted:

Restarts VLANaccessAgent after displaying a confirmation message.

Example

The following shows an example of restarting VLANaccessAgent:

```
> restart vaa
VAA restart OK? (y/n): y
>
```

Display items

None

Impact on communication

- While VLANaccessAgent is being restarted, dynamic MAC addresses cannot be registered by using VLANaccessAgent.
- After restart, if the authentication server has registered the MAC address, the authentication server performs re-authentication automatically. If the authentication server has not registered the MAC address, re-authentication from a terminal is required.

Response messages

Table 8-11: List of response messages for the restart vaa command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
VAA doesn't seem to be running.	This command failed because the VLANaccessAgent program is not started. If VLANaccessAgent has not been configured, this message is output.
VAA program failed to be restarted.	An attempt to restart the VLANaccessAgent program by using this command failed. Re-execute the command.

Notes

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

Storage directory: `/usr/var/core/`

Core file: `vaad.core`

If the specified file already exists, the file is overwritten unconditionally. Therefore, back up the file in advance if necessary.

dump protocols vaa [OP-VAA]

Outputs to a file detailed event trace information and control table information collected by VLANAccessAgent.

Syntax

```
dump protocols vaa
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following shows an example of specifying a VLANAccessAgent dump:

```
> dump protocols vaa
>
```

Display items

None

Impact on communication

None

Response messages

Table 8-12: List of response messages for the dump protocols vaa command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to VAA program.	Communication with the VLANAccessAgent program failed. Re-execute the command. If this error occurs frequently, use the <code>show fense logging</code> command and the <code>dump protocols vaa</code> command to acquire the vaa status and the FENSE server logs (see the manual for the FENSE server for details), and then check the FENSE server status. After that, use the <code>restart vaa</code> command to restart VLANAccessAgent.
File open error.	An attempt to open or access a dump file failed.
VAA is not configured.	VLANAccessAgent has not been configured. Check the configuration.

Notes

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

Storage directory: `/usr/var/vaa/`

File: `vaad_dump.gz`

If the specified file already exists, the file is overwritten unconditionally. Therefore, back up the file in advance if necessary.

Chapter

9. 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 logging
clear ip dhcp snooping logging
restart dhcp snooping
dump protocols dhcp snooping
```

show ip dhcp snooping binding

Displays the DHCP snooping binding database.

Syntax

```
show ip dhcp snooping binding [[ip] <ip address>] [mac <mac address>]
                               [vlan <vlan id>]
                               [interface <interface type> <interface number>]
                               [{ static | dynamic }]
```

Input mode

User mode and administrator mode

Parameters

[ip] <ip address>

Displays the binding database entry for the specified IP address.

mac <mac address>

Displays the binding database entry for the specified MAC address.

vlan <vlan id>

Displays the binding database entry for the specified VLAN interface.

For <vlan id>, specify the VLAN ID set by the `ip dhcp snooping vlan` configuration command.

interface <interface type> <interface number>

Displays the binding database entry for the specified interface.

For <interface type> <interface number>, the following values can be set:

- gigabitethernet <nif no.>/<port no.>
- tengigabitethernet <nif no.>/<port no.>
- port-channel <channel group number>

For details about the valid setting range of <nif no.>/<port no.> and <channel group number>, see *Specifiable values for parameters*.

{ static | dynamic }

static

Displays the binding database entry for statically registered entries.

dynamic

Displays the binding database entry for dynamically registered entries.

Operation when a parameter is omitted

This command can display only the entries that meet the conditions specified by the parameter. If no parameters are set, entries are displayed with no condition applied. If multiple parameters are specified, the entries conforming to the conditions will be displayed.

Operation when all parameters are omitted:

Displays all entries.

Example

The following figure shows an example of displaying all DHCP snooping entries.

Figure 9-1: Result of executing the DHCP snooping binding database display command

```

> show ip dhcp snooping binding
Date 2010/04/20 12:00:00 UTC
Agent URL: flash
Last succeeded time: 2010/04/20 11:50:00 UTC
Total Bindings Used/Max      :      5/   500
Total Source guard Used/Max:      2/   500

Bindings: 5
MAC Address      IP Address      Expire(min)  Type      VLAN  Port
0012.e287.0001   192.168.0.201    -            static*    1     1/1
0012.e287.0002   192.168.0.204   1439         dynamic    2     1/4
0012.e287.0003   192.168.0.203    -            static     3     1/3
0012.e287.0004   192.168.0.202   3666         dynamic    4     ChGr:2
0012.e2be.b0fb   192.168.100.11   59           dynamic*   12    1/11
>

> show ip dhcp snooping binding 192.168.0.202
Date 2010/04/20 12:00:00 UTC
Agent URL: flash
Last succeeded time: 2010/04/20 11:50:00 UTC
Total Bindings Used/Max      :      5/   500
Total Source guard Used/Max:      2/   500

Bindings: 1
MAC Address      IP Address      Expire(min)  Type      VLAN  Port
0012.e287.0004   192.168.0.202   3666         dynamic    4     ChGr:2
>

```

Display items

Table 9-1: Items displayed for the show ip dhcp snooping binding command

Item	Meaning	Displayed information
Agent URL	Save location for the binding database	Displays setting information in the configuration. flash: Indicates internal flash memory. mc: Indicates a memory card. -: Not specified
Last succeeded time	Date and time the Switch last saved [#] (year/month/day hour:minute:second time-zone)	Displays the date and time when information was saved to the save location. - is displayed for the following cases: <ul style="list-style-type: none"> The agent URL is not specified. The database has never been saved. The number of entries to be restored is zero.
Total Bindings Used/Max: <Used>/<Max>	Number of entries registered in the binding database and maximum number of entries that can be registered	<Used>: Number of registered entries <Max>: Maximum number of entries that can be registered
Total Source guard Used/Max: <Used>/<Max>	Number of entries which are applied to an interface and for which terminal filter is enabled, and maximum number of applicable entries	<Used>: Number of applied entries <Max>: Maximum number of entries that can be applied
Bindings	Number of displayed binding databases	n/a
MAC Address	Terminal MAC address	n/a
IP Address	Terminal IP address	n/a
Expire(min)	Aging time (in minutes)	If there is no limit in the number of static entries or the aging time, - is displayed.

Item	Meaning	Displayed information
Type	Entry type	static: Indicates a static entry. static*: Indicates a static entry (for a terminal filter). dynamic: Indicates a dynamic entry. dynamic*: Indicates a dynamic entry (for a terminal filter).
VLAN	ID of a VLAN to which a terminal is connected	n/a
Port	Port to which a terminal is connected	If the interface is gigabitethernet or tengigabitethernet, the NIF number and the port number are displayed. For port-channel, the following value is displayed: ChGr: 1 to ChGr: 63

Legend n/a: Not applicable

#: If the binding database has been restored due to Switch restart or for another reason, the time that the restore information was saved is displayed.

Impact on communication

None

Response messages

Table 9-2: List of response messages for the show ip dhcp snooping binding command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not operating.
Illegal NIF -- <nif no.>.	The specified NIF number is invalid. Make sure the specified parameter is correct, and then try again. <nif no.>: Indicates the NIF number.
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Indicates the port number.
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: Location of the error

Notes

None

clear ip dhcp snooping binding

Clears the DHCP snooping binding database. This command clears only the entries that have been registered dynamically.

Syntax

```
clear ip dhcp snooping binding [[ip] <ip address>] [mac <mac address>]
                               [vlan <vlan id>]
                               [interface <interface type> <interface number>]
```

Input mode

User mode and administrator mode

Parameters

[ip] <ip address>

Clears the binding database for the specified IP address.

mac <mac address>

Clears the binding database for the specified MAC address.

vlan <vlan id>

Clears the binding database for the specified VLAN interface.

For <vlan id>, specify the VLAN ID set by the `ip dhcp snooping vlan` configuration command.

interface <interface type> <interface number>

Clears the binding database for the specified interface.

For <interface type> <interface number>, the following values can be set:

- gigabitethernet <nif no.>/<port no.>
- tengigabitethernet <nif no.>/<port no.>
- port-channel <channel group number>

For details about the valid setting range of <nif no.>/<port no.> and <channel group number>, see *Specifiable values for parameters*.

Operation when a parameter is omitted

This command can clear only the entries that meet the conditions specified by the parameter. If no parameters are specified, the entries are cleared without being limited by any conditions. If multiple parameters are specified, the entries conforming to the conditions will be cleared.

Operation when all parameters are omitted:

Clears all the dynamically registered entries.

Example

The following figure shows an example of clearing all the dynamically registered entries.

Figure 9-2: Result of executing the command for clearing the binding database for DHCP snooping

```
> clear ip dhcp snooping binding
>
```

Display items

None

Impact on communication

The access from the terminal corresponding to a cleared entry is strictly restricted until learning is completed again.

Response messages

Table 9-3: List of response messages for the clear ip dhcp snooping binding command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not operating.
Illegal NIF -- <nif no.>.	The specified NIF number is invalid. Make sure the specified parameter is correct, and then try again. <nif no.>: Indicates the NIF number.
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Indicates the port number.
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: Location of the error

Notes

None

show ip dhcp snooping statistics

Displays statistics for DHCP snooping.

Syntax

```
show ip dhcp snooping statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure shows an example of displaying statistics for DHCP snooping.

Figure 9-3: Result of executing the command for displaying statistics for DHCP snooping

```
> show ip dhcp snooping statistics
Date 2010/04/20 12:00:00 UTC
Database Exceeded: 0
Total DHCP Packets: 8995
Port          Recv          Filter
1/1           170           170
1/3           1789          10
:
1/25          0             0
ChGr:1        3646          2457
>
```

Display items

Table 9-4: Items displayed for DHCP snooping statistics

Item	Meaning	Displayed information
Database Exceeded	Number of times that binding database entries exceeded the maximum allowed number	n/a
Total DHCP Packets	Total number of DHCP packets processed on untrusted ports in DHCP snooping	n/a
Port	An untrusted port for which DHCP snooping is enabled	If the interface is gigabitethernet or tengigabitethernet, the NIF number and the port number are displayed. For port-channel, the following value is displayed: ChGr:1 to ChGr:63
Recv	Number of DHCP packets received on untrusted ports for DHCP snooping	The number of packets discarded by Filter is included.
Filter	Of the DHCP packets received (Recv) on the untrusted port for DHCP snooping, the number of DHCP packets discarded as invalid packets	n/a

Legend n/a: Not applicable

Impact on communication

None

Response messages

Table 9-5: List of response messages for the show ip dhcp snooping statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not operating.
Program error occurred: <i><error message></i>	A program error occurred. Re-execute the command. <i><error message></i> : Location of the error

Notes

When port mirroring is used, if DHCP snooping is enabled by the default VLAN, the mirror port is also displayed using this command.

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

The following figure shows an example of clearing the DHCP snooping statistics.

Figure 9-4: Result of executing the command for clearing the DHCP snooping statistics

```
> clear ip dhcp snooping statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 9-6: List of response messages for the clear ip dhcp snooping statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not operating.
Program error occurred: <i><error message></i>	A program error occurred. Re-execute the command. <i><error message></i> : Location of the error

Notes

None

show ip arp inspection statistics

Displays the statistics for dynamic ARP inspection.

Syntax

```
show ip arp inspection statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure shows an example of displaying statistics for dynamic ARP inspection.

Figure 9-5: Result of executing the command for displaying the statistics for dynamic ARP inspection

```
> show ip arp inspection statistics
Date 2010/04/20 12:00:00 UTC
Port      Forwarded      Dropped  ( DB mismatch      Invalid  )
1/1        0                15      (          15       0       )
1/2        584             883      (          883       0       )
1/3        0                0        (           0        0       )
          :
ChGr:2      170             53      (           53       0       )
>
```

Display items

Table 9-7: Items displayed for statistics for dynamic ARP inspection

Item	Meaning	Displayed information
Port	Port number	If the interface is gigabitethernet or tengigabitethernet, the NIF number and the port number are displayed. For port-channel, the following value is displayed: ChGr:1 to ChGr:63
Forwarded	Number of forwarded ARP packets	n/a
Dropped	Total number of discarded ARP packets	Total number of packets listed in the DB mismatch and Invalid
DB mismatch	The number of ARP packets discarded because a mismatch of the binding database was found through a basic check	n/a
Invalid	The number of ARP packets discarded because a mismatch of the binding database was found through an optional inspection	n/a

Legend n/a: Not applicable

Impact on communication

None

Response messages

Table 9-8: List of response messages for the show ip arp inspection statistics command

Message	Description
ARP Inspection doesn't seem to be running.	The command could not be executed because dynamic ARP inspection is not operating.
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Program error occurred: <i><error message></i>	A program error occurred. Re-execute the command. <i><error message></i> : Location of the error

Notes

When port mirroring is used, if dynamic ARP inspection is enabled in the default VLAN, the mirror port is also displayed using this command.

clear ip arp inspection statistics

Clears the dynamic ARP inspection statistics.

Syntax

```
clear ip arp inspection statistics
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure shows an example of clearing dynamic ARP inspection statistics.

Figure 9-6: Result of executing the command for clearing dynamic ARP inspection statistics

```
> clear ip arp inspection statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 9-9: List of response messages for the clear ip arp inspection statistics command

Message	Description
ARP Inspection doesn't seem to be running.	The command could not be executed because dynamic ARP inspection is not operating.
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: Location of the error

Notes

None

show ip dhcp snooping logging

Displays the operation log messages collected by the DHCP snooping program.

Syntax

```
show ip dhcp snooping logging [{ error | warning | notice | info }]
```

Input mode

User mode and administrator mode

Parameters

{ error | warning | notice | info }

Specify the level of operation log message to be displayed. From output messages of the level specified by using the `ip dhcp snooping loglevel` configuration command, log entries whose severity level is equal to or greater than that specified by using this `show ip dhcp snooping logging` command are displayed.

Operation when this parameter is omitted:

The same operation log messages as those displayed when `notice` is specified is displayed.

Example

The following figure shows an example of displaying an operation log message for DHCP snooping.

Figure 9-7: Result of executing the command for displaying an operation log message of DHCP snooping

```
> show ip dhcp snooping logging
Date 2010/04/20 12:00:00 UTC
Apr 20 11:00:00 ID=2201 NOTICE DHCP server packets were received at an untrust
port(1/2/1/0012.e2ff.fe01/192.168.100.254) .
>
```

Display items

The following shows the display format of a message.

```
Apr 20 11:00:00 ID=2201 NOTICE DHCP server packets were received at an untrust
(1)   (2)   (3)   (4)                               (5)
port(1/2/1/0012.e2ff.fe01/192.168.100.254).
```

- (1) Date: Displays the date (month and day) when the event indicated in the operation log message occurred.
- (2) Time: Displays the time when the event indicated in the operation log message occurred.
- (3) Message ID
- (4) Level: The following table shows the levels and their description.

Table 9-10: Levels and their description

Level	Type	Description
ERROR	Problem	Interruption of communication is detected or configurations of events were inconsistent.
WARN	Warning	Malicious packets were detected or events that occurred when configurations were inconsistent.

Level	Type	Description
NOTICE	Notification	Errors that occur during normal operation or events that occurred when configurations were inconsistent.
INFO	Regular	A normal event that occurs during normal operation

(5) Message text

The following table shows the contents of operation log messages.

Table 9-11: List of operation log messages

Message ID	Level	Message text	Description
1109	INFO	The binding entry was deleted all.	[Meaning] All binding database entries were deleted. [Explanation of message variables] None. [Action] None
1110	INFO	The source guard entry was deleted all.	[Meaning] All terminal filter entries were deleted. [Explanation of message variables] None. [Action] None
1201	INFO	The binding entry was created(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	[Meaning] An entry was added to the binding database. [Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] None
1202	INFO	The binding entry timed out(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	[Meaning] An entry was deleted from the binding database because an aging time expired. [Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] None

Message ID	Level	Message text	Description
1203	INFO	The binding entry was deleted by received DHCPRELEASE(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] An entry was deleted from the binding database because DHCPRELEASE was received.</p> <p>[Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] None</p>
1204	INFO	The binding entry was deleted by received DHCPDECLINE(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] An entry was deleted from the binding database because DHCPDECLINE was received.</p> <p>[Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] None</p>
1205	INFO	The binding entry was renewed(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] A binding database entry was updated because lease renewal was detected.</p> <p>[Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] None</p>
1206	INFO	The binding entry was deleted(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] An entry was deleted from the binding database.</p> <p>[Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] None</p>

Message ID	Level	Message text	Description
1207	INFO	The source guard entry was added(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] A terminal filter entry was added.</p> <p>[Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] None</p>
1208	INFO	The source guard entry was deleted(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] A terminal filter entry was deleted.</p> <p>[Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] None</p>
1301	INFO	The binding entry was created(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] An entry was added to the binding database.</p> <p>[Explanation of message variables] ChGr:<channel group number> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] None</p>
1302	INFO	The binding entry timed out(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] An entry was deleted from the binding database because an aging time expired.</p> <p>[Explanation of message variables] ChGr:<channel group number> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] None</p>

Message ID	Level	Message text	Description
1303	INFO	The binding entry was deleted by received DHCPRELEASE(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] An entry was deleted from the binding database because DHCPRELEASE was received.</p> <p>[Explanation of message variables] ChGr:<channel group number>/ <vlan id>/ <mac address>/ <ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] None</p>
1304	INFO	The binding entry was deleted by received DHCPDECLINE(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] An entry was deleted from the binding database because DHCPDECLINE was received.</p> <p>[Explanation of message variables] ChGr:<channel group number>/ <vlan id>/ <mac address>/ <ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] None</p>
1305	INFO	The binding entry was renewed(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] A binding database entry was updated because lease renewal was detected.</p> <p>[Explanation of message variables] ChGr:<channel group number>/ <vlan id>/ <mac address>/ <ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] None</p>
1306	INFO	The binding entry was deleted(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] An entry was deleted from the binding database.</p> <p>[Explanation of message variables] ChGr:<channel group number>/ <vlan id>/ <mac address>/ <ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] None</p>

Message ID	Level	Message text	Description
2105	NOTICE	Discard of packets occurred by a reception rate limit of DHCP packets and ARP packets.	<p>[Meaning] Packets were discarded due to the reception rate limit for DHCP packets and ARP packets. [Explanation of message variables] None. [Action] Review the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.</p>
2201	NOTICE	DHCP server packets were received at an untrust port(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] An invalid DHCP server was detected. This message is output once every five minutes on a port-by-port basis. [Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address> / <ip address>: Indicates DHCP server information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] Check the connected device.</p>
2202	NOTICE	Lease release was received from the client who isn't in binding(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] Invalid lease release was detected. This message is output once every five minutes on a port-by-port basis. [Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] If this occurs frequently, it might have been caused by an attack. Check the connected devices.</p>
2203	NOTICE	DHCP direct request was received from the client who isn't in binding(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] An invalid DHCP request was detected. This message is output once every five minutes on a port-by-port basis. [Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address. [Action] If this occurs frequently, it might have been caused by an attack. Check the connected devices.</p>

Message ID	Level	Message text	Description
2204	NOTICE	ARP packet was received from the client who isn't in binding(<nif no.>/<port no.>/<vlan id>/<mac address>).	<p>[Meaning] An ARP packet that does not match the binding database was detected. This message is output once every five minutes on a port-by-port basis. [Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address>: Indicates ARP terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address.</p> <p>[Action] Review the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.</p>
2301	NOTICE	DHCP server packets were received at an untrust port(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] An invalid DHCP server was detected. This message is output once every five minutes on a port-by-port basis. [Explanation of message variables] ChGr:<channel group number> / <vlan id> / <mac address> / <ip address>: Indicates DHCP server information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] Check the connected device.</p>
2302	NOTICE	Lease release was received from the client who isn't in binding(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] Invalid lease release was detected. This message is output once every five minutes on a port-by-port basis. [Explanation of message variables] ChGr:<channel group number> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] If this occurs frequently, it might have been caused by an attack. Check the connected devices.</p>

Message ID	Level	Message text	Description
2303	NOTICE	DHCP direct request was received from the client who isn't in binding (ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] An invalid DHCP request was detected. This message is output once every five minutes on a port-by-port basis.</p> <p>[Explanation of message variables] ChGr:<channel group number> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] If this occurs frequently, it might have been caused by an attack. Check the connected devices.</p>
2304	NOTICE	ARP packet was received from the client who isn't in binding(ChGr:<channel group number>/<vlan id>/<mac address>).	<p>[Meaning] An ARP packet that does not match the binding database was detected. This message is output once every five minutes on a port-by-port basis.</p> <p>[Explanation of message variables] ChGr:<channel group number> / <vlan id> / <mac address>: Indicates ARP terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address.</p> <p>[Action] Review the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.</p>
3201	WARN	DHCP packet discard with Option82(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] A packet with Option82 was discarded. This message is output once every five minutes on a port-by-port basis.</p> <p>[Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] Review the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.</p>

Message ID	Level	Message text	Description
3202	WARN	Discard of the DHCP packet which SMAC and chaddr isn't identical(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] A DHCP packet whose source MAC address and client hardware address do not match was discarded.</p> <p>This message is output once every five minutes on a port-by-port basis.</p> <p>[Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information.</p> <p><nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] Review the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.</p>
3203	WARN	ARP packet was discarded for src-mac inspection(<nif no.>/<port no.>/<vlan id>/<mac address>).	<p>[Meaning] An ARP packet whose source MAC address contained in Layer 2 header and source MAC address contained in the ARP header do not match was discarded.</p> <p>This message is output once every five minutes on a port-by-port basis.</p> <p>[Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address>: Indicates ARP terminal information.</p> <p><nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address.</p> <p>[Action] Check the connected devices because this might be caused by an attack.</p>
3204	WARN	ARP packet was discarded for dst-mac inspection(<nif no.>/<port no.>/<vlan id>/<mac address>).	<p>[Meaning] An ARP packet whose destination MAC address contained in Layer 2 header and destination MAC address contained in the ARP header do not match was discarded.</p> <p>This message is output once every five minutes on a port-by-port basis.</p> <p>[Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address>: Indicates ARP terminal information.</p> <p><nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address.</p> <p>[Action] Check the connected devices because this might be caused by an attack.</p>

Message ID	Level	Message text	Description
3205	WARN	ARP packet was discarded for ip inspection(<nif no.>/<port no.>/<vlan id>/<mac address>).	<p>[Meaning] An ARP packet that has an invalid IP address was discarded. This message is output once every five minutes on a port-by-port basis.</p> <p>[Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address>: Indicates ARP terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address.</p> <p>[Action] Check the connected devices because this might be caused by an attack.</p>
3301	WARN	DHCP packet discard with Option82(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] A packet with Option82 was discarded. This message is output once every five minutes on a port-by-port basis.</p> <p>[Explanation of message variables] ChGr:<channel group number> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] Review the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.</p>
3302	WARN	Discard of the DHCP packet which SMAC and chaddr isn't identical(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] A DHCP packet whose source MAC address and client hardware address do not match was discarded. This message is output once every five minutes on a port-by-port basis.</p> <p>[Explanation of message variables] ChGr:<channel group number> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] Review the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.</p>

Message ID	Level	Message text	Description
3303	WARN	ARP packet was discarded for src-mac inspection(ChGr:<channel group number>/<vlan id>/<mac address>).	<p>[Meaning] An ARP packet whose source MAC address contained in Layer 2 header and source MAC address contained in the ARP header do not match was discarded. This message is output once every five minutes on a port-by-port basis.</p> <p>[Explanation of message variables] ChGr:<channel group number> / <vlan id> / <mac address>: Indicates ARP terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address.</p> <p>[Action] Check the connected devices because this might be caused by an attack.</p>
3304	WARN	ARP packet was discarded for dst-mac inspection(ChGr:<channel group number>/<vlan id>/<mac address>).	<p>[Meaning] An ARP packet whose destination MAC address contained in Layer 2 header and destination MAC address contained in the ARP header do not match was discarded. This message is output once every five minutes on a port-by-port basis.</p> <p>[Explanation of message variables] ChGr:<channel group number> / <vlan id> / <mac address>: Indicates ARP terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address.</p> <p>[Action] Check the connected devices because this might be caused by an attack.</p>
3305	WARN	ARP packet was discarded for ip inspection(ChGr:<channel group number>/<vlan id>/<mac address>).	<p>[Meaning] An ARP packet that has an invalid IP address was discarded. This message is output once every five minutes on a port-by-port basis.</p> <p>[Explanation of message variables] ChGr:<channel group number> / <vlan id> / <mac address>: Indicates ARP terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address.</p> <p>[Action] Check the connected devices because this might be caused by an attack.</p>

Message ID	Level	Message text	Description
4201	ERROR	The number of the binding entry exceeded the capacity of this system(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] The number of entries in the binding database exceeds the capacity limit of the switch.</p> <p>[Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] Review the system configuration. If this message is displayed because a static entry has been added, delete the relevant static entry, and then review the system configuration.</p>
4203	ERROR	The number of the source guard entry exceeded the capacity of this system(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] The number of entries for the terminal filter exceeds the capacity limit of a Switch.</p> <p>[Explanation of message variables] <nif no.> / <port no.> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] Review the system configuration. If this message is displayed because a static entry or a channel group has been added, delete the relevant static entry or channel group, and then review the system configuration.</p>
4301	ERROR	The number of the binding entry exceeded the capacity of this system(ChGr:<channel group number>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] The number of entries in the binding database exceeds the capacity limit of the switch.</p> <p>[Explanation of message variables] ChGr:<channel group number> / <vlan id> / <mac address> / <ip address>: Indicates DHCP client terminal information. <channel group number>: Indicates the channel group number. <vlan id>: Indicates the VLAN ID. <mac address>: Indicates the MAC address. <ip address>: Indicates the IP address.</p> <p>[Action] Review the system configuration. If this message is displayed because a static entry has been added, delete the relevant static entry, and then review the system configuration.</p>

Impact on communication

None

Response messages

Table 9-12: List of response messages for the show ip dhcp snooping logging command

Message	Description
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not operating.
Program error occurred: <i><error message></i>	A program error occurred. Re-execute the command. <i><error message></i> : Location of the error

Notes

None

clear ip dhcp snooping logging

Clears log messages collected by the DHCP snooping program.

Syntax

```
clear ip dhcp snooping logging
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure shows an example of clearing log messages for the DHCP snooping.

Figure 9-8: Result of executing the command for clearing the log messages for DHCP snooping

```
> clear ip dhcp snooping logging
>
```

Display items

None

Impact on communication

None

Response messages

Table 9-13: List of response messages for the clear ip dhcp snooping logging command

Message	Description
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not operating.
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: Location of the error

Notes

None

restart dhcp snooping

Restarts the DHCP snooping program.

Syntax

```
restart dhcp snooping [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the DHCP snooping program without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

core-file

When the DHCP snooping program is restarted, the core file of the program (dhcp_snoopingd.core) is output.

Operation when this parameter is omitted:

A core file is not output.

Operation when all parameters are omitted:

Outputs the confirmation message before restarting the DHCP snooping program.

Example

Figure 9-9: Result of executing the command for restarting the DHCP snooping program

```
> restart dhcp snooping
DHCP snooping program restart OK? (y/n):y
>
```

Display items

None

Impact on communication

None

Response messages

Table 9-14: List of response messages for the restart dhcp snooping command

Message	Description
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not operating.
dhcp_snoopingd failed to restart.	An attempt to restart the DHCP snooping program failed. Re-execute the command.
Restarting dhcp_snoopingd, wait awhile.	The DHCP snooping program is being restarted. Wait a while.

Notes

1. Core output file: /usr/var/core/dhcp_snoopingd.core

2. Do not add or delete the configuration related to DHCP snooping while the DHCP snooping program is being restarted. In addition, do not use the `copy` command to copy the configuration. The binding database might become invalid.
3. Do not switch systems within 30 seconds of the DHCP snooping program restarting. In addition, do not use the `copy` command to copy the configuration. The binding database might become invalid.

dump protocols dhcp snooping

Outputs to a file logs or internal information collected by the DHCP snooping program.

Syntax

```
dump protocols dhcp snooping
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure shows an example of outputting logs or internal information for DHCP snooping to a file.

Figure 9-10: Result of executing the DHCP snooping dump command

```
> dump protocols dhcp snooping
>
```

Display items

None

Impact on communication

None

Response messages

Table 9-15: List of response messages for the dump protocols dhcp snooping command

Message	Description
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not operating.
Program error occurred: <i><error message></i>	A program error occurred. Re-execute the command. <i><error message></i> : Location of the error

Notes

Output file: /usr/var/dhsn/dhcp_snoopingd.dmp

Chapter

10. Redundancy of BCUs, CSUs, and MSUs

inactivate standby
activate standby
redundancy force-switchover
synchronize

inactivate standby

Inactivates an active standby system.

By executing this command, you can replace a standby BCU for AX6700S, a standby CSU for AX6600S, or a standby MSU for AX6300S without turning off the power.

Syntax

```
inactivate [-f] standby
```

Input mode

User mode and administrator mode

Parameters

-f

If this parameter is specified, this command is executed without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

1. The following shows an example of inactivating a standby system.

```
inactivate standby
```

2. A confirmation message appears.

```
inactivate standby system OK? (y/n):
```

If you enter *y*, the standby system is inactivated.

Display items

None

Impact on communication

None

Response messages

Table 10-1: List of response messages for the inactivate standby command

Message	Description
Can't accept command (system is busy).	The command cannot be accepted (because the system is busy). Re-execute the command later.
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Standby system is already inactive.	The standby system has already been inactivated.
Standby system is notconnect.	The standby system is not installed.

Notes

1. To restore a standby system that has been changed to *inactive* by this command to *active*, use the `activate standby` command.

2. If you execute the `inactivate standby` command, log information on the standby system is collected.
3. If you execute the `inactivate standby` command, you cannot save a configuration that is being edited.
4. If you execute the `inactivate standby` command and restart the Switch when the standby system is inactivated, the inactive state of the standby system is retained.
5. When the Switch is duplexed (redundant), if you execute the `inactivate standby` command, the `System mode changed from duplex to simplex` log message is displayed.
6. When you execute the `ppupdate` command to update the HDC (Hardware Dependent Code) of an active system, if you use the `inactivate standby` command to inactivate the standby system, the inactive state of the standby system is canceled and the standby system is activated.

activate standby

When a standby system is inactivated or after a Switch is restarted, if this command is executed while the standby system is installed, the standby system is set to the active state.

Syntax

```
activate standby
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following shows an example of setting the standby system to the active state:

```
activate standby
```

Display items

None

Impact on communication

None

Response messages

Table 10-2: List of response messages for the activate standby command

Message	Description
Can't accept command (system is busy).	The command cannot be accepted (because the system is busy). Re-execute the command later.
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Standby system is not inactive.	The standby system is not inactivated.
Standby system is notconnect.	The standby system is not installed.

Notes

It takes a few seconds for this command to re-display the prompt.

redundancy force-switchover

Replaces the active system with the standby system in a redundant configuration.

Syntax

`redundancy force-switchover`

Input mode

User mode and administrator mode

Parameters

None

Example

The following shows an example of replacing the active system with the standby system in a redundant configuration:

```
>redundancy force-switchover    Press the Enter key.
```

Display items

None

Impact on communication

- Some packets might be lost temporarily while the system is being replaced.
- To reconfigure network information after the system is replaced, communication might be lost temporarily.

Response messages

Table 10-3: List of response messages for the redundancy force-switchover command

Message	Description
Can't accept command (Active BSU is nothing).	There is no active BSU.
Can't accept command (system is busy).	The command cannot be accepted (because the system is busy). Re-execute the command later.
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Now switchover executing.	The system is being switched.
Now synchronize executing.	The <code>synchronize</code> command is being executed. Re-execute the <code>redundancy force-switchover</code> command after the <code>synchronize</code> command completes.
Now, configuration discord.	Configurations for the active system and for the standby system do not match.
Now, configuration file is editing.	The configuration file is being edited or synchronized. If it is being edited, quit editing and then re-execute the command. If it is not being edited, wait a while, and re-execute the command. Note, however, that this message might be displayed temporarily if the standby system is being started.
Now, configuration file is writing.	The configuration file is being saved or synchronized. If it is being saved, re-execute the command after the configuration is saved. If it is not being saved, wait a while, and re-execute the command. Note, however, that this message might be displayed temporarily if the standby system is being started.

Message	Description
Now, license key discord.	License keys for the active system and for the standby system do not match.
Now, power control mode changing.	Power control mode is being changed. Re-execute the command after the following log message is displayed: The change of power control mode was completed.
Standby system is failure.	A failure occurs in the standby system.
Standby system is notconnect.	The standby system is not installed.

Notes

If you switch between the active and standby systems by using this command, allow an interval of approximately 30 seconds before re-executing this command.

synchronize

Copies the following contents stored in the internal flash memory of the active system to the standby system:

1. Configurations
2. Password file
3. User account
4. Home directory
5. DUID information file of the IPv6 DHCP server
6. License key file
7. Internal Web authentication DB, user authentication information file, and the Web authentication page
8. Internal MAC-based authentication DB

Syntax

```
synchronize [{userfile | diff}]
synchronize [diff] account
```

Input mode

Administrator mode

Parameters

{userfile | diff}

userfile

Copies the files created under the home directory.

diff

Displays the synchronization status between the active system and the standby system. Specify this parameter to decide whether synchronization is required.

diff

Displays the synchronization status between the active system and the standby system. Specify this parameter to decide whether synchronization is required.

account

The synchronization status of only files related to user information (2. Password file, 3. User account, and 4. Home directory shown above) can be displayed and copied. Note that if this parameter is specified, a software version check is not performed for the active system and the standby system.

Operation when all parameters are omitted:

Files other than files created under home directories are copied.

Example

1. Synchronizes a standby system:
#synchronize
2. Displays the confirmation message asking whether to perform synchronization.
Synchronize OK? (y/n): _

If `y` is entered, synchronization starts.

If `n` is entered, the user is returned to the command prompt without performing synchronization.

#

Display items

None

Impact on communication

None

Response messages

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

Message	Description
Can't execute because operation mode is simplex now.	The command cannot be executed because the system is in simplex mode.
Can't execute for software version mismatch.	The command cannot be executed because the versions of software do not match.
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Now another user is executing user account command, please try again.	Another user is executing a user account related command. Re-execute the command after the related command completes.
Now switchover executing.	The command can not be executed because the system is being switched.
Synchronization files copy failed.	An attempt to copy the file to be synchronized failed. Wait a while, and then re-execute the command. Note, however, that if this response message is output with the <code>No space left on device</code> message, follow the step 7 in Notes below to re-execute the command.
Synchronization files open failed.	An attempt to open the file to be synchronized failed. Re-execute the command.
The command execution failed, because configuration file is editing.	This command cannot be executed because another user is editing the configuration.
There are some mismatch items.	Some items do not match.

Notes

1. When executing this command, do not allow another user to log in, log out, or execute a command. Otherwise, the command might not be terminated correctly.
2. This command cannot be executed if the versions of software for the active system and the standby system do not match. Note, however, that the command can be executed regardless of the software versions if the `account` parameter is specified.
3. If there are differences in user accounts, they become the same as the user account which is currently used. As a result, a user account for the standby system might be deleted.
4. Depending on the size of the configuration file or the number of files in the home directory, it might take time to execute the command.
5. If the `diff` parameter is specified, the `.clihistory` file in the home directory is also compared. Therefore, `NG` might be displayed for the `home directory` item.

6. If you log in to the standby system, log out first, and then execute this command.
7. If there is a file that exceeds the internal flash memory capacity in the standby system, copying a file might fail. Pay special attention if BCUs or MSUs with different internal flash memory capacities are installed in the active system and the standby system. If you failed to copy files to be synchronized, delete the files in the user area of the active and standby systems before re-executing the `synchronize` command.

Chapter

11. GSRP

```
show gsrp
show gsrp aware
clear gsrp
set gsrp master
clear gsrp port-up-delay
clear gsrp forced-shift
restart gsrp
dump protocols gsrp
```

show gsrp

Displays GSRP information.

Syntax

```
show gsrp [<gsrp group id> { vlan-group <vlan group id list> | [port <port list>]
[channel-group-number <channel group list>] } ] [detail]
```

Input mode

User mode and administrator mode

Parameters

<gsrp group id> { vlan-group <vlan group id list> | [port <port list>] [channel-group-number <channel group list>] }

<gsrp group id>

Displays GSRP information for the specified GSRP group ID.

The specifiable values are from 1 to 65535.

vlan-group <vlan group id list>

Displays GSRP information for the specified VLAN group ID.

The specifiable values are from 1 to 128.

[port <port list>] [channel-group-number <channel group list>]

Displays GSRP information about the specified port or the specified channel group. The port and the channel group can be specified at the same time. In that case, GSRP information for the specified port and the specified channel group is displayed.

port <port list>

For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*. Ports configured as direct link ports, and ports belonging to VLANs that are part of VLAN groups can be specified.

channel-group-number <channel group list>

For details about how to specify <channel group list>, see *Specifiable values for parameters*. IDs for channel groups configured as direct links and for channel groups belonging to VLANs that are part of VLAN groups can be specified.

Operation when this parameter is omitted:

All GSRP information is displayed.

detail

Displays detailed information about GSRP.

The display contents are the same when a VLAN group is specified.

Operation when this parameter is omitted:

Displays summary information about GSRP.

Operation when all parameters are omitted:

All GSRP summary information is displayed.

Example 1

Figure 11-1: Example of displaying GSRP summary information

```

> show gsrp
Date 2006/03/14 12:00:00 UTC

GSRP ID: 3
Local MAC Address      : 0012.e2a8.2527
Neighbor MAC Address   : 0012.e2a8.2505
Total VLAN Group Counts : 3
Layer 3 Redundancy     : On

VLAN Group ID   Local State   Neighbor State
1               Backup       Master
2               (disable)    -
8               Master       -

```

Display items in Example 1

Table 11-1: Items displayed for GSRP summary information

Item	Meaning	Displayed information
GSRP ID	GSRP group ID	1 to 65535
Local MAC Address	MAC address of the Switch	--
Neighbor MAC Address	MAC address of the partner switch	- is displayed if the partner switch is unknown.
Total VLAN Group Counts	Total number of VLAN groups in the Switch	0 to 128
Layer 3 Redundancy	Layer 3 redundancy switching	Off: Not set. On: The Layer 3 redundancy switching functionality is enabled.
VLAN Group ID	VLAN group ID	1 to 128
Local State	Status of VLAN groups on the Switch	Master: Indicates master status. Backup: Indicates backup status. Backup(Lock): Indicates backup (fixed) status. Backup(Waiting): Indicates backup (master wait) status. Backup(No Neighbor): Indicates backup (neighbor unknown) status. (disable) Indicates disabled status.
Neighbor State	Status of VLAN groups on the partner switch	Master: Indicates master status. Backup: Indicates backup status. Backup(Lock): Indicates backup (fixed) status. Backup(Waiting): Indicates backup (master wait) status. Backup(No Neighbor): Indicates backup (neighbor unknown) status. (- is displayed if the partner switch is unknown.)

Example 2

Figure 11-2: Example of displaying GSRP information when a VLAN group ID is specified

11. GSRP

```
> show gsrp 3 vlan-group 1,2,8
Date 2006/03/14 12:00:00 UTC
```

GSRP ID: 3

```
Local MAC Address      : 0012.e2a8.2527
Neighbor MAC Address   : 0012.e2a8.2505
Total VLAN Group Counts : 3
Layer 3 Redundancy     : On
```

VLAN Group ID : 1

```
VLAN ID      : 110,200-2169
Member Port   : 1/6-8
Active Port   : 1/6-8
Last Transition : 2006/03/14 10:00:00 (Master to Backup)
Transition by reason : Priority was lower than neighbor's
Master to Backup Counts : 4
Backup to Master Counts : 4
Virtual MAC Address : 0000.8758.1387
```

	Local	Neighbor
State	: Backup	Master
Acknowledged State	: Backup	-
Advertise Hold Timer	: 3	-
Priority	: 100	101
Active Ports	: 3	3
Up Ports	: 3	-

VLAN Group ID : 2

```
VLAN ID      : 120
Member Port   : -
Active Port   : -
Last Transition : - ( - )
Transition by reason : -
Master to Backup Counts : -
Backup to Master Counts : -
Virtual MAC Address : 0000.8758.138f
```

	Local	Neighbor
State	: (disable)	-
Acknowledged State	: -	-
Advertise Hold Timer	: -	-
Priority	: 100	-
Active Ports	: -	-
Up Ports	: -	-

VLAN Group ID : 8

```
VLAN ID      : 180
Member Port   : 1/6-8
Active Port   : 1/6-8
Last Transition : 2006/03/14 11:00:00 (Backup to Master)
Transition by reason : "set gsrp master"command was executed
Master to Backup Counts : 0
Backup to Master Counts : 1
Virtual MAC Address : 0000.8758.13bf
```

	Local	Neighbor
State	: Master	-
Acknowledged State	: -	-
Advertise Hold Timer	: 0	-
Priority	: 100	-
Active Ports	: 3	-
Up Ports	: 3	-

>

Display items in Example 2

Table 11-2: Items displayed for GSRP information when a VLAN group ID is specified

Item	Meaning	Displayed information
GSRP ID	GSRP group ID	1 to 65535
Local MAC Address	MAC address of the Switch	--
Neighbor MAC Address	MAC address of the partner switch	- is displayed if the partner switch is unknown.
Total VLAN Group Counts	Total number of VLAN groups in the Switch	0 to 128
Layer 3 Redundancy	Layer 3 redundancy switching	off: Not set. on: The Layer 3 redundancy switching functionality is enabled.
VLAN Group ID	VLAN group ID	1 to 128
VLAN ID	VLAN ID	1 to 4095 When used in combination with Ring Protocol, VLANs that do not belong to the VLAN group are not included.
Member Port	Ports belonging to a VLAN which is configured for a VLAN group	- is displayed if no active ports belong to a VLAN group, or if the VLAN group is disabled.
Active Port	Active port	- is displayed if no active ports belong to a VLAN group, or if the VLAN group is disabled. Note, however, that a ring port is not counted as an active port.
Last Transition	Last state transition time	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second The state transition is shown within parentheses. - is displayed if no state transitions have been performed, or if the VLAN group is disabled.

Item	Meaning	Displayed information
Transition by reason	Reason for the state transition	<p>Active ports was more than neighbor's: The number of active ports on the Switch is greater than the number of active ports on the partner switch. Priority was higher than neighbor's.: The priority of the Switch is higher than that of the partner switch.</p> <p>MAC address was larger than neighbor's: The MAC address of the Switch is greater than that of the partner switch.</p> <p>"set gsrp master" command was executed: The set gsrp master command was executed.</p> <p>Direct link failure was detected: A direct link failure was detected.</p> <p>Forced shift time was expired The automatic master transition wait time elapsed.</p> <p>Active ports was less than neighbor's: The number of active ports in the Switch is smaller than the number of active ports in the partner switch.</p> <p>Priority was lower than neighbor's: The priority of the Switch is lower than that of the partner switch.</p> <p>MAC address was smaller than neighbor's: The MAC address of the Switch is smaller than that of the partner switch.</p> <p>BackupLock was enabled: backup-lock was set.</p> <p>Double Master was detected: It was detected that the Switch and the partner switch were in master status.</p> <p>- is displayed if no state transitions have been performed, or the port is disabled. Also, when the GSRP device does not recognize the partner switch in master state, if the restart vlan command is executed, - is displayed.</p>
Master to Backup Counts	Number of transitions from master status to backup status (statistics)	0 to 4294967295 - is displayed if the VLAN group is disabled.
Backup to Master Counts	Number of transitions from backup status to master status (statistics)	0 to 4294967295 - is displayed if the VLAN group is disabled.
Virtual MAC Address	Virtual MAC address	- is displayed when the Layer 3 redundancy switching functionality is not set.
Local	Information about the Switch	--
Neighbor	Information about the partner switch	- is displayed if the partner switch is unknown.

Item	Meaning	Displayed information
State	VLAN group status	Master: Indicates master status. Backup: Indicates backup status. Backup(Lock): Indicates backup (fixed) status. Backup(Waiting): Indicates backup (master wait) status. Backup(No Neighbor): Indicates backup (neighbor unknown) status. (disable): Indicates disabled status.
Acknowledged State	Status of a VLAN group on the Switch which is recognized by the partner switch	Master: Indicates master status. Backup: Indicates backup status. Backup(Lock): Indicates backup (fixed) status. Backup(Waiting): Indicates backup (master wait) status. Backup(No Neighbor): Indicates backup (neighbor unknown) status. - is displayed if the partner switch is unknown or disabled. (- is displayed for information about the partner switch.)
Advertise Hold Timer	Length of time that an Advertise frame continues to be active	0 to 120 (seconds) - is displayed if the VLAN group is disabled. (- is displayed for information about the partner switch.)
Priority	Priority information	0 to 255 (The greater the value, the higher the priority.)
Active Ports	Number of active ports	0 to the maximum number of ports per switch. - is displayed if the VLAN group is disabled. Note, however, that a ring port is not counted as an active port.
Up Ports	Number of enabled ports belonging to a VLAN that is configured to be in a VLAN group	0 to the maximum number of ports per switch. - is displayed if the VLAN group is disabled. (- is displayed for information about the partner switch.)

Example 3

Figure 11-3: Example of displaying detailed GSRP information

```

> show gsrp detail
Date 2008/11/07 12:00:00 UTC

GSRP ID: 3
Local MAC Address      : 0012.e2a8.2527
Neighbor MAC Address   : 0012.e2a8.2505
Total VLAN Group Counts : 3
GSRP VLAN ID          : 105
Direct Port            : 1/10-11
Limit Control          : Off
GSRP Exception Port    : 1/1-5
No Neighbor To Master  : manual
Backup Lock            : disable
Port Up Delay          : 0
Last Flush Receive Time : -
Forced Shift Time      : -

```

```

Layer 3 Redundancy      : On
Virtual Link ID        : 100 (VLAN ID : 20)

Advertise Hold Time     Local      Neighbor
Advertise Hold Timer    : 5        5
Advertise Interval      : 4        -
Selection Pattern       : 1        1
                        : ports-priority-mac  ports-priority-mac

VLAN Group ID          Local State      Neighbor State
1                      Backup           Master
2                      (disable)        -
8                      Master           -
>

```

Display items in Example 3

Table 11-3: Items displayed for detailed GSRP information

Item	Meaning	Displayed information
GSRP ID	GSRP group ID	1 to 65535
Local MAC Address	MAC address of the Switch	--
Neighbor MAC Address	MAC address of the partner switch	- is displayed if the partner switch is unknown.
Total VLAN Group Counts	Total number of VLAN groups in the Switch	0 to 128
GSRP VLAN ID	VLAN ID used for transmitting Advertise frames	1 to 4095
Direct Port	Port used for transmitting Advertise frames	- is displayed if the port is not configured.
Limit Control	Functionality restricting GSRP control to VLANs that are in VLAN groups	Off: Not set. On: The functionality restricting GSRP control to VLANs that are in VLAN groups is being applied.
GSRP Exception Port	Port which is not subject to GSRP control	- is displayed if the port is not configured. When used with Ring Protocol, if a ring port is configured, it is displayed as Exception Port.
No Neighbor To Master	Operation setting in backup (neighbor unknown) status	manual: Until a GSRP Advertise frame is received or a master transition command is executed, backup (neighbor unknown) status continues. direct-down: If a direct link goes down, it automatically transitions to master status.
Backup Lock	backup-lock configuration setting	enable: backup-lock configuration is set. disable: backup-lock configuration is not set.
Port Up Delay	Delay time until an active port becomes subject to be counted when the line is enabled	0 to 43200 (seconds) or infinity (infinity means unlimited.)
Last Flush Receive Time	Time when the last GSRP Flush request frame was received	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second - is displayed if no GSRP Flush request frames were received.

Item	Meaning	Displayed information
Forced Shift Time	Automatic master transition wait time delay	-: Not set. 0 to 3600 (seconds) During the transition wait time, the time until the transition will occur is displayed in the following form: (Now Waiting, 20Sec, left)
Layer 3 Redundancy	Layer 3 redundancy switching	off: Not set. on: The Layer 3 redundancy switching functionality is enabled.
Virtual Link ID	Virtual link ID	1 to 250 - is displayed if no virtual link IDs are set. Information enclosed in parentheses indicates the virtual link VLAN ID.
Local	Information about the Switch	--
Neighbor	Information about the partner switch	- is displayed if the partner switch is unknown.
Advertise Hold Time	Retention time of an Advertise frame	1 to 120 (seconds) (The value set by using the <code>advertise-holdtime</code> configuration command is displayed.)
Advertise Hold Timer	Length of time that an Advertise frame continues to be active	0 to 120 (seconds) (- is displayed for information about the partner switch.)
Advertise Interval	Transmission interval between Advertise frames	0.5 to 60 (seconds)
Selection Pattern	Method for selecting the master or backup state	ports-priority-mac: The number of active ports, the priority, and the MAC address of the Switch are selected in that order. priority-ports-mac: The priority, the number of active ports, and the MAC address of the Switch are selected in that order.
VLAN Group ID	VLAN group ID	1 to 128
Local State	Status of VLAN groups on the Switch	Master: Indicates master status. Backup: Indicates backup status. Backup(Lock): Indicates backup (fixed) status. Backup(Waiting): Indicates backup (master wait) status. Backup(No Neighbor): Indicates backup (neighbor unknown) status. (disable): Indicates disabled status.
Neighbor State	Status of VLAN groups on the partner switch	Master: Indicates master status. Backup: Indicates backup status. Backup(Lock): Indicates backup (fixed) status. Backup(Waiting): Indicates backup (master wait) status. Backup(No Neighbor): Indicates backup (neighbor unknown) status (- is displayed if the partner switch is unknown).

Example 4

Figure 11-4: Example of displaying GSRP information when a port is specified

```
> show gsrp 10 port 1/6-11
Date 2006/03/14 12:00:00 UTC

GSRP ID: 10
Port Information
1/6      GSRP      : Active      Port      : Up
        Type      : Member      Flush      : Reset      Delay      : 0
        TxFrame    : 0           RxFrame    : 0           Discard Frame : 0
1/7      GSRP      : Active      Port      : Up
        Type      : Member      Flush      : Reset      Delay      : 0
        TxFrame    : 0           RxFrame    : 0           Discard Frame : 0
1/8      GSRP      : Active      Port      : Up
        Type      : Member      Flush      : GSRP      Delay      : 0
        TxFrame    : 0           RxFrame    : 0           Discard Frame : 0
1/10     GSRP      : Not Active   Port      : Up
(CH: 1) Type      : Direct      Flush      : No           Delay      : 0
        TxFrame    : 960        RxFrame    : 954        Discard Frame : 0
1/11     GSRP      : Not Active   Port      : Up
(CH: 1) Type      : Direct      Flush      : No           Delay      : 0
        TxFrame    : 960        RxFrame    : 954        Discard Frame : 0

>
```

Display items in Example 4

Table 11-4: Items displayed for GSRP information when a port is specified

Item	Meaning	Displayed information
GSRP ID	GSRP group ID	1 to 65535
Port Information	Port information	--
<nif no.>/<port no.>	Port number	--
CH	Channel group number	--
GSRP	Status of a port belonging to a VLAN configured for a VLAN group or a port belonging to a GSRP-management VLAN	Active: Indicates that the port status is active Not Active: Indicates that the port status is not active.
Port	Port status	Up: Indicates that the port is up. Down: Indicates that the port is down.
Type	Port type	Direct: Indicates that the port is a direct link port. Member: Indicates that the port belongs to a VLAN configured for a VLAN group.
Flush	Method of clearing mac_address_table for neighboring switches	GSRP: The GSRP Flush request frame is sent. Reset: The port reset functionality is used. No: The GSRP Flush request frame is not sent.

Item	Meaning	Displayed information
Delay	Delay time until an active port becomes subject to be counted when the line is enabled	Indicates the remaining time until a port belonging to a VLAN set for a VLAN group becomes an active port. 0 to 43200 (seconds) or infinity
TxFram	Number of sent GSRP Advrtise frames (statistics)	0 to 4294967295
RxFram	Number of received GSRP Advrtise frames (statistics)	0 to 4294967295
Discard Frame	Number of GSRP Advrtise frames discarded when they are received (statistics)	0 to 262140 (The maximum value is 65535 (the maximum number by reason why the frame is discarded) times 4 (the number of components).)

Example 5

Figure 11-5: Example of displaying detailed GSRP information when a port is specified

```
> show gsrp 10 port 1/6 detail
Date 2006/03/14 12:00:00 UTC

GSRP ID: 10
Port Information
1/6      GSRP      : Active      Port      : Up
        Type      : Member      Flush     : Reset      Delay      : 0
        TxFram    : 0           RxFrame   : 0         Discard Frame : 0
        Discard Frame by reason
          mismatch GSRP VLAN ID : 0
          mismatch GSRP ID      : 0
          loopback GSRP frame   : 0
          illegal GSRP frame    : 0

>
```

Display items in Example 5

Table 11-5: Items displayed for GSRP information when a port is specified

Item	Meaning	Displayed information
GSRP ID	GSRP group ID	1 to 65535
Port Information	Port information	--
<nif no.>/<port no.>	Port number	--
CH	Channel group number	--
GSRP	Status of a port belonging to a VLAN which is configured for a VLAN group	Active: Indicates that the port status is active Not Active: Indicates that the port status is not active.
Port	Port status	Up: Indicates that the port is up. Down: Indicates that the port is down.

Item	Meaning	Displayed information
Type	Port type	Direct: Indicates that the port is a direct link port. Member: Indicates that the port belongs to a VLAN configured for a VLAN group.
Flush	Method of clearing <code>mac_address_table</code> for neighboring switches	GSRP: The GSRP Flush request frame is sent. Reset: The port reset functionality is used. No: The GSRP Flush request frame is not sent.
Delay	Delay time until an active port becomes subject to be counted when the line is enabled	Indicates the remaining time until a port belonging to a VLAN set for a VLAN group becomes an active port. 0 to 43200 (seconds) or <i>infinity</i>
TxFram	Number of sent GSRP Advertise frames (statistics)	0 to 4294967295
RxFram	Number of received GSRP Advertise frames (statistics)	0 to 4294967295
Discard Frame	Number of GSRP Advertise frames discarded when they are received (statistics)	0 to 262140 (The maximum value is 65535 (the maximum number by reason why the frame is discarded) times 4 (the number of components).)
Discard Frame by reason	Detailed statistics for discarded frames by reason	--
mismatch GSRP VLAN ID	Number of GSRP Advertise frames discarded due to GSRP-management VLAN ID mismatch (statistics)	0 to 65535
mismatch GSRP ID	Number of GSRP Advertise frames discarded due to GSRP ID mismatch (statistics)	0 to 65535 Note: Counted only if frames are transmitted via a direct link.
loopback GSRP frame	Number of GSRP Advertise frames discarded because a GSRP Advertise frame sent from the Switch was received (statistics)	0 to 65535
illegal GSRP frame	Number of GSRP Advertise frames discarded because an invalid GSRP Advertise frame was received. (statistics)	0 to 65535

Impact on communication

None

Response messages

Table 11-6: List of response messages for the show gsrp command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to GSRP program.	Communication with the GSRP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart gsrp</code> command to restart the GSRP program.
GSRP is not configured.	GSRP has not been configured. Check the configuration.
Specified GSRP ID is not configured: <i><gsrp group id></i> .	The specified GSRP group ID has not been configured. <i><gsrp group id></i> : Indicates the GSRP group ID.
Specified port is not operational. :	The specified port and channel group are not active.
Specified VLAN group ID is not configured: <i><vlan group id></i> .	The specified VLAN group ID has not been configured. <i><vlan group id></i> : Indicates the VLAN group ID.

Notes

The counter will no longer be updated when statistics reach the maximum value.

show gsrp aware

Displays GSRP aware information.

Syntax

show gsrp aware

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 11-6: Example of displaying the show gsrp aware command

```
> show gsrp aware
Date 2006/03/14 12:00:00 UTC

Last mac_address_table Flush Time : 2006/03/14 11:00:00
GSRP Flush Request Parameters :
  GSRP ID : 10          VLAN Group ID : 1    Port : 1/8
  Source MAC Address : 0012.e2a8.2527

>
```

Display items

Table 11-7: Items displayed for GSRP aware information

Item	Meaning	Displayed 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 ID	1 to 65535
VLAN Group ID	VLAN group ID for the received GSRP Flush request frame	1 to 128 (Indicates the ID of the VLAN group for which the master and backup were switched.)
Port	Port on which a GSRP Flush request frame was received	--
Source MAC Address	MAC address from which the received GSRP Flush request frame was sent	--

Impact on communication

None

Response messages

Table 11-8: List of response messages for the show gsrp aware command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to GSRP program.	Communication with the GSRP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart gsrp</code> command to restart the GSRP program.
No received flush request frame.	No GSRP Flush request frames were received.

Notes

Receiving a GSRP Flush request frame clears all `mac_address_table` for every VLAN group IDs.

clear gsrp

Clears the GSRP statistics.

Syntax

```
clear gsrp [<gsrp group id> { vlan-group <vlan group id list> | [port <port list>]
[channel-group-number <channel group list>] } ]
```

Input mode

User mode and administrator mode

Parameters

<gsrp group id> { vlan-group <vlan group id list> | [port <port list>] [channel-group-number <channel group list>] }

<gsrp group id>

Clears all statistics for GSRP relating to the specified GSRP group ID.

Specifiable values for GSRP group IDs are from 1 to 65535.

vlan-group <vlan group id list>

Clears statistics for GSRP relating to the specified VLAN group ID.

The specifiable values are from 1 to 128.

The items to be cleared are Master to Backup Counts and Backup to Master Counts.

[port <port list>] [channel-group-number <channel group list>]

Clears statistics for GSRP relating to the specified port or channel group. Both port and channel groups can be specified at the same time. In this case, GSRP statistics for the specified port and statistics for the specified channel group are cleared.

Operation when this parameter is omitted:

Clears statistics for GSRP relating to all ports and channel groups.

port <port list>

Clears statistics for GSRP relating to the specified port.

The items to be cleared are TxFrame, RxFrame, Discard Frame, mismatch GSRP VLAN ID, mismatch GSRP ID, loopback GSRP frame, and illegal GSRP frame.

For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Clears statistics for GSRP relating to the specified channel group.

The items to be cleared are TxFrame, RxFrame, Discard Frame, mismatch GSRP VLAN ID, mismatch GSRP ID, loopback GSRP frame, and illegal GSRP frame. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Clears all GSRP statistics.

Example

Figure 11-7: Example of clearing all GSRP statistics

```
> clear gsrp
>
```

Figure 11-8: Example of clearing GSRP statistics when a VLAN group ID is specified

```

> show gsrp 10 vlan-group 1
Date 2006/03/14 12:00:00 UTC

GSRP ID: 10
Local MAC Address      : 0012.e2a8.2527
Neighbor MAC Address   : 0012.e2a8.2505
Total VLAN Group Counts : 1

VLAN Group ID : 1
VLAN ID          : 110,200-2169
Member Port      : 1/6-8
Active Port      : 1/6-8
Last Transition   : 2006/03/14 10:00:00 (Master to Backup)
Transition by reason : Priority was lower than neighbor's
Master to Backup Counts : 4
Backup to Master Counts : 4

State              Local      Neighbor
Acknowledged State : Backup    Master
Advertise Hold Timer : 3        -
Priority           : 100      101
Active Ports       : 3        3
Up Ports           : 3        -

> clear gsrp 10 vlan-group 1

> show gsrp 10 vlan-group 1
Date 2006/03/14 12:00:00 UTC

GSRP ID: 10
Local MAC Address      : 0012.e2a8.2527
Neighbor MAC Address   : 0012.e2a8.2505
Total VLAN Group Counts : 1

VLAN Group ID : 1
VLAN ID          : 110,200-2169
Member Port      : 1/6-8
Active Port      : 1/6-8
Last Transition   : 2006/03/14 10:00:00 (Master to Backup)
Transition by reason : Priority was lower than neighbor's
Master to Backup Counts : 0
Backup to Master Counts : 0

State              Local      Neighbor
Acknowledged State : Backup    Master
Advertise Hold Timer : 3        -
Priority           : 100      101
Active Ports       : 3        3
Up Ports           : 3        -

```

Figure 11-9: Example of clearing GSRP statistics when a port is specified

```

> show gsrp 10 port 1/10 detail
Date 2006/03/14 12:00:00 UTC

GSRP ID: 10
Port Information
1/10 GSRP : Not Active Port : Up
(CH: 1) Type : Direct Flush : No Delay : 0
TxFrame : 1027 RxFrame : 1020 Discard Frame : 2
Discard Frame by reason
mismatch GSRP VLAN ID : 1
mismatch GSRP ID : 1
loopback GSRP frame : 0

```

```

        illegal GSRP frame          : 0

> clear gsrp 10 port 1/10

> show gsrp 10 port 1/10 detail
Date 2006/03/14 12:00:00 UTC

GSRP ID: 10
Port Information
1/10    GSRP      : Not Active Port    : Up
(CH: 1) Type      : Direct      Flush   : No          Delay          : 0
        TxFrame   : 0           RxFrame  : 0          Discard Frame   : 0
        Discard Frame by reason
        mismatch GSRP VLAN ID      : 0
        mismatch GSRP ID           : 0
        loopback GSRP frame        : 0
        illegal GSRP frame         : 0

```

Display items

None

Impact on communication

None

Response messages

Table 11-9: List of response messages for the clear gsrp command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to GSRP program.	Communication with the GSRP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart gsrp</code> command to restart the GSRP program.
GSRP is not configured.	GSRP has not been configured. Check the configuration.
Specified GSRP ID is not configured:<gsrp group id>.	The specified GSRP group ID has not been configured. <gsrp group id>: Indicates the GSRP group ID.
Specified port is not operational. :	The specified port and channel group are not active.
Specified VLAN group ID is not configured:<vlan group id>.	The specified VLAN group ID has not been configured. <vlan group id>: Indicates the VLAN group ID.

Notes

- Even if statistics are cleared, the value for the MIB information obtained by using SNMP is not cleared.
- If the configuration is deleted or added, the target statistics are cleared.

set gsrp master

Changes backup (neighbor unknown) status to master status.

This command is effective only for backup (neighbor unknown) status.

Syntax

```
set gsrp master <gsrp group id> vlan-group <vlan group id> [-f]
```

Input mode

User mode and administrator mode

Parameters

<gsrp group id>

Specify a GSRP group ID.

Specifiable values for GSRP group IDs are in the range from 1 to 65535.

<vlan group id>

After a confirmation message is output, changes the status of the specified VLAN group ID to master status.

Specifiable values for a VLAN group ID are from 1 to 128.

-f

Switches the status to master status without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Example

Figure 11-10: Example of executing a master transition command

```
> set gsrp master 10 vlan-group 8
Transit to Master. Are you sure? (y/n):y
> set gsrp master 10 vlan-group 8 -f
>
```

Display items

None

Impact on communication

The status is switched from communication disabled to communication enabled.

Response messages

Table 11-10: List of response messages for the set gsrp master command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to GSRP program.	Communication with the GSRP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart gsrp</code> command to restart the GSRP program.

Message	Description
GSRP is not configured.	GSRP has not been configured. Check the configuration.
Specified GSRP ID is not configured:<gsrp group id>	The specified GSRP group ID has not been configured. <gsrp group id>: Indicates the GSRP group ID.
Specified VLAN group ID is not configured:<vlan group id>.	The specified VLAN group ID has not been configured. <vlan group id>: Indicates the VLAN group ID.
Specified VLAN group is not no neighbor state.	The specified VLAN group is not in backup (neighbor unknown) status. Use the <code>show gsrp</code> command to make sure the specified VLAN group is in backup (neighbor unknown) status before re-executing the <code>set gsrp master</code> command.

Notes

Execute this command after making sure the applicable VLAN group of the partner switch is in backup status.

clear gsrp port-up-delay

Immediately puts the specified port, which is both active and belongs to a VLAN that is configured to be a member of a VLAN group, in active port status without waiting for the delay time that was specified using the `port-up-delay` configuration command.

Syntax

```
clear gsrp port-up-delay [port <port list>] [channel-group-number <channel group list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Immediately puts a specified port, which is both active and belongs to a VLAN that is configured to be a member of a VLAN group, in active status. 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>

Immediately puts a specified channel group, which is both active and belongs to a VLAN that is configured to be a member of a VLAN group, in active status. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when all parameters are omitted:

Immediately puts all ports, which are both active and belongs to a VLAN that is configured to be a member of a VLAN group, in active status.

Example

Figure 11-11: Example of executing the clear gsrp port-up-delay command

```
> show gsrp 10 port 1/6-10
Date 2006/03/14 12:00:00 UTC

GSRP ID: 10
Port Information
1/6      GSRP      : Not Active Port      : Up
        Type      : Member   Flush      : Reset      Delay      : 43172
        TxFrame    : 0        RxFrame    : 0        Discard Frame : 0
1/7      GSRP      : Not Active Port      : Up
        Type      : Member   Flush      : Reset      Delay      : 43174
        TxFrame    : 0        RxFrame    : 0        Discard Frame : 0
1/8      GSRP      : Active    Port      : Up
        Type      : Member   Flush      : GSRP      Delay      : 0
        TxFrame    : 0        RxFrame    : 0        Discard Frame : 0
1/10     GSRP      : Not Active Port      : Up
(CH: 1) Type      : Direct   Flush      : No        Delay      : 0
        TxFrame    : 1993    RxFrame    : 1987    Discard Frame : 0

> clear gsrp port-up-delay

> show gsrp 10 port 1/6-10
Date 2006/03/14 12:00:00 UTC

GSRP ID: 10
Port Information
1/6      GSRP      : Active    Port      : Up
        Type      : Member   Flush      : Reset      Delay      : 0
        TxFrame    : 0        RxFrame    : 0        Discard Frame : 0
1/7      GSRP      : Active    Port      : Up
```

11. GSRP

```

      Type      : Member      Flush   : Reset      Delay       : 0
      TxFrame   : 0           RxFrame : 0           Discard Frame : 0
1/8  GSRP      : Active      Port    : Up
      Type      : Member      Flush   : GSRP      Delay       : 0
      TxFrame   : 0           RxFrame : 0           Discard Frame : 0
1/10 GSRP      : Not Active Port    : Up
(CH: 1) Type    : Direct      Flush   : No          Delay       : 0
      TxFrame   : 2073        RxFrame : 2068        Discard Frame : 0
```

>

Figure 11-12: Example of executing the port-up-delay command when a port is specified

```
> show gsrp 10 port 1/6
Date 2006/03/14 12:00:00 UTC

GSRP ID: 10
Port Information
1/6  GSRP      : Not Active Port    : Up
      Type      : Member      Flush   : Reset      Delay       : 43180
      TxFrame   : 0           RxFrame : 0           Discard Frame : 0

> clear gsrp port-up-delay port 1/6

> show gsrp 10 port 1/6
Date 2006/03/14 12:00:00 UTC

GSRP ID: 10
Port Information
1/6  GSRP      : Active      Port    : Up
      Type      : Member      Flush   : Reset      Delay       : 0
      TxFrame   : 0           RxFrame : 0           Discard Frame : 0

>
```

Display items

None

Impact on communication

None

Response messages

Table 11-11: List of response messages for the clear gsrp port-up-delay command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to GSRP program.	Communication with the GSRP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart gsrp</code> command to restart the GSRP program.
GSRP is not configured.	GSRP has not been configured. Check the configuration.
Specified port is not operational. :	The specified port and channel group are not active.

Notes

None

clear gsrp forced-shift

Disables the automatic-transition-to-master and associated wait (delay) that usually applies when a GSRP switch is independently started. The current status of the VLAN group remains unchanged, and the GSRP switch is not changed to master status next time it is independently started.

This command is valid until the status is changed to master status automatically by the master transition functionality the GSRP switch is independently started.

Syntax

```
clear gsrp forced-shift [<gsrp group id>]
```

Input mode

User mode and administrator mode

Parameters

<gsrp group id>

For the designated GSRP group ID, disables the automatic-transition-to-master and associated wait (delay). If wait status is disabled, the current status of the VLAN group remains unchanged, and the GSRP switch is not automatically changed to master status.

Specifiable values for GSRP group IDs are from 1 to 65535.

Operation when this parameter is omitted:

For all GSRP groups, disables the automatic-transition-to-master and associated wait (delay). If wait status is disabled, the current status of the VLAN group remains unchanged, and the GSRP switch is not automatically changed to master status.

Example

Figure 11-13: Example of executing the command for canceling the automatic master transition wait state

```
> clear gsrp forced-shift 1
>
```

Display items

None

Impact on communication

None

Response messages

Table 11-12: List of response messages for the clear gsrp forced-shift command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to GSRP program.	Communication with the GSRP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart gsrp</code> command to restart the GSRP program.
GSRP is not configured.	GSRP has not been configured. Check the configuration.

Message	Description
Specified GSRP ID is not configured:< <i>gsrp group id</i> >	The specified GSRP group ID has not been configured. < <i>gsrp group id</i> >: Indicates the GSRP group ID.

Notes

None

restart gsrp

Restarts the GSRP program.

Syntax

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

Input mode

User mode and administrator mode

Parameters

-f

Restarts the GSRP program without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file when the program is restarted.

Operation when this parameter is omitted:

A core file is not output.

Operation when all parameters are omitted:

Restarts the GSRP program after displaying a confirmation message.

Example

Figure 11-14: Example of restarting GSRP

```
> restart gsrp

gsrp program restart OK? (y/n):y
>

> restart gsrp -f
>
```

Display items

None

Impact on communication

Frames cannot be received in VLANs belonging to a VLAN group of GSRP.

Response messages

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

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
GSRP program failed to be restarted.	An attempt to restart the GSRP program by using this command failed. Re-execute the command.

Notes

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

Storage directory: /usr/var/core/

Core file: `gsrpd.core`

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

dump protocols gsrp

Dumps detailed event trace information and control table information collected by the GSRP program to a file.

Syntax

```
dump protocols gsrp
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 11-15: Example of executing GSRP dump

```
> dump protocols gsrp
>
```

Display items

None

Impact on communication

None

Response messages

Table 11-14: List of response messages for the dump protocols gsrp command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to GSRP program.	Communication with the GSRP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart gsrp</code> command to restart the GSRP program.
File open error.	An attempt to open or access a dump file failed.

Notes

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

Storage directory: `/usr/var/gsrp/`

File: `gsrp_dump.gz`

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

Chapter

12. VRRP

```
show vrrpstatus (IPv4)
clear vrrpstatus (IPv4)
swap vrrp (IPv4)
show vrrpstatus (IPv6)
clear vrrpstatus (IPv6)
swap vrrp (IPv6)
show track (IPv4)
show track (IPv6)
```

show vrrpstatus (IPv4)

Displays the VRRP virtual router status and the VRRP-management VLAN status.

Syntax

```
show vrrpstatus [ { vrrp-vlan | [detail][statistics][group][protocol ip]
                   [ { name <virtual router name> | interface vlan <vlan id>
                     [vrid <vrid>] } ] } ]
```

Input mode

User mode and administrator mode

Parameters

vrrp-vlan

Displays information about a VRRP-management VLAN.

[detail][statistics][group]

detail

Displays detailed information about the virtual router status.

statistics

Display statistics for virtual routers.

group

Displays group information.

Operation when this parameter is omitted:

Displays information about the virtual router status.

[protocol ip] [{ name <virtual router name> | interface vlan <vlan id> [vrid <vrid>] }]

protocol ip

Displays information about an IPv4 protocol virtual router.

Operation when this parameter is omitted:

Displays information about both IPv4 and IPv6-protocol virtual routers.

name <virtual router name>

Specifies a virtual router name.

interface vlan <vlan id>

Specifies the interface that is used to configure the virtual router.

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

vrid <vrid>

Specifies the router ID.

Operation when this parameter is omitted:

Displays information about all virtual routers that are configured by that VLAN.

Operation when this parameter is omitted:

Displays information about all virtual routers.

Operation when all parameters are omitted:

Displays a list of virtual routers, and information about their statuses.

Example 1

Figure 12-1: Example of displaying summary information about IPv4 protocol virtual routers

```
> show vrrpstatus protocol ip      Press the Enter key.
Date 2008/12/15 12:00:00 UTC
VLAN0010 VRID 1 VRF 2 MASTER virtual-ip 170.10.10.2 priority 150/150 primary
VRRPNAME1
VLAN0020 VRID 1 MASTER virtual-ip 170.10.10.4 follow VRRPNAME1
VLAN0030 VRID 2 BACKUP virtual-ip 170.10.10.3 priority 100/100
>
```

Display items in Example 1

Table 12-1: Items displayed in the summary information about IPv4 protocol virtual routers

Item	Meaning		Displayed information
<i><interface name> VRID <vrid> [VRF <vrf id>] <state> virtual-ip <virtual ip address> {priority <priority> /<original priority> [primary <virtual router name>] follow <primary virtual router name>}</i>			
Summary information	<i><interface name></i>	Name of the interface where a virtual router is operating	--
	VRID <vrid>	Virtual router ID	--
	VRF <vrf id> [OP-NPAR]	VRF ID	Not displayed if the virtual router is operating in a global network.
	<state>	Current status of a virtual router	MASTER: Indicates the master status. BACKUP: Indicates the backup status. INITIAL: Indicates the initial status. Standby virtual routers are in the INITIAL status.
	virtual-ip <virtual ip address>	Virtual IP address	--
	priority <priority> /<original priority>	Virtual router priority	<priority>: Indicates the current virtual router priority. <original priority>: Indicates the priority set in the configuration. If configuration settings are omitted, the initial value, 100, is displayed.
	primary <virtual router name>	Virtual router name	If the virtual router name is not set, or the router is a follower virtual router, this item is not displayed.
	follow <primary virtual router name>	Name of a followed primary virtual router	For a follower virtual router, the name is displayed.

Example 2

Figure 12-2: Example of displaying VRRP-management VLANs

```
> show vrrpstatus vrrp-vlan      Press the Enter key.
Date 2008/12/15 12:00:00 UTC
vrrp-vlan                        : VLAN0010
Flush Request Frame sent         : 3 (Mon Dec 15 11:05:01 2008)
>
```

Display items in Example 2

Table 12-2: Items displayed for VRRP-management VLANs

Item	Meaning	Displayed information
vrrp-vlan : <interface name>	Name of the interface specified as the VRRP-management VLAN	--
Flush Request Frame sent : <number of frame> [(<date>)]	Number of times that Flush Request frames were sent, and the time when such a frame was last sent	<number of frame>: Indicates the number of times that Flush Request frames were sent. <date>: Indicates the time when such a frame was last sent. If the Flush Request frame has not been sent, the time when a frame was last sent is not displayed.

Example 3

Figure 12-3: Example of displaying the detailed virtual router status (for primary virtual routers)

```
> show vrrpstatus detail interface vlan 10 vrid 1    Press the Enter key.
Date 2009/07/15 12:00:00 UTC
VLAN0010: VRID 1 VRF 2
  Virtual Router IP Address : 170.10.10.2
  Virtual MAC Address : 0000.5e00.0101
  Virtual Router Name : VRRPNAME1 (primary)
  Virtual Router Follow :-
  Number of Follow virtual routers : 4
  Current State : MASTER
  Admin State : enable
  Priority : 80 /100
  IP Address Count : 1
  Master Router's IP Address : 170.10.10.2
  Primary IP Address : 170.10.10.1
  Authentication Type : SIMPLE TEXT PASSWORD(Disable)
  Authentication Key : ABCDEFG(Disable)
  Advertisement Interval : 250 msec
  Master Advertisement Interval : 1000 msec
  Preempt Mode : ON
  Preempt Delay : 60
  Non Preempt swap timer : 30
  Accept Mode : ON
  Virtual Router Up Time : Mon Jun  8 16:55:00 2009
  track 10 VLAN0022 VRF 3 Status : (IF UP) Down Priority : 50
    Target Address : 192.168.0.20
    Vrrp Polling Status : reachable
  track 20 VLAN0023 Status : (IF UP) Down Priority : 40
  track 30 gigabitethernet 1/10 Status : (IF DOWN) Down Priority : 20
  track 40 port-channel 2 Status : (IF UP) Down Priority : 20
  IPv4 Advertisement Type :ietf-unified-spec-02-mode
>
```

Figure 12-4: Example of displaying the detailed virtual router status (for follower virtual routers)

```
> show vrrpstatus detail interface vlan 10 vrid 2    Press the Enter key.
Date 2009/07/15 12:00:00 UTC
VLAN0010: VRID 2 VRF 2
  Virtual Router IP Address : 170.10.10.2
  Virtual MAC Address : 0000.5e00.0102
  Virtual Router Name : VRRPNAME2 (follow )
  Virtual Router Follow :VRRPNAME1 (VLAN0010: VRID 1 VRF 2 )
  Number of Follow virtual routers : 0
  Current State : MASTER
```

```

Admin State : enable
Priority : -/100(Disable)
IP Address Count : 1
Master Router's IP Address : -
Primary IP Address : 170.10.10.1
Authentication Type : SIMPLE TEXT PASSWORD(Disable)
Authentication Key : ABCDEFG(Disable)
Advertisement Interval : 250 msec (Disable)
Master Advertisement Interval : -(Disable)
Preempt Mode : ON(Disable)
Preempt Delay : 60(Disable)
Non Preempt swap timer :30(Disable)
Accept Mode : ON
Virtual Router Up Time : Mon Jun  8 16:55:00 2009
track 10 VLAN0022 VRF 3 Status : (Disable) Down Priority : 50
    Target Address : 192.168.0.20
    Vrrp Polling Status : (Disable)
track 20 VLAN0023  Status : (Disable) Down Priority : 40
track 30 gigabitethernet 1/10 Status : (Disable) Down Priority : 20
track 40 port-channel 2 Status : (Disable) Down Priority : 20
IPv4 Advertisement Type :ietf-unified-spec-02-mode(Disable)
>

```

Display items in Example 3

Table 12-3: Items displayed for the virtual router status

Item	Meaning	Displayed information
<code><interface name> : VRID</code> <code><vrid> [VRF <vrf id>]</code>	Name of the interface where a virtual router is operating, and its VRID information	<code><interface name></code> : Indicates the name of the interface where the virtual router is operating. <code><vrid></code> : Indicates the virtual router ID. VRF <code><vrf id></code> : Indicates the VRF ID. Not displayed if the virtual router is operating in a global network. [OP-NPAR]
Virtual Router IP Address : <code><ip address> [(ADDRESS OWNER)]</code>	IP address of the virtual router	(ADDRESS OWNER) : Displayed if the user is the owner of the address.
Virtual MAC Address : <code><mac address></code>	MAC address of a virtual router	--
Virtual Router Name : <code><virtual router name></code> ({primary follow})	Virtual router name	{primary follow}: Indicates the type of the virtual router.
Virtual Router Follow : <code><virtual router name></code> ({<interface name> : VRID <vrid> [VRF <vrf id>]not running})	Name of a followed primary virtual router	<code><virtual router name></code> : - is displayed for a primary virtual router. For a follower virtual router, the name of the followed primary virtual router is displayed. <code><interface name></code> : Indicates the name of the interface where a primary virtual router is operating. <code><vrid></code> : Indicates the virtual router ID of the primary virtual router. VRF <code><vrf id></code> : Indicates the VRF ID of the primary virtual router. This item is not displayed if the primary virtual router is operating in a global network. [OP-NPAR] not running: A primary virtual router with the specified name was not found.

Item	Meaning	Displayed information
Number of Follow virtual routers : <N>	Number of follower virtual routers	N: Indicates a value from 0 to 4094.
Current State : <status>	Current status of a virtual router	MASTER: Indicates the master status. BACKUP: Indicates the backup status. INITIAL: Indicates the initial status. Standby virtual routers are in the INITIAL status.
Admin State : [enable disable <flag>]	Current operating status of a virtual router	enable: Indicates that the virtual router is operating. disable: Indicates that the virtual router is not operating. <flag>: Indicates the reason why the virtual router is not operating. (IF DOWN) : Indicates that the status of the applicable interface is DOWN. (TRACK DOWN) : The priority was set to 0 by the tracking functionality. (PRIMARY DISABLE) : The primary virtual router is disabled or not defined. (NOIP) : The IP address of the applicable interface was not set. (NOJOIN) : An attempt to join a multicast group failed. (S/W FAIL) : An attempt to register a virtual MAC address in the hardware failed.
Priority : <priority>/<original priority> [(Disable)]	Virtual router priority	<priority>: Indicates the current virtual router priority. - is displayed for a follower virtual router or a standby router. <original priority>: Indicates the priority set in the configuration. If configuration settings are omitted, the initial value, 100, is displayed. (Disable): Indicates that the operation is invalid. For a follower virtual router or a standby router, this functionality is invalid. For a primary virtual router, this item is not displayed.
IP Address Count : <N>	Number of virtual router IP addresses	--
Master Router's IP Address : <ip address>	IP address of a router currently in the master status	- is displayed for a follower virtual router.
Primary IP Address : <ip address>	IP address of an interface for which VRRP is configured	--
Authentication Type : <type>[(Disable)]	Packet authentication type	NONE: No packet authentication is performed. SIMPLE TEXT PASSWORD: Indicates a text password. (Disable): Indicates that the operation is invalid. For a follower virtual router, this functionality is disabled. This functionality is also disabled if the router is not supported in VRRP operation mode.
Authentication Key : <text>[(Disable)]	Text password	(Disable): Indicates that the operation is invalid. For a follower virtual router, this functionality is disabled. This functionality is also disabled if the router is not supported in VRRP operation mode.

Item	Meaning	Displayed information
Advertisement Interval : <N> {sec msec} [(Disable)]	Interval for sending ADVERTISEMENT packets	1 to 255 seconds, or 250 to 40950 ms. (Disable) : Indicates that the operation is invalid. For a follower virtual router, this functionality is disabled. For a primary virtual router, this item is not displayed.
Master Advertisement Interval : { <milli second> msec - (Disable) }	Interval for sending ADVERTISEMENT packets as a master device (in ms)	10 to 40950 (Disable) : Indicates that the operation is invalid. This functionality is disabled if VRRP operation mode is other than ietf-unified-spec-02-mode.
Preempt Mode : {ON OFF} [(Disable)]	Automatic switch-back setting	ON: Indicates that the automatic switch-back functionality is enabled. OFF: Indicates that the automatic switch-back functionality is suppressed. (Disable) : Indicates that the operation is invalid. For a follower virtual router, this functionality is disabled. For a primary virtual router, this item is not displayed.
Preempt Delay : <second> [(Now Waiting, <N> sec left)] [(Disable)]	Suppression timer setting period (seconds)	(Now Waiting, <N> sec left): Displays the remaining time until the state is changed to master while switching to master is suppressed by this setting. N: Indicates a value from 1 to 65535. (Disable) : Indicates that the operation is invalid. For a follower virtual router, this functionality is disabled. For a primary virtual router, this item is not displayed.
Non Preempt swap timer : <second> [(Now Waiting, <N> sec left)] [(Disable)]	Switch-back suppression time (in seconds) while automatic switch-back is suppressed	(Now Waiting, <N> sec left): Displays the remaining time until the state is changed to master while switching to master is suppressed by this setting. N: Indicates a value from 1 to 65535. (Disable) : Indicates that the operation is invalid. For a follower virtual router, this functionality is disabled. For a primary virtual router, this item is not displayed.
Accept Mode : {ON OFF}	Accept mode	ON: Indicates accept mode. OFF: Indicates that accept mode is turned off. For an address owner, - is displayed regardless of the address mode setting.
Virtual Router Up Time : <time string>	Time when a virtual router is changed from the INITIAL status	This item is not displayed if the virtual router is in the INITIAL status.

Item	Meaning	Displayed information
track <track-number> {<interface name> [VRF <vrf id>]<interface type> <interface number>} Status : <status> {Down Priority Critical Priority} : <priority>	Information about a track assigned to a virtual router	<track-number>: Indicates the number of the track assigned to a virtual router. <interface name>: Indicates the interface name of the VLAN interface that monitors for failures. VRF <vrf id>: Indicates the VRF ID. When the destination for VRRP polling is a global network, this item is not displayed. [OP-NPAR] <interface type> <interface number>: Indicates an interface that monitors for failures. gigabitethernet <nif no.> / <port no.>: Indicates a 10BASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X interface that monitors failures. tengigabitethernet <nif no.> / <port no.>: Indicates a 10GBASE-R interface that monitors for failures. port-channel <channel group number>: Indicates a channel-group interface that monitors for failures. <status>: Indicates the current status of an interface that monitors failures. (IF UP): Indicates that the interface is in the UP status. (IF DOWN): Indicates that the interface is in the DOWN status. (Disable): Indicates that the track assigned to a virtual router is disabled. Method for changing priority Down Priority : <priority>: Indicates the priority is decreased if an interface that monitors failures is in the DOWN status. Critical Priority : <priority>: Indicates the priority to be replaced when the interface that monitors failures is in the DOWN status.
Target Address : <target-address> [(check reply interface)]	Destination address for VRRP polling	<target-address>: Indicates the target address for VRRP polling. This item is not displayed if the IP address for VRRP polling has not been specified, or for an interface that monitors failures. (check reply interface): This information is displayed if the track check-reply-interface configuration command has been used to configure this.

Item	Meaning	Displayed information
Vrrp Polling Status : <status>[<reason>]	VRRP polling information	<p>This item is not displayed if the IP address for VRRP polling has not been specified, or for an interface that monitors failures.</p> <p><status>: Indicates connectivity by VRRP polling. reachable: Indicates that communication is possible. (Disable): Indicates that the operation is invalid. unreachable: Indicates that communication is impossible.</p> <p><reason>: Provides a detailed reason why communication is impossible. This information is displayed if <status> is unreachable. (interface down): Indicates that the source interface for polling is in the DOWN status. (no response): Indicates that there were no responses from the polling destination. (no route): Indicates that there are no routes to the polling destination. (invalid response): When the track check-reply-interface configuration command is set, responses from the interface that sent the polling request and also from another interface were received.</p>
IPv4 Advertisement Type : <type>[(Disable)]	Type of sending ADVERTISEMENT packets	<p>rfc3768-mode: Sends ADVERTISEMENT packets that conform to RFC 3768. ietf-unified-spec-02-mode: Sends ADVERTISEMENT packets according to draft-ietf-vrrp-unified-spec-02.</p> <p>(Disable): Indicates that the operation is invalid. For a follower virtual router, this functionality is disabled. For a primary virtual router, this item is not displayed.</p>

Example 4

Figure 12-5: Example of displaying virtual router statistics

```

> show vrrpstatus statistics interface vlan 10 vrid 1    Press the Enter key.
Date 2009/07/15 12:00:00 UTC
VLAN0010: VRID 1 VRF 2
  5 times transitions to master
  1500 advertisement received
    0 with bad advertisement interval
    0 with authentication failed
    0 with bad ip ttl
    3 with priority zero
    0 with invalid type
    0 with bad ip address list
    0 with bad authentication type
    0 with authentication type mismatch
    0 with packet length error
    0 with different VRRP version
    0 with low priority
  1300 advertisement sent
    0 with priority zero
  1 virtual MAC learning frame sent
  0 change by command
  0 change by interface down
  0 change by receiving advertisement with high priority
  0 change by Master_Down_Timer timeout
  0 master transition delay count
  track 10 VLAN0022 VRF 3 Target-Address : 192.168.0.20
    VRRP Polling round-trip min/avg/max = 0.266/0.274/0.286 ms

```

```

1 priority down by detected
track 20 VLAN0023 line-protocol
0 priority down by detected
track 30 gigabitethernet 1/10 line-protocol
0 priority down by detected
track 40 port-channel 2 line-protocol
0 priority down by detected

```

>

Display items in Example 4

Table 12-4: Items displayed for virtual router statistics

Item	Meaning	Displayed information
<interface name> : VRID <vrid> [VRF <vrf id>]	Name of the interface where a virtual router is operating, and its VRID information	<p><interface name>: Indicates the name of the interface where the virtual router is operating.</p> <p><vrid>: Indicates the virtual router ID.</p> <p>VRF <vrf id>: Indicates the VRF ID. Not displayed if the virtual router is operating in a global network. [OP-NPAR]</p>
<number of packets> times transitions to master	Number of transitions to the master status	--
<number of packets> advertisement received	Number of received ADVERTISEMENT packets	--
<number of packets> with bad advertisement interval	Number of received ADVERTISEMENT packets that have invalid packet-sending intervals	--
<number of packets> with authentication failed	Number of received ADVERTISEMENT packets of which authentication failed	--
<number of packets> with bad ip ttl	Number of received ADVERTISEMENT packets whose TTL for the IP header is not 255	--
<number of packets> with priority zero	Number of received ADVERTISEMENT packets whose priority level is 0	--
<number of packets> with invalid type	Number of received packets that had an invalid type field	--
<number of packets> with bad ip address list	Number of received ADVERTISEMENT packets that have invalid virtual router IPv4 addresses	--
<number of packets> with bad authentication type	Number of received ADVERTISEMENT packets with invalid packet authentication types	--
<number of packets> with authentication type mismatch	Number of received ADVERTISEMENT packets whose packet authentication type did not match the local setting.	--

Item	Meaning	Displayed information
<number of packets> with packet length error	Number of received ADVERTISEMENT packets whose packet length was invalid	--
<number of packets> with different VRRP version	Number of received packets whose version of ADVERTISEMENT packets and that of VRRP operation mode do not match	--
<number of packets> with low priority	Number of received ADVERTISEMENT packets with lower priority	--
<number of packets> advertisement sent	Number of sent ADVERTISEMENT packets	--
<number of packets> with priority zero	Number of sent ADVERTISEMENT packets whose priority is 0	--
<number of frames> virtual MAC learning frame sent	Number of sent MAC address learning frames	--
<N> change by command	Number of times that the <code>swap vrrp</code> command was executed	--
<N> change by interface down	Number of status transitions due to interface going down	--
<N> change by receiving advertisement with high priority	Number of status transitions caused by receipt of a high priority ADVERTISEMENT packet	--
<N> change by Master_Down_Timer timeout	Number of status transitions because the Master Down Timer timed out	--
<N> master transition delay count	Number of times that the suppression timer has been started	--

Item	Meaning	Displayed information
track <track-number> {<interface name> [VRF <vrf id>] <interface type> <interface number>} {Target-Address : <target-address> line-protocol}	VRRP polling information assigned to a virtual router	<p><track-number>: Indicates the number of the track assigned to a virtual router.</p> <p><interface name>: Indicates the name of an interface that monitors failures.</p> <p>VRF <vrf id>: Indicates the VRF ID. When the destination for VRRP polling is a global network, this item is not displayed. [OP-NPAR]</p> <p><interface type> <interface number>: Indicates an interface that monitors for failures.</p> <p>gigabitethernet <nif no.> / <port no.>: Indicates a 10BASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X interface that monitors failures.</p> <p>tengigabitethernet <nif no.> / <port no.>: Indicates a 10GBASE-R interface that monitors for failures.</p> <p>port-channel <channel group number>: Indicates a channel-group interface that monitors for failures.</p> <p>Target-Address : <target-address>: Indicates the destination IP address for VRRP polling.</p> <p>line-protocol: Applied to an interface that monitors failures.</p>
VRRP Polling round-trip min/avg/max =<minimum>/<average>/<maximum> ms	Packet response time for VRRP polling	<p>This item is not displayed if the IP address for VRRP polling has not been specified, or for an interface that monitors failures.</p> <p><minimum> / <average> / <maximum>: Indicates the minimum value, average value, and maximum value.</p>
<N> priority down by detected	Number of times that the priority has been decreased due to a track error	--

Example 5

Figure 12-6: Example of displaying virtual router group information (for primary virtual routers)

```

> show vrrpstatus group name VRRPNAME1    Press the Enter key.
Date 2008/12/15 12:00:00 UTC
VLAN0010: VRID 1 VRF 2
  Virtual Router Name          : VRRPNAME1 (primary)
  Virtual Router Follow       : -
  Number of Follow virtual routers : 4
  Followed by virtual routers :
    VLAN0020: VRID 1 VRF 2

```

```
VLAN0030: VRID 1 VRF 2
VLAN0040: VRID 1 VRF 2
VLAN0050: VRID 1 VRF 2
```

Figure 12-7: Example of displaying virtual router group information (for follower virtual routers)

```
> show vrrpstatus group interface vlan 10 vrid 1    Press the Enter key.
Date 2008/12/15 12:00:00 UTC
VLAN0020: VRID 1 VRF 2
  Virtual Router Name           : VRRPNAME2 (follow)
  Virtual Router Follow         : VRRPNAME1 (VLAN0010: VRID 1 VRF 2 )
  Number of Follow virtual routers: 0
  Followed by virtual routers   : -
```

Display items in Example 5

Table 12-5: Items displayed for virtual router group information

Item	Meaning	Displayed information
<i><interface name></i> : VRID <i><vrid></i> [VRF <i><vrf id></i>]	Name of the interface where a virtual router is operating, and its VRID information	<i><interface name></i> : Indicates the name of the interface where the virtual router is operating. <i><vrid></i> : Indicates the virtual router ID. VRF <i><vrf id></i> : Indicates the VRF ID. Not displayed if the virtual router is operating in a global network. [OP-NPAR]
Virtual Router Name : <i><virtual router name></i> ({primary follow})	Virtual router name	{primary follow}: Indicates the type of the virtual router.
Virtual Router Follow : <i><virtual router name></i> ({ <i><interface name></i> : VRID <i><vrid></i> [VRF <i><vrf id></i>]} not running})	Name of a followed primary virtual router	<i><virtual router name></i> : - is displayed for a primary virtual router. For a follower virtual router, the name of the followed primary virtual router is displayed. <i><interface name></i> : Indicates the name of the interface where a primary virtual router is operating. <i><vrid></i> : Indicates the virtual router ID of the primary virtual router. VRF <i><vrf id></i> : Indicates the VRF ID of the primary virtual router. This item is not displayed if the primary virtual router is operating in a global network. [OP-NPAR] not running: A primary virtual router with the specified name was not found.
Number of Follow virtual routers : <i><N></i>	Number of follower virtual routers	--

Item	Meaning	Displayed information
Followed by virtual routers: <i><interface name></i> : VRID <i><vrid></i> [VRF <i><vrf id></i>]	List of follower virtual routers	<p>- is displayed for a follower virtual router.</p> <p><i><interface name></i>: Indicates the name of an interface where a follow virtual router is operating.</p> <p><i><vrid></i>: Indicates the virtual router ID.</p> <p>VRF <i><vrf id></i>: Indicates the VRF ID. Not displayed if the virtual router is operating in a global network. [OP-NPAR]</p>

Impact on communication

None

Response messages

Table 12-6: List of response messages for the show vrrpstatus(IPv4) command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
no entries.	There are no applicable virtual routers.
Vrrp-vlan disable because virtual router is not configured.	The VRRP-management VLAN is disabled because no virtual routers are configured.
Vrrp-vlan not configured.	The VRRP-management VLAN has not been configured.

Notes

None

clear vrrpstatus (IPv4)

Clears the counter for VRRP virtual router statistics and the counter for VRRP-management VLAN statistics.

Syntax

```
clear vrrpstatus [ { vrrp-vlan | [protocol ip] [{ name <virtual router name> |
interface vlan <vlan id> [vrid <vrid>] }] } ]
```

Input mode

User mode and administrator mode

Parameters

vrrp-vlan

Clears statistics for VRRP-management VLANs.

[protocol ip] [{ name <virtual router name> | interface vlan <vlan id> [vrid <vrid>] }]

protocol ip

Clears the IPv4 protocol virtual router statistics.

Operation when this parameter is omitted:

Clears the statistics for both IPv4 and IPv6-protocol virtual routers.

name <virtual router name>

Specifies a virtual router name.

interface vlan <vlan id>

Specifies the interface that is used to configure the virtual router.

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

vrid <vrid>

Specifies the router ID.

Operation when this parameter is omitted:

Clears all virtual router information configured via the VLAN.

Operation when all parameters are omitted:

Clears the counter for all virtual router statistics.

Example

Figure 12-8: Example of clearing the counter for virtual router statistics

```
> clear vrrpstatus interface vlan 10 vrid 1    Press the Enter key.
>
```

Figure 12-9: Example of clearing the counter for VRRP-management VLAN statistics

```
> clear vrrpstatus vrrp-vlan    Press the Enter key.
>
```

Display items

None

Impact on communication

None

Response messages

Table 12-7: List of response messages for the clear vrrpstatus(IPv4) command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
no entries.	There are no applicable virtual routers.
Vrrp-vlan disable because virtual router is not configured.	The VRRP-management VLAN is disabled because no virtual routers are configured.
Vrrp-vlan not configured.	The VRRP-management VLAN has not been configured.

Notes

None

swap vrrp (IPv4)

Changes the device status when switch-back is suppressed.

If the device is in the master status, it is changed to the backup status.

If the device is in the backup status, it is changed to the master status.

Syntax

```
swap vrrp [-f] { name <virtual router name> | interface vlan <vlan id> [vrid <vrid>]
}
```

Input mode

User mode and administrator mode

Parameters

-f

Executes the command without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

name <virtual router name>

Specifies a virtual router name.

interface vlan <vlan id>

Specifies the interface that is used to configure the virtual router.

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

vrid <vrid>

Specifies the router ID.

Operation when this parameter is omitted:

Displays confirmation messages for the virtual routers configured for the specified interface.

Example

The following figure shows how to change VRID 1 and VRID 20 virtual routers that are configured for VLAN 10, which are currently operating in the master status, to the backup status.

Figure 12-10: Example of performing switch-back for virtual routers

```
> swap vrrp interface vlan 10
Exchange VRRP 1 OK? (y/n): y
Exchange VRRP 20 OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Response messages

Table 12-8: List of response messages for the `swap vrrp(IPv4)` command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Command execution cannot be performed to follow virtual router.	This command cannot be executed for follower virtual routers.
Command execution cannot be performed to owner's virtual router of an initial state.	This command cannot be executed for virtual routers in the initial status.
Command execution cannot be performed to owner's virtual router.	This command cannot be executed for the virtual router of the address owner.
no entries.	There are no applicable virtual routers.

Notes

- If this command is executed from a virtual router that has lower or equal priority (including the default priority), the device status might not be changed to the master status.
- This command cannot be entered for an address owner's virtual router, a follower virtual router, or a virtual router in the initial status.
- If a switch-back command is executed while switch-back is suppressed, the command is given priority and switch-back is performed.
- If the command is executed when switch-back is not suppressed, switch-back is performed, even though that does not seem to be the case because the status of the virtual router with the higher priority is changed to the master status by the automatic switch-back functionality.
- When the command is executed, both virtual routers are swapped to the backup or master status temporarily, but they are changed back to the master or backup status automatically.
- When switch-back cannot be performed due to a failure of other devices, if the command is executed, communication is suspended for 4 seconds by default.
- In a configuration where the `no vrrp preempt` and the `vrrp timers non-preempt-swap` configuration commands are set for all devices that make up the VRRP, if a switch-back command is executed in the master device, all devices change to the backup status until the period set for the `vrrp timers non-preempt-swap` command elapses. To avoid this situation, do not set the `vrrp timers non-preempt-swap` command for at least one of the devices that makes up the VRRP. If all the devices are in the backup status, you can make one of the devices the master device by executing the `swap vrrp` command and specifying the device.

The table below lists the results of executing this command. No status change in the following table indicates situation where it does not seem that switch-back is performed.

Table 12-9: List of execution results for the swap vrrp(IPv4) command

--			Local device is being suppressed		Local device is not suppressed	
			Another device is being suppressed	Another device is not being suppressed	Another device is being suppressed	Another device is not being suppressed
Local device (Master)	Comparison of the priority for the local device and another device	High	Switched	Switched	No status change	No status change
		Equal	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.
		Low	Switch-back	Switch-back	Switch-back	Switch-back
Local device (Backup)		High	Switch-back	Switch-back	Switch-back	Switch-back
		Equal	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.
		Low	No status change	No status change	No status change	No status change

Terms used in the above table:

- Local device: A device in which the `swap vrrp` command is executed.
- Another device: A device other than the local device.
- Switched: The priority of the master local device is changed from high to low.

show vrrpstatus (IPv6)

Displays the VRRP virtual router status and the VRRP-management VLAN status.

Syntax

```
show vrrpstatus [ { vrrp-vlan | [detail][statistics] [group] [protocol ipv6]
                  [ { name <virtual router name> | interface vlan <vlan id>
                    [vrid <vrid>] } ] } ]
```

Input mode

User mode and administrator mode

Parameters

vrrp-vlan

Displays information about a VRRP-management VLAN.

[detail][statistics][group]

detail

Displays detailed information about the virtual router status.

statistics

Display statistics for virtual routers.

group

Displays group information.

Operation when this parameter is omitted:

Displays information about the virtual router status.

[protocol ipv6] [{ name <virtual router name> | interface vlan <vlan id> [vrid <vrid>] }]

protocol ipv6

Displays information about an IPv6-protocol virtual router.

Operation when this parameter is omitted:

Displays information about both IPv4 and IPv6-protocol virtual routers.

name <virtual router name>

Specifies a virtual router name.

interface vlan <vlan id>

Specifies the interface that is used to configure the virtual router.

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

vrid <vrid>

Specifies the router ID.

Operation when this parameter is omitted:

Displays information about all virtual routers that are configured by that VLAN.

Operation when this parameter is omitted:

Displays information about all virtual routers.

Operation when all parameters are omitted:

Displays a list of virtual routers, and information about their statuses.

Example 1

Figure 12-11: Example of displaying summary information about IPv6-protocol virtual routers

```
> show vrrpstatus protocol ipv6      Press the Enter key.
Date 2009/07/15 12:00:00 UTC
VLAN0010 VRID 1 VRF 2 MASTER virtual-ip 100:0:11::100 priority 150/150 primary
VRRPNAME1
VLAN0012 VRID 1 MASTER virtual-ip 100:0:12::100 follow VRRPNAME1
VLAN0013 VRID 1 BACKUP virtual-ip 100:0:13::100 priority 100/100
>
```

Display items in Example 1

Table 12-10: Items displayed in the summary information about IPv6-protocol virtual routers

Item	Meaning	Displayed information	
<interface name> VRID <vrid> [VRF <vrf id>] <state> virtual-ip <virtual ip address> {priority <priority>}/<original priority> [primary <virtual router name>] follow <primary virtual router name>}			
Summary information	<interface name>	Name of the interface where a virtual router is operating	--
	VRID <vrid>	Virtual router ID	--
	VRF <vrf id> [OP-NPAR]	VRF ID	Not displayed if the virtual router is operating in a global network.
	<state>	Current status of a virtual router	MASTER: Indicates the master status. BACKUP: Indicates the backup status. INITIAL: Indicates the initial status. Standby virtual routers are in the INITIAL status.
	virtual-ip <virtual ip address>	Virtual IP address	--
	priority <priority>/<original priority>	Virtual router priority	<priority>: Indicates the current virtual router priority. <original priority>: Indicates the priority set in the configuration. If configuration settings are omitted, the initial value, 100, is displayed.
	primary <virtual router name>	Virtual router name	If the virtual router name is not set, or the router is a follower virtual router, this item is not displayed.
	follow <primary virtual router name>	Name of a followed primary virtual router	For a follower virtual router, the name is displayed.

Example 2

Figure 12-12: Example of displaying VRRP-management VLANs

```
> show vrrpstatus vrrp-vlan      Press the Enter key.
Date 2008/12/15 12:00:00 UTC
vrrp-vlan                        : VLAN0010
Flush Request Frame sent         : 3 (Mon Dec 15 11:05:01 2008)
>
```

Display items in Example 2

Table 12-11: Items displayed for VRRP-management VLANs

Item	Meaning	Displayed information
vrrp-vlan : <interface name>	Name of the interface specified as the VRRP-management VLAN	--
Flush Request Frame sent : <number of frame> [(<date>)]	Number of times that Flush Request frames were sent, and the time when such a frame was last sent	<p><number of frame>: Indicates the number of times that Flush Request frames were sent.</p> <p><date>: Indicates the time when such a frame was last sent. If the Flush Request frame has not been sent, the time when a frame was last sent is not displayed.</p>

Example 3

Figure 12-13: Example of displaying the detailed virtual router status (for primary virtual routers)

```
> show vrrpstatus detail interface vlan 10 vrid 3    Press the Enter key.
Date 2009/07/15 12:00:00 UTC
VLAN0010: VRID 3 VRF 2
  Virtual Router IP Address : fe80::1234
  Virtual MAC Address : 0000.5e00.0203
  Virtual Router Name : VRRPNAME1 (primary)
  Virtual Router Follow : -
  Number of Follow virtual routers : 4
  Current State : MASTER
  Admin State : enable
  Priority : 100/120
  IP Address Count : 1
  Master Router's IP Address : fe80::abcd
  Primary IP Address : fe80::abcd
  Authentication Type : SIMPLE TEXT PASSWORD(Disable)
  Authentication Key : ABCDEFG(Disable)
  Advertisement Interval : 250 msec
  Master Advertisement Interval :1000 msec
  Preempt Mode : ON
  Preempt Delay : 60
  Non Preempt swap timer : 30
  Accept Mode : ON
  Virtual Router Up Time : Mon Jun  8 16:55:00 2009
  track 10 VLAN0022 VRF 3 Status : (IF UP) Down Priority : 50
    Target Address : fe80::ba
    Vrrp Polling Status : reachable
  track 30 gigabitethernet 1/10 Status : (IF DOWN) Down Priority : 20
  track 40 port-channel 2 Status : (IF UP) Down Priority : 20
  IPv6 Advertisement Type : ietf-unified-spec-02-mode
>
```

Figure 12-14: Example of displaying the detailed virtual router status (for follower virtual routers)

```
> show vrrpstatus detail interface vlan 10 vrid 3    Press the Enter key.
Date 2009/07/15 12:00:00 UTC
VLAN0010: VRID 3 VRF 2
  Virtual Router IP Address : fe80::1234
  Virtual MAC Address : 0000.5e00.0203
  Virtual Router Name : VRRPNAME2 (follow)
  Virtual Router Follow : VRRPNAME1 (VLAN0010: VRID 1 VRF 2)
  Number of Follow virtual routers : 0
  Current State : MASTER
  Admin State : enable
```

```

Priority : -/120(Disable)
IP Address Count : 1
Master Router's IP Address : -
Primary IP Address : fe80::abcd
Authentication Type : SIMPLE TEXT PASSWORD(Disable)
Authentication Key : ABCDEFG(Disable)
Advertisement Interval : 250 msec(Disable)
Master Advertisement Interval : -(Disable)
Preempt Mode : ON(Disable)
Preempt Delay : 60(Disable)
Non Preempt swap timer : 30(Disable)
Accept Mode : ON
Virtual Router Up Time : Mon Jun  8 16:55:00 2009
track 10 VLAN0022 VRF 3 Status : (Disable) Down Priority : 50
    Target Address : fe80::ba
    Vrrp Polling Status : (Disable)
track 30 gigabitethernet 1/10 Status : (Disable) Down Priority : 20
track 40 port-channel 2 Status : (Disable) Down Priority : 20
IPv6 Advertisement Type : ietf-unified-spec-02-mode(Disable)

```

>

Display items in Example 3

Table 12-12: Items displayed for the virtual router status

Item	Meaning	Displayed information
<i><interface name></i> : VRID <i><vrid></i> [VRF <i><vrf id></i>]	Name of the interface where a virtual router is operating, and its VRID information	<i><interface name></i> : Indicates the name of the interface where the virtual router is operating. <i><vrid></i> : Indicates the virtual router ID. VRF <i><vrf id></i> : Indicates the VRF ID. Not displayed if the virtual router is operating in a global network. [OP-NPAR]
Virtual Router IP Address : <i><ip address></i> [(ADDRESS OWNER)]	IP address of the virtual router	(ADDRESS OWNER): Displayed if the user is the owner of the address.
Virtual MAC Address : <i><mac address></i>	MAC address of a virtual router	--
Virtual Router Name : <i><virtual router name></i> (<i>{primary follow}</i>)	Virtual router name	<i>{primary follow}</i> : Indicates the type of the virtual router.
Virtual Router Follow : <i><virtual router name></i> (<i>{<interface name></i> : VRID <i><vrid></i> [VRF <i><vrf id></i>]}not running)	Name of a followed primary virtual router	<i><virtual router name></i> : - is displayed for a primary virtual router. For a follower virtual router, the name of the followed primary virtual router is displayed. <i><interface name></i> : Indicates the name of the interface where a primary virtual router is operating. <i><vrid></i> : Indicates the virtual router ID of the primary virtual router. VRF <i><vrf id></i> : Indicates the VRF ID of the primary virtual router. This item is not displayed if the primary virtual router is operating in a global network. [OP-NPAR] not running: A primary virtual router with the specified name was not found.

Item	Meaning	Displayed information
Number of Follow virtual routers : <N>	Number of follower virtual routers	N: Indicates a value from 0 to 4094.
Current State : <status>	Current status of a virtual router	MASTER: Indicates the master status. BACKUP: Indicates the backup status. INITIAL: Indicates the initial status. Standby virtual routers are in the INITIAL status.
Admin State : [enable disable<flag>]	Current operating status of a virtual router	enable: Indicates that the virtual router is operating. disable: Indicates that the virtual router is not operating. <flag>: Indicates the reason why the virtual router is not operating. (IF DOWN): Indicates that the status of the applicable interface is DOWN. (TRACK DOWN): The priority was set to 0 by the tracking functionality. (PRIMARY DISABLE): The primary virtual router is disabled or not defined. (NOIP): The IP address of the applicable interface was not set. (NOJOIN): An attempt to join a multicast group failed. (S/W FAIL): An attempt to register a virtual MAC address in the hardware failed.
Priority : <priority>/<original priority>[(Disable)]	Virtual router priority	<priority>: Indicates the current virtual router priority. - is displayed for a follower virtual router or a standby router. <original priority>: Indicates the priority set in the configuration. If configuration settings are omitted, the initial value, 100, is displayed. (Disable): Indicates that the operation is invalid. For a follower virtual router or a standby router, this functionality is invalid. For a primary virtual router, this item is not displayed.
IP Address Count : <N>	Number of virtual router IP addresses	--
Master Router's IP Address : <ip address>	IP address of a router currently in the master status	- is displayed for a follower virtual router.
Primary IP Address: <ip address>	IP address of an interface for which VRRP is configured	--
Authentication Type : <type>[(Disable)]	Packet authentication type	NONE: No packet authentication is performed. SIMPLE TEXT PASSWORD: Indicates a text password. (Disable): Indicates that the operation is invalid. For a follower virtual router, this functionality is disabled. This functionality is also disabled if the router is not supported in VRRP operation mode.
Authentication Key : <text>[(Disable)]	Text password	(Disable): Indicates that the operation is invalid. For a follower virtual router, this functionality is disabled. This functionality is also disabled if the router is not supported in VRRP operation mode.

Item	Meaning	Displayed information
Advertisement Interval : <N> {sec msec} [(Disable)]	Interval for sending ADVERTISEMENT packets	1 to 255 seconds, or 250 to 40950 ms. (Disable): Indicates that the operation is invalid. For a follower virtual router, this functionality is disabled. For a primary virtual router, this item is not displayed.
Master Advertisement Interval : { <milli second> msec - (Disable) }	Interval for sending ADVERTISEMENT packets as a master device (in ms)	10 to 40950 (Disable): Indicates that the operation is invalid. This functionality is disabled if VRRP operation mode is other than ietf-unified-spec-02-mode.
Preempt Mode : {ON OFF} [(Disable)]	Automatic switch-back setting	ON: Indicates that the automatic switch-back functionality is enabled. OFF: Indicates that the automatic switch-back functionality is suppressed. (Disable): Indicates that the operation is invalid. For a follower virtual router, this functionality is disabled. For a primary virtual router, this item is not displayed.
Preempt Delay : <second> [(Now Waiting, <N> sec left)] [(Disable)]	Suppression timer setting period (seconds)	(Now Waiting, <N>sec left): Displays the remaining time until the state is changed to master while switching to master is suppressed by this setting. N: Indicates a value from 1 to 65535. (Disable): Indicates that the operation is invalid. For a follower virtual router, this functionality is disabled. For a primary virtual router, this item is not displayed.
Non Preempt swap timer : <second> [(Now Waiting, <N>sec left)] [(Disable)]	Switch-back suppression time (in seconds) while automatic switch-back is suppressed	(Now Waiting, <N>sec left): Displays the remaining time until the state is changed to master while switching to master is suppressed by this setting. N: Indicates a value from 1 to 65535. (Disable): Indicates that the operation is invalid. For a follower virtual router, this functionality is disabled. For a primary virtual router, this item is not displayed.
Accept Mode : {ON OFF}	Accept mode	ON: Indicates accept mode. OFF: Indicates that accept mode is turned off. For an address owner, - is displayed regardless of the address mode setting.
Virtual Router Up Time : <time string>	Time when a virtual router is changed from the INITIAL status	This item is not displayed if the virtual router is in the INITIAL status.

Item	Meaning	Displayed information
track <track-number> {<interface name> [VRF <vrf id>]<interface type> <interface number>} Status : <status> {Down Priority Critical Priority} : <priority>	Information about a track assigned to a virtual router	<p><track-number>: Indicates the number of the track assigned to a virtual router.</p> <p><interface name>: Indicates the interface name of the VLAN interface that monitors for failures.</p> <p>VRF <vrf id>: Indicates the VRF ID. When the destination for VRRP polling is a global network, this item is not displayed. [OP-NPAR]</p> <p><interface type> <interface number>: Indicates an interface that monitors for failures. gigabitethernet <nif no.>/<port no.>: Indicates a 10BASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X interface that monitors failures. tengigabitethernet <nif no.>/<port no.>: Indicates a 10GBASE-R interface that monitors for failures. port-channel <channel group number>: Indicates a channel-group interface that monitors for failures.</p> <p><status>: Indicates the current status of an interface that monitors failures. (IF UP): Indicates that the interface is in the UP status. (IF DOWN): Indicates that the interface is in the DOWN status. (Disable): Indicates that the track assigned to a virtual router is disabled.</p> <p>Method for changing priority Down Priority : <priority>: Indicates the priority is decreased if an interface that monitors failures is in the DOWN status. Critical Priority : <priority>: Indicates the priority to be replaced when the interface that monitors failures is in the DOWN status.</p>
Target Address : <target-address> [(check reply interface)]	Destination address for VRRP polling	<p><target-address>: Indicates the target address for VRRP polling. This item is not displayed if the IP address for VRRP polling has not been specified, or for an interface that monitors failures.</p> <p>(check reply interface): This information is displayed if the track check-reply-interface configuration command has been used to configure this.</p>

Item	Meaning	Displayed information
Vrrp Polling Status : <status>[<reason>]	VRRP polling information	<p>This item is not displayed if the IP address for VRRP polling has not been specified, or for an interface that monitors failures.</p> <p><status>: Indicates connectivity by VRRP polling. reachable: Indicates that communication is possible. (Disable): Indicates that the operation is invalid. unreachable: Indicates that communication is impossible.</p> <p><reason>: Provides a detailed reason why communication is impossible. This information is displayed if <status> is unreachable. (interface down): Indicates that the source interface for polling is in the DOWN status. (no response): Indicates that there were no responses from the polling destination. (no route): Indicates that there are no routes to the polling destination. (invalid response): When the track check-reply-interface configuration command is set, responses from the interface that sent the polling request and also from another interface were received.</p>
IPv6 Advertisement Type : <type>[(Disable)]	Type of sending ADVERTISEMENT packets	<p>Type of sending ADVERTISEMENT packets ietf-ipv6-spec-02-mode: Sends ADVERTISEMENT packets according to draft-ietf-vrrp-ipv6-spec-02. ietf-ipv6-spec-07-mode: Sends ADVERTISEMENT packets according to draft-ietf-vrrp-ipv6-spec-07. ietf-unified-spec-02-mode: Sends ADVERTISEMENT packets according to draft-ietf-vrrp-unified-spec-02.</p> <p>(Disable): Indicates that the operation is invalid. For a follower virtual router, this functionality is disabled. For a primary virtual router, this item is not displayed.</p>

Example 4

Figure 12-15: Example of displaying virtual router statistics

```

> show vrrpstatus statistics interface vlan 10 vrid 3    Press the Enter key.
Date 2009/07/15 12:00:00 UTC
VLAN0010: VRID 3 VRF 2
  1 times transitions to master
 247 advertisement received
    0 with bad advertisement interval
    0 with authentication failed
    0 with bad ipv6 hoplimit
    0 with priority zero
    0 with invalid type
    0 with bad ipv6 address
    0 with bad authentication type
    0 with authentication type mismatch
    0 with packet length error
    0 with different VRRP version
    0 with low priority
1747 advertisement sent
    0 with priority zero
1 virtual MAC learning frame sent
0 change by command
0 change by interface down
0 change by receiving advertisement with high priority

```

```

0 change by Master_Down_Timer timeout
0 master transition delay count
track 10 VLAN0022 VRF 3 Target-Address : fe80::ba
  VRRP Polling round-trip min/avg/max = 0.266/0.274/0.286 ms
  1 priority down by detected
>

```

Display items in Example 4

Table 12-13: Items displayed for virtual router statistics

Item	Meaning	Displayed information
<interface name> : VRID <vrid> [VRF <vrf id>]	Name of the interface where a virtual router is operating, and its VRID information	<interface name>: Indicates the name of the interface where the virtual router is operating. <vrid>: Indicates the virtual router ID. VRF <vrf id>: Indicates the VRF ID. Not displayed if the virtual router is operating in a global network. [OP-NPAR]
<number of packets> times transitions to master	Number of transitions to the master status	--
<number of packets> advertisement received	Number of received ADVERTISEMENT packets	--
<number of packets> with bad advertisement interval	Number of received ADVERTISEMENT packets that have invalid packet-sending intervals	--
<number of packets> with authentication failed	Number of received ADVERTISEMENT packets of which authentication failed	--
<number of packets> with bad ipv6 hoplimit	Number of received ADVERTISEMENT packets whose HopLimit for the IPv6 header was not 255	--
<number of packets> with priority zero	Number of received ADVERTISEMENT packets whose priority level is 0	--
<number of packets> with invalid type	Number of received packets that had an invalid type field	--
<number of packets> with bad ipv6 address	Number of received ADVERTISEMENT packets that had invalid virtual router IPv6 addresses	--
<number of packets> with bad authentication type	Number of received ADVERTISEMENT packets with invalid packet authentication types	--
<number of packets> with authentication type mismatch	Number of received ADVERTISEMENT packets whose packet authentication type did not match the local setting.	--

Item	Meaning	Displayed information
<number of packets> with packet length error	Number of received ADVERTISEMENT packets whose packet length was invalid	--
<number of packets> with different VRRP version	Number of received packets whose version of ADVERTISEMENT packets and that of VRRP operation mode do not match	--
<number of packets> with low priority	Number of received ADVERTISEMENT packets with lower priority	--
<number of packets> advertisement sent	Number of sent ADVERTISEMENT packets	--
<number of packets> with priority zero	Number of sent ADVERTISEMENT packets whose priority is 0	--
<number of frames> virtual MAC learning frame sent	Number of sent MAC address learning frames	--
<N> change by command	Number of times that the <code>swap vrrp</code> command was executed	--
<N> change by interface down	Number of status transitions due to interface going down	--
<N> change by receiving advertisement with high priority	Number of status transitions caused by receipt of a high priority ADVERTISEMENT packet	--
<N> change by Master_Down_Timer timeout	Number of status transitions because the Master Down Timer timed out	--
<N> master transition delay count	Number of times that the suppression timer has been started	--

Item	Meaning	Displayed information
track <track-number> {<interface name> [VRF <vrf id>] <interface type> <interface number>} {Target-Address : <target-address> line-protocol}	VRRP polling information assigned to a virtual router	<p><track-number>: Indicates the number of the track assigned to a virtual router.</p> <p><interface name>: Indicates the name of an interface that monitors failures.</p> <p>VRF <vrf id>: Indicates the VRF ID. When the destination for VRRP polling is a global network, this item is not displayed. [OP-NPAR]</p> <p><interface type> <interface number>: Indicates an interface that monitors for failures. gigabitethernet <nif no.>/<port no.>: Indicates a 10BASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X interface that monitors failures. tengigabitethernet <nif no.>/<port no.>: Indicates a 10GBASE-R interface that monitors for failures. port-channel <channel group number>: Indicates a channel-group interface that monitors for failures.</p> <p>Target-Address : <target-address>: Indicates the target address for VRRP polling.</p> <p>line-protocol: Applied to an interface that monitors failures.</p>
VRRP Polling round-trip min/avg/max =<minimum>/<average>/<maximum> ms	Packet response time for VRRP polling	<p>This item is not displayed if the IP address for VRRP polling has not been specified, or for an interface that monitors failures.</p> <p><minimum>/<average>/<maximum>: Indicates the minimum value, average value, and maximum value.</p>
<N> priority down by detected	Number of times that the priority has been decreased due to a track error	--

Example 5

Figure 12-16: Example of displaying virtual router group information (for primary virtual routers)

```
> show vrrpstatus group name VRRPNAME1    Press the Enter key.
Date 2009/07/15 12:00:00 UTC
VLAN0010: VRID 1 VRF 2
  Virtual Router Name           : VRRPNAME1 (primary)
  Virtual Router Follow         : -
  Number of Follow virtual routers : 4
  Followed by virtual routers   :
    VLAN0020: VRID 1 VRF 2
    VLAN0030: VRID 1 VRF 2
    VLAN0040: VRID 1 VRF 2
    VLAN0050: VRID 1 VRF 2
```

Figure 12-17: Example of displaying virtual router group information (for follower virtual routers)

```
> show vrrpstatus group interface vlan 10 vrid 1    Press the Enter key.
Date 2009/07/15 12:00:00 UTC
```

```

VLAN0020: VRID 1 VRF 2
  Virtual Router Name      : VRRPNAME2 (follow)
  Virtual Router Follow    : VRRPNAME1 (VLAN0010: VRID 1 VRF 2 )
  Number of Follow virtual routers: 0
  Followed by virtual routers : -

```

Display items in Example 5

Table 12-14: Items displayed for virtual router group information

Item	Meaning	Displayed information
<i><interface name></i> : VRID <i><vrid></i> [VRF <i><vrf id></i>]	Name of the interface where a virtual router is operating, and its VRID information	<i><interface name></i> : Indicates the name of the interface where the virtual router is operating. <i><vrid></i> : Indicates the virtual router ID. VRF <i><vrf id></i> : Indicates the VRF ID. Not displayed if the virtual router is operating in a global network. [OP-NPAR]
Virtual Router Name : <i><virtual router name></i> ({primary follow})	Virtual router name	{primary follow}: Indicates the type of the virtual router.
Virtual Router Follow : <i><virtual router name></i> ({ <i><interface name></i> : VRID <i><vrid></i> [VRF <i><vrf id></i>]not running})	Name of a followed primary virtual router	<i><virtual router name></i> : - is displayed for a primary virtual router. For a follower virtual router, the name of the followed primary virtual router is displayed. <i><interface name></i> : Indicates the name of the interface where a primary virtual router is operating. <i><vrid></i> : Indicates the virtual router ID of the primary virtual router. VRF <i><vrf id></i> : Indicates the VRF ID of the primary virtual router. This item is not displayed if the primary virtual router is operating in a global network. [OP-NPAR] not running: A primary virtual router with the specified name was not found.
Number of Follow virtual routers : <i><N></i>	Number of follower virtual routers	--
Followed by virtual routers: <i><interface name></i> : VRID <i><vrid></i> [VRF <i><vrf id></i>]	List of follower virtual routers	- is displayed for a follower virtual router. <i><interface name></i> : Indicates the name of an interface where a follower virtual router is operating. <i><vrid></i> : Indicates the virtual router ID. VRF <i><vrf id></i> : Indicates the VRF ID. Not displayed if the follower virtual router is operating in a global network. [OP-NPAR]

Impact on communication

None

Response messages

Table 12-15: List of response messages for the show vrrpstatus(IPv6) command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
no entries.	There are no applicable virtual routers.
Vrrp-vlan disable because virtual router is not configured.	The VRRP-management VLAN is disabled because no virtual routers are configured.
Vrrp-vlan not configured.	The VRRP-management VLAN has not been configured.

Notes

None

clear vrrpstatus (IPv6)

Clears the counter for VRRP virtual router statistics and the counter for VRRP-management VLAN statistics.

Syntax

```
clear vrrpstatus [ { vrrp-vlan | [protocol ipv6] [{ name <virtual router name> |
interface vlan <vlan id> [vrid <vrid>] }] } ]
```

Input mode

User mode and administrator mode

Parameters

vrrp-vlan

Clears statistics for VRRP-management VLANs.

[protocol ipv6] [{ name <virtual router name> | interface vlan <vlan id> [vrid <vrid>] }]

protocol ipv6

Clears the counter for IPv6-protocol virtual router statistics.

Operation when this parameter is omitted:

Clears the statistics for both IPv4 and IPv6-protocol virtual routers.

name <virtual router name>

Specifies a virtual router name.

Operation when this parameter is omitted:

Clears all virtual router information.

interface vlan <vlan id>

Specifies the interface that is used to configure the virtual router.

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

vrid <vrid>

Specifies the router ID.

Operation when this parameter is omitted:

Clears all virtual router information configured via the VLAN.

Operation when all parameters are omitted:

Clears the counter for all virtual router statistics.

Example

Figure 12-18: Example of clearing the counter for virtual router statistics

```
> clear vrrpstatus interface vlan 10 vrid 3    Press the Enter key.
>
```

Figure 12-19: Example of clearing the counter for VRRP-management VLAN statistics

```
> clear vrrpstatus vrrp-vlan    Press the Enter key.
>
```

Display items

None

Impact on communication

None

Response messages*Table 12-16:* List of response messages for the clear vrrpstatus(IPv6) command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
no entries.	There are no applicable virtual routers.
Vrrp-vlan disable because virtual router is not configured.	The VRRP-management VLAN is disabled because no virtual routers are configured.
Vrrp-vlan not configured.	The VRRP-management VLAN has not been configured.

Notes

None

swap vrrp (IPv6)

Changes the device status when switch-back is suppressed.

If the device is in the master status, it is changed to the backup status.

If the device is in the backup status, it is changed to the master status.

Syntax

```
swap vrrp [-f] { name <virtual router name> | interface vlan <vlan id> [vrid <vrid>]
}
```

Input mode

User mode and administrator mode

Parameters

-f

Executes the command without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

name <virtual router name>

Specifies a virtual router name.

interface vlan <vlan id>

Specifies the interface that is used to configure the virtual router.

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

vrid <vrid>

Specifies the router ID.

Operation when this parameter is omitted:

Displays confirmation messages for the virtual routers configured via the specified VLAN.

Example

The following figure shows how to switch VRID 3 and VRID 40 virtual routers configured for VLAN 10, which are currently operating in the master status, to the backup status.

Figure 12-20: Example of performing switch-back for virtual routers

```
> swap vrrp interface vlan 10
Exchange VRRP 3 OK? (y/n): y
Exchange VRRP 40 OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Response messages

Table 12-17: List of response messages for the swap vrrp(IPv6) command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Command execution cannot be performed to follow virtual router.	This command cannot be executed for follower virtual routers.
Command execution cannot be performed to owner's virtual router of an initial state.	This command cannot be executed for virtual routers in the initial status.
Command execution cannot be performed to owner's virtual router.	This command cannot be executed for the virtual router of the address owner.
no entries.	There are no applicable virtual routers.

Notes

- If this command is executed from a virtual router that has lower or equal priority (including the default priority), the device status might not be changed to the master status.
- This command cannot be entered for an address owner's virtual router, a follower virtual router, or a device in the initial state.
- If a switch-back command is executed while switch-back is suppressed, the command is given priority and switch-back is performed.
- If the command is executed when switch-back is not suppressed, switch-back is performed, even though that does not seem to be the case because the status of the virtual router with the higher priority is changed to the master status by the automatic switch-back functionality.
- When the command is executed, both virtual routers are swapped to the backup or master status temporarily, but they are changed back to the master or backup status automatically.
- When switch-back cannot be performed due to a failure of other devices, if the command is executed, communication is suspended for 4 seconds by default.
- In a configuration where the `no vrrp preempt` and the `vrrp timers non-preempt-swap` configuration commands are set for all devices that make up the VRRP, if a switch-back command is executed in the master device, all devices change to the backup status until the period set for the `vrrp timers non-preempt-swap` command elapses. To avoid this situation, do not set the `vrrp timers non-preempt-swap` command for at least one of the devices that makes up the VRRP. If all the devices are in the backup status, you can make one of the devices the master device by executing the `swap vrrp` command and specifying the device.

The table below lists the results of executing this command. No status change in the following table indicates situation where it does not seem that switch-back is performed.

Table 12-18: Result of executing the swap vrrp(IPv6) command

--			Local device is being suppressed		Local device is not suppressed	
			Another device is being suppressed	Another device is not being suppressed	Another device is being suppressed	Another device is not being suppressed
Local device (Master)	Comparison of the priority for the local device and another device	High	Switched	Switched	No status change	No status change
		Equal	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.
		Low	Switch-back	Switch-back	Switch-back	Switch-back
Local device (Backup)		High	Switch-back	Switch-back	Switch-back	Switch-back
		Equal	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.	The status of the device with the greater IP address is changed to the master status.
		Low	No status change	No status change	No status change	No status change

Terms used in the above table:

- Local device: A device in which the `swap vrrp` command is executed.
- Another device: A device other than the local device.
- Switched: The priority of the master local device is changed from high to low.

show track (IPv4)

Displays VRRP track information.

Syntax

```
show track <track number> [detail]
show track [detail]
    { [protocol ip] [interface vlan <vlan id>]
      | [interface <interface type> <interface number>] }
```

Input mode

User mode and administrator mode

Parameters

<track number>

Specify the track number.

detail

Displays detailed statistics.

Operation when this parameter is omitted:

Displays a track overview.

{[protocol ip] [interface vlan <vlan id>] | [interface <interface type> <interface number>]}

protocol ip

Displays track information set for the IPv4 protocol IP interface.

interface vlan <vlan id>

Specifies a VLAN interface for which a track is configured.

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

interface <interface type> <interface number>

Specifies the interface that monitors failures.

For <interface type> <interface number>, the following values can be set:

- gigabitethernet <nif no.>/<port no.>
- tengigabitethernet <nif no.>/<port no.>

For the specifiable range of <nif no.>/<port no.> values, see *Specifiable values for parameters*.

- port-channel <channel group number>

For the specifiable range of <channel group number> values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Displays all track information.

Operation when all parameters are omitted:

Displays the list of tracks and track information.

Example

- The following figure shows an example of displaying the list of IPv4 protocol tracks.

Figure 12-21: Example of displaying IPv4 protocol track information

```
> show track protocol ip      Press the Enter key.
Date 2009/07/15 12:00:00 UTC
track : 10  interface : VLAN0022  Mode : (interface)
track : 20  interface : VLAN0031 VRF 10 Mode : (polling)
>
```

- The following figure shows an example of displaying detailed track information.

Figure 12-22: Example of displaying detailed track information

```
> show track detail interface vlan 31      Press the Enter key.
Date 2009/07/15 12:00:00 UTC
track : 20  interface : VLAN0031 VRF 10 Mode : (polling)
      Target Address : 170.10.10.10
      Assigned to :
        VLAN0010: VRID 1
        VLAN0100: VRID 100 VRF 20
>
```

Display items

Table 12-19: Items displayed for the show track(IPv4) command

Item	Meaning	Displayed information
track : <track-number> interface : {<interface name> [VRF <vrf id>] <interface type> <interface number>} Mode : <mode>	Summary information about track settings	<p><track-number>: Indicates the number of the track assigned to a virtual router.</p> <p>interface : { <interface name> [VRF <vrf id>] <interface type> <interface number>}: Indicates information about an interface that monitors failures. (not assigned) is displayed if the track interface configuration command is not set.</p> <p><interface name>: Indicates the interface name of the VLAN interface that monitors for failures.</p> <p>VRF <vrf id>: Indicates the VRF ID. This item is not displayed if the VLAN interface that monitors failures is a global network. [OP-NPAR]</p> <p><interface type> <interface number>: Indicates an interface that monitors for failures. gigabitethernet <nif no.>/<port no.>: Indicates a 10BASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X interface that monitors failures. tengigabitethernet <nif no.>/<port no.>: Indicates a 10GBASE-R interface that monitors for failures. port-channel<channel group number>: Indicates a channel-group interface that monitors for failures.</p> <p>Mode : <mode>: Indicates the monitoring mode of the track. This item is not displayed if the track interface configuration command is not set. (interface): Monitors the interface status. (polling): Monitors the polling status.</p>
Target Address : <target_address>	Destination IP address for VRRP polling	This item is not displayed if it has not been set.
check_status_interval : <seconds>	Interval (in seconds) between VRRP polling attempts	This item is not displayed if it has not been set. Initial value: 6
check_trial_times : <count>	Number of attempts until the status is changed by VRRP polling	This item is not displayed if it has not been set. Initial value: 4
failure_detection_interval : <seconds>	Interval (in seconds) between VRRP polling attempts when a failure is detected	This item is not displayed if it has not been set. Initial value: 2
failure_detection_times : <count>	Number of attempts until the status is changed when VRRP polling detects a failure	This item is not displayed if it has not been set. Initial value: 3

Item	Meaning	Displayed information
recovery_detection_interval : <seconds>	Interval (in seconds) between attempts when VRRP polling detects restoration	This item is not displayed if it has not been set. Initial value: 2
recovery_detection_times : <count>	Number of attempts until the status is changed when VRRP polling detects restoration	This item is not displayed if it has not been set. Initial value: 3
check_reply_interface : on	Whether to check if the interface sent by VRRP polling and the interface that received the response match	This item is not displayed if it has not been set.
Assigned to : <interface name>: VRID <vrid> [VRF <vrf id>]	List of virtual routers to which a track is assigned	This item is not displayed if no tracks are assigned to a virtual router. <interface name>: Indicates the name of an interface for which a virtual router, to which a track is assigned, is configured. <vrid>: Indicates the virtual router ID of a virtual router to which a track is assigned. VRF <vrf id>: Indicates the VRF ID. Not displayed if the virtual router is operating in a global network. [OP-NPAR]

Impact on communication

None

Response messages

Table 12-20: List of response messages for the show track(IPv4) command

Message	Description
no entries.	There are no applicable tracks.

Notes

None

show track (IPv6)

Displays VRRP track information.

Syntax

```
show track <track number> [detail]
show track [detail]
    { [protocol ipv6] [interface vlan <vlan id>]
      | [interface <interface type> <interface number>] }
```

Input mode

User mode and administrator mode

Parameters

<track number>

Specify the track number.

detail

Displays detailed statistics.

Operation when this parameter is omitted:

Displays a track overview.

{[protocol ipv6][interface vlan <vlan id>] [interface <interface type> <interface number>]}

protocol ipv6

Displays track information set for the IPv6-protocol IP interface.

interface vlan <vlan id>

Specifies a VLAN interface for which a track is configured.

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

interface <interface type> <interface number>

Specifies the interface that monitors failures.

For <interface type> <interface number>, the following values can be set:

- gigabitethernet <nif no.>/<port no.>
- tengigabitethernet <nif no.>/<port no.>

For the specifiable range of <nif no.>/<port no.> values, see *Specifiable values for parameters*.

- port-channel <channel group number>

For the specifiable range of <channel group number> values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Displays all track information.

Operation when all parameters are omitted:

Displays the list of tracks and track information.

Example

- The following figure shows an example of displaying the list of IPv6 protocol tracks.

Figure 12-23: Example of displaying IPv6 protocol track information

```
> show track protocol ipv6      Press the Enter key.
Date 2009/07/15 12:00:00 UTC
track : 10  interface : VLAN0022  Mode : (interface)
track : 30  interface : VLAN0032 VRF 10 Mode : (polling)
>
```

- The following figure shows an example of displaying detailed track information.

Figure 12-24: Example of displaying detailed track information

```
> show track detail interface vlan 32      Press the Enter key.
Date 2009/07/15 12:00:00 UTC
track : 30  interface : VLAN0032 VRF 10 Mode : (polling)
      Target Address : 100::6789
      Assigned to :
        VLAN0010: VRID 3
        VLAN0100: VRID 200 VRF 20
>
```

Display items

Table 12-21: Items displayed for the show track(IPv6) command

Item	Meaning	Displayed information
track : <track-number> interface : {<interface name> [VRF <vrf id>]<interface type> <interface number>}Mode : <mode>	Summary information about track settings	<p><track-number>: Indicates the number of the track assigned to a virtual router.</p> <p>interface : {<interface name> [VRF <vrf id>]<interface type> <interface number>}: Indicates information about an interface that monitors failures. (not assigned) is displayed if the track interface configuration command is not set.</p> <p><interface name>: Indicates the interface name of the VLAN interface that monitors for failures.</p> <p>VRF <vrf id>: Indicates the VRF ID. This item is not displayed if the VLAN interface that monitors failures is a global network. [OP-NPAR]</p> <p><interface type> <interface number>: Indicates an interface that monitors for failures.</p> <p>gigabitethernet <nif no.>/<port no.>: Indicates a 10BASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X interface that monitors failures.</p> <p>tengigabitethernet <nif no.>/<port no.>: Indicates a 10GBASE-R interface that monitors for failures.</p> <p>port-channel<channel group number>: Indicates a channel-group interface that monitors for failures.</p> <p>Mode : <mode>: Indicates the monitoring mode of the track.</p> <p>This item is not displayed if the track interface configuration command is not set.</p> <p>(interface): Monitors the interface status.</p> <p>(polling): Monitors the polling status.</p>

Item	Meaning	Displayed information
Target Address : <target_address>	Destination IP address for VRRP polling	This item is not displayed if it has not been set.
check_status_interval : <seconds>	Interval (in seconds) between VRRP polling attempts	This item is not displayed if it has not been set. Initial value: 6
check_trial_times : <count>	Number of attempts until the status is changed by VRRP polling	This item is not displayed if it has not been set. Initial value: 4
failure_detection_interval : <seconds>	Interval (in seconds) between VRRP polling attempts when a failure is detected	This item is not displayed if it has not been set. Initial value: 2
failure_detection_times : <count>	Number of attempts until the status is changed when VRRP polling detects a failure	This item is not displayed if it has not been set. Initial value: 3
recovery_detection_interval : <seconds>	Interval (in seconds) between attempts when VRRP polling detects restoration	This item is not displayed if it has not been set. Initial value: 2
recovery_detection_times : <count>	Number of attempts until the status is changed when VRRP polling detects restoration	This item is not displayed if it has not been set. Initial value: 3
check_reply_interface : on	Whether to check if the interface sent by VRRP polling and the interface that received the response match	This item is not displayed if it has not been set.
Assigned to : <interface name>: VRID <vrid> [VRF <vrf id>]	List of virtual routers to which a track is assigned	This item is not displayed if no tracks are assigned to a virtual router. <interface name>: Indicates the name of an interface for which a virtual router, to which a track is assigned, is configured. <vrid>: Indicates the virtual router ID of a virtual router to which a track is assigned. VRF <vrf id>: Indicates the VRF ID. Not displayed if the virtual router is operating in a global network. [OP-NPAR]

Impact on communication

None

Response messages

Table 12-22: List of response messages for the show track(IPv6) command

Message	Description
no entries.	There are no applicable tracks.

Notes

None

Chapter

13. IEEE 802.3ah/UDLD

```
show efmoam
show efmoam statistics
clear efmoam statistics
restart efmoam
dump protocols efmoam
```

show efmoam

Displays the IEEE 802.3ah/OAM configuration information and the status of ports.

Syntax

```
show efmoam [port <port list>] [detail]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Displays the IEEE 802.3ah/OAM configuration information for the specified port.

For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

The IEEE 802.3ah/OAM configuration information for all ports is displayed.

detail

Displays configuration information for all ports that send and receive OAMPDU frames.

Note, however, that this parameter is not displayed if a port in passive mode does not recognize the partner device.

Operation when this parameter is omitted:

No information about ports in passive mode is displayed.

Operation when all parameters are omitted:

The IEEE 802.3ah/OAM configuration information for all ports that are not in passive mode is displayed.

Example 1

The following figure is an example of displaying brief information related to the IEEE 802.3ah/OAM configuration.

Figure 13-1: Example of displaying IEEE 802.3ah/OAM brief information

```
> show efmoam
Date 2006/10/02 23:59:59 UTC
Status: Enabled
udld-detection-count: 30
Port   Link status   UDLD status   Dest MAC
1/1    Up              detection     * 0012.e298.dc20
1/2    Down           active        unknown
1/4    Down (uni-link) detection     unknown
>
```

Display items in Example 1

Table 13-1: Items displayed for IEEE 802.3ah/OAM brief information

Item	Meaning	Displayed information
Status	Status of the IEEE 802.3ah/OAM functionality of the Switch	Enabled: Indicates that the IEEE 802.3ah/OAM functionality is enabled. Disabled: Indicates that the IEEE 802.3ah/OAM functionality is disabled.

Item	Meaning	Displayed information
udld-detection-count	Number of response timeouts for detecting failures	3 to 300 (times)
Port	Port information	--
<nif no.> / <port no.>	Port number	The NIF number and the port number of the port whose information is to be displayed
Link status	Link status of the applicable port	Up: Indicates that the port status is Up. Down: Indicates that the port status is Down. Down (uni-link): Indicates that the port status is Down (unidirectional link failure detection). Down (loop): Indicates that the port status is Down (loop detection).
UDLD status	UDLD operating status by the IEEE 802.3ah/UDLD functionality for each port	detection: Indicates that failure detection is performed. active: Indicates that OAMPDU frames are being sent and responses are received.
Dest MAC	MAC address of the port on the partner device	unknown is displayed if no information has been received from the partner device. If a bidirectional link is confirmed, * is displayed on the left of the MAC address.

Example 2

The following figure is an example of displaying detailed information related to the IEEE 802.3ah/OAM configuration by specifying the `detail` parameter.

Figure 13-2: Example of displaying detailed IEEE 802.3ah/OAM information

```
> show efmoam detail
Date 2006/10/02 23:59:59 UTC
Status: Enabled
udld-detection-count: 30
Port   Link status   UDLD status   Dest MAC
1/1    Up             detection     * 0012.e298.dc20
1/2    Down          active        unknown
1/3    Up            passive       0012.e298.7478
1/4    Down (uni-link) detection     unknown
>
```

Display items in Example 2

Table 13-2: Items displayed for detailed IEEE 802.3ah/OAM information

Item	Meaning	Displayed information
Status	Status of the IEEE 802.3ah/OAM functionality of the Switch	Enabled: Indicates that the IEEE 802.3ah/OAM functionality is enabled. Disabled: Indicates that the IEEE 802.3ah/OAM functionality is disabled.
udld-detection-count	Number of response timeouts for detecting failures	3 to 300 (times)
Port	Port information	--
<nif no.> / <port no.>	Port number	The NIF number and the port number of the port whose information is to be displayed

Item	Meaning	Displayed information
Link status	Link status of the applicable port	Up: Indicates that the port status is Up. Down: Indicates that the port status is Down. Down (uni-link) : Indicates that the port status is Down (unidirectional link failure detection). Down (loop) : Indicates that the port status is Down (loop detection).
UDLD status	UDLD operating status by the IEEE 802.3ah/UDLD functionality for each port	detection: Indicates that failure detection is performed. active: Indicates that OAMPDU frames are being sent and responses are received. passive: Only OAMPDU frames are responded to.
Dest MAC	MAC address of the partner device	unknown is displayed if no information has been received from the partner device. Note, however, that no unknown ports are displayed in passive mode. If a bidirectional link is confirmed in active mode, * is displayed on the left of the MAC address.

Impact on communication

None

Response messages

Table 13-3: List of response messages for the show efmoam command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to IEEE802.3ah/OAM program.	Communication with the IEEE 802.3ah/OAM program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart efmoam</code> command to restart the IEEE 802.3ah/OAM program.
IEEE802.3ah/OAM doesn't seem to be running.	This command failed because the IEEE 802.3ah/OAM program is being restarted. Re-execute the command.

Notes

If a system switchover of BCUs, CSUs, or MSUs occurred, Down is displayed as the item displayed for Link Status, but detailed information, such as (uni-link) or (loop), is not displayed.

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 figure is an example of displaying statistics for all configured IEEE 802.3ah/OAM.

Figure 13-3: Example of displaying statistics for IEEE 802.3ah/OAM

```
>show efmoam statistics
Date 2006/10/02 23:59:59 UTC
Port 1/1 [detection]
  OAMPDUs   :Tx      =      295  Rx      =      295
              Invalid =        0  Unrecogn.=        0
  TLVs      :Invalid =        0  Unrecogn.=        0
  Info TLV  :Tx_Local =      190  Tx_Remote=      105  Rx_Remote=      187
              Timeout =         3  Invalid  =         0  Unstable =         0
  Inactivate:TLV    =         0  Timeout  =         0
Port 1/2 [active]
  OAMPDUs   :Tx      =      100  Rx      =      100
              Invalid =         0  Unrecogn.=         0
  TLVs      :Invalid =         0  Unrecogn.=         0
  Info TLV  :Tx_Local =      100  Tx_Remote=      100  Rx_Remote=      100
              Timeout =         0  Invalid  =         0  Unstable =         0
  Inactivate:TLV    =         0  Timeout  =         0
Port 1/3 [passive]
  OAMPDUs   :Tx      =      100  Rx      =      100
              Invalid =         0  Unrecogn.=         0
  TLVs      :Invalid =         0  Unrecogn.=         0
  Info TLV  :Tx_Local =         0  Tx_Remote=      100  Rx_Remote=      100
              Timeout =         0  Invalid  =         0  Unstable =         0
  Inactivate:TLV    =         0  Timeout  =         0
>
```

Display items

Table 13-4: Items displayed for IEEE 802.3ah/OAM statistics

Item	Meaning	Displayed information
Port	Port information	--
<nif no.>/<port no.>	Port number	The NIF number and the port number of the port whose information is to be displayed

Item	Meaning	Displayed information
UDLD status	UDLD operating status by the IEEE 802.3ah/UDLD functionality for each port	detection: Indicates that a failure is detected. active: Indicates that Information OAMPDU frames are sent and responded to. passive: Only OAMPDU frames are responded to.
OAMPDUs	Statistics for frames	--
Tx	Number of OAMPDUs that have been sent for each port	0 to 4294967295
Rx	Number of OAMPDUs that have been received for each port	0 to 4294967295
Invalid	Number of OAMPDUs that have been received but were discarded because they were invalid	0 to 4294967295
Unrecogn.	Number of unsupported OAMPDUs that have been received	0 to 4294967295
TLVs	TLV statistics	--
Invalid	Number of TLVs that were determined as having format errors and discarded	0 to 4294967295
Unrecogn.	Number of TLVs that conform to regulations but cannot be recognized by the current version	0 to 4294967295
Info TLV	TLV statistics for Information OAMPDU frames	--
Tx_Local	Number of times that Local Information TLV was sent	0 to 4294967295
Tx_Remote	Number of times that Local Information TLV from the partner device was received and Remote Information TLV was edited and then sent	0 to 4294967295
Rx_Remote	Number of received Local Information TLVs for responses from the partner device	0 to 4294967295
Timeout	Number of times that response timeout occurred on a port	0 to 4294967295
Invalid	Number of TLVs that were determined as having format errors and discarded	0 to 4294967295
Unstable	Number of times that control frames were received from a different device on a currently connected port	0 to 4294967295 If this number is updated, multiple devices might be connected via a hub.
Inactivate	Statistics for failure detections	--
TLV	Number of times that failures showing the received TLV contents were detected	0 to 4294967295
Timeout	Number of times that failures were detected through consecutive response timeouts	0 to 4294967295

Impact on communication

None

Response messages*Table 13-5:* List of response messages for the show efmoam statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to IEEE802.3ah/OAM program.	Communication with the IEEE 802.3ah/OAM program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart efmoam</code> command to restart the IEEE 802.3ah/OAM program.
IEEE802.3ah/OAM doesn't seem to be running.	This command failed because the IEEE 802.3ah/OAM program is being restarted. Re-execute the command.
There is no statistics to show.	There are no statistics to be displayed.

Notes

Ports on which no OAMPDUs have been sent or received in passive mode are not displayed.

clear efmoam statistics

Clears the IEEE 802.3ah/OAM statistics.

Syntax

```
clear efmoam statistics [port <port list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Clears the IEEE 802.3ah/OAM statistics for the specified port.

For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Clears all IEEE 802.3ah/OAM statistics for the Switch.

Example

The following figure is an example of clearing the IEEE 802.3ah/OAM statistics.

Figure 13-4: Example of clearing IEEE 802.3ah/OAM statistics

```
> clear efmoam statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 13-6: List of response messages for the clear efmoam statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to IEEE802.3ah/OAM program.	Communication with the IEEE 802.3ah/OAM program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart efmoam</code> command to restart the IEEE 802.3ah/OAM program.
IEEE802.3ah/OAM doesn't seem to be running.	This command failed because the IEEE 802.3ah/OAM program is being restarted. Re-execute the command.

Notes

None

restart efmoam

Restarts IEEE 802.3ah/OAM.

Syntax

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

Input mode

User mode and administrator mode

Parameters

-f

Restarts IEEE 802.3ah/OAM without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file when the program is restarted.

Operation when this parameter is omitted:

A core file is not output.

Operation when all parameters are omitted:

Restarts IEEE 802.3ah/OAM after displaying a confirmation message.

Example

Figure 13-5: Example of restarting the IEEE 802.3ah/OAM program

```
> restart efmoam
IEEE802.3ah/OAM program restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Response messages

Table 13-7: List of response messages for the restart efmoam command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
IEEE802.3ah/OAM doesn't seem to be running.	This command failed because the IEEE 802.3ah/OAM program is being restarted. Re-execute the command.

Notes

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

Storage directory: /usr/var/core/

Core file: efmoamd.core

If a file with this name already exists, the file is overwritten unconditionally. Therefore, backup the

file in advance, if necessary.

dump protocols efmoam

Outputs to a file detailed event trace information and control table information collected for IEEE 802.3ah/OAM.

Syntax

```
dump protocols efmoam
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 13-6: Example of performing a dump for IEEE 802.3ah/OAM

```
> dump protocols efmoam
>
```

Display items

None

Impact on communication

None

Response messages

Table 13-8: List of response messages for the dump protocols efmoam command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to IEEE802.3ah/OAM program.	Communication with the IEEE 802.3ah/OAM program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart efmoam</code> command to restart IEEE 802.3ah/OAM.
File open error.	An attempt to open or access a dump file failed. Re-execute the command later.
IEEE802.3ah/OAM doesn't seem to be running.	This command failed because the IEEE 802.3ah/OAM program is being restarted. Re-execute the command.

Notes

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

Storage directory: `/usr/var/efmoam/`

File: `efmoamd_dump.gz`

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

Chapter

14. L2 Loop Detection

show loop-detection
show loop-detection statistics
show loop-detection logging
clear loop-detection statistics
clear loop-detection logging
restart loop-detection
dump protocols loop-detection

show loop-detection

Displays the L2 loop detection information.

Syntax

```
show loop-detection [port <port list>] [channel-group-number <channel group list>]
```

Input mode

User mode and administrator mode

Parameters

```
[port <port list>] [channel-group-number <channel group list>]
```

Displays L2 loop detection information for the specified ports and channel groups. Ports and channel groups can be specified at the same time. In this case, L2 loop detection information about either the specified ports or the specified channel groups is displayed.

port <port list>

Displays L2 loop detection information for the specified port numbers. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Displays L2 loop detection information for the specified channel group link aggregation (in a list). For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Displays all L2 loop detection information, not limiting it to specific ports or specific channel groups.

Example

The following figure shows an example of displaying L2 loop detection information.

Figure 14-1: Example of displaying L2 loop detection information

```
> show loop-detection
Date 2008/04/21 12:10:10 UTC
Loop Detection ID      :64
Interval Time          :10
Output Rate            :30pps
Threshold              :1000
Hold Time              :300
Auto Restore Time      :3600
VLAN Port Counts
  Configuration        :103          Capacity      :300
Port Information
  Port  Status  Type      DetectCnt  RestoringTimer  SourcePort  Vlan
  1/1   Up      send-inact  100       -               1/3         4090
  1/2   Down    send-inact   0         -               -           -
  1/3   Up      send       100       -               1/1         4090
  1/4   Up      exception   0         -               -           -
  1/5   Down(loop) send-inact 1000      1510        CH:32 (U)    100
  CH:1  Up      trap        0         -               -           -
  CH:32 Up      uplink      -         -               1/5         100
>
```

Display items

Table 14-1: Items displayed for L2 loop detection information

Item	Meaning	Displayed information
Loop Detection ID	ID of the L2 loop detection functionality	--
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 until the port changes to inactive status	The number of times that L2 loop detection frames for inactivating a port were received is displayed.
Hold Time	Retention time for the number of detections (in seconds)	The period of time to retain the number of times that L2 loop detection frames for inactivating a port were received is displayed. When the number is to be retained indefinitely, infinity is displayed.
Auto Restore Time	Automatic restoration time (in seconds)	Period of time before an inactive port is automatically switched to an active port. - is displayed if the port is not automatically restored.
Configuration	Number of ports set to send L2 loop detection frames	The number of VLAN ports [#] that are set to send L2 loop detection frames is displayed. If this value is greater than the value displayed for the number of ports allowed to send L2 loop detection frames, the excess L2 loop detection frames cannot be sent.
Capacity	Number of ports allowed to send L2 loop detection frames	The number of VLAN ports [#] where L2 loop detection frames can be sent at the defined transmission rate is displayed.
Port	Port number or channel group number	<nif no.>/<port no.>: Indicates the port number. CH: <channel group number>: Indicates the channel group number.
Status	Port state	Up: Indicates that the port status is Up. Down: Indicates that the port status is Down. Down(loop): Indicates that the port status is Down due to the L2 loop detection 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	Current number of detections	The number of times that L2 loop detection frames were received within the retention time for the number of detections is displayed. For an uplink port, - is displayed. The number of receptions on the uplink port is counted on the sending port. The number of receptions is updated until it reaches 10000.
RestoringTimer	Time remaining until automatic restoration (in seconds)	The time before the port is activated automatically is displayed. - is displayed if the port is not automatically restored.

Item	Meaning	Displayed information
SourcePort	Port for sending L2 loop detection frames	The sending port used when an L2 loop detection frame was last received. <nif no.> / <port no.>: Indicates the port number. CH: <channel group number>: Indicates the channel group number. For the receive uplink port, (U) is displayed. - is displayed if no L2 loop detection frames have been received.
Vlan	Source VLAN ID of the L2 loop detection frame	Displays the source VLAN ID when an L2 loop detection frame was last received.

#: Total number of VLANs set for the applicable physical ports or channel groups.

Impact on communication

None

Response messages

Table 14-2: List of response messages for the show loop-detection command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Loop Detection program.	Communication with the L2 loop detection program failed. Re-execute the command.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the functionality has not been enabled. Check the configuration.
No corresponding port information.	No port and channel group information for L2 loop detection was found.

Notes

None

show loop-detection statistics

Displays the L2 loop detection statistics.

Syntax

```
show loop-detection statistics [port <port list>] [channel-group-number <channel
group list>]
```

Input mode

User mode and administrator mode

Parameters

[port <port list>] [channel-group-number <channel group list>]

Displays L2 loop detection statistics for the specified ports and channel groups. Ports and channel groups can be specified at the same time. In this case, L2 loop detection statistics related to either the specified ports or the specified channel groups are displayed.

port <port list>

Displays L2 loop detection statistics for the specified port number. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Displays L2 loop detection statistics for the channel groups specified in list format in the specified link aggregation. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Displays all L2 loop detection statistics, not limiting them to specific ports or specific channel groups.

Example

The following figure is an example of displaying L2 loop detection statistics.

Figure 14-2: Example of displaying L2 loop detection statistics

```
> show loop-detection statistics
Date 2008/04/21 12:10:10 UTC
Port:1/1  Up                Type :send-inact
  TxFrame      :                10000000  RxFrame      :                1200
  Inactive Count:                3         RxDiscard    :                30
  Last Inactive : 2008/04/10 19:20:20      Last RxFrame : 2008/04/21 12:02:10
Port:1/2  Down              Type :send-inact
  TxFrame      :                0         RxFrame      :                0
  Inactive Count:                0         RxDiscard    :                0
  Last Inactive :                -         Last RxFrame :                -
Port:1/3  Up                Type :send
  TxFrame      :                10000000  RxFrame      :                600
  Inactive Count:                0         RxDiscard    :                0
  Last Inactive :                -         Last RxFrame : 2008/04/10 19:20:20
Port:1/4  Up                Type :exception
  TxFrame      :                0         RxFrame      :                0
  Inactive Count:                0         RxDiscard    :                0
  Last Inactive :                -         Last RxFrame :                -
Port:1/5  Down(loop)        Type :send-inact
  TxFrame      :                12000      RxFrame      :                1
  Inactive Count:                1         RxDiscard    :                0
  Last Inactive : 2008/04/21 09:30:50      Last RxFrame : 2008/04/21 09:30:50
CH:1      Up                Type :trap
```

14. L2 Loop Detection

```

TxFrame      : 0 RxFrame      : 0
Inactive Count: 0 RxDiscard   : 0
Last Inactive : - Last RxFrame : -
CH:32 Up      Type :uplink
TxFrame      : 0 RxFrame      : 100
Inactive Count: 0 RxDiscard   : 0
Last Inactive : - Last RxFrame : 2008/04/21 09:30:50
>

```

Display items

Table 14-3: Items displayed for L2 loop detection statistics

Item	Meaning	Displayed information
Port	Port number	<nif no.>/<port no.>: Indicates the port number.
CH	Channel group number	<channel group number>: Indicates the channel group number.
Up	The port is in Up status.	--
Down	The port is in Down status.	--
Down(loop)	The port status is Down due to the L2 loop detection 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 that the port or channel group was inactivated	--
RxDiscard	Number of L2 loop detection frames that have been received and discarded	--
Last Inactive	Time when the port or channel group was last inactivated	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second - is displayed if the port or channel group has never been in inactive status.
Last RxFrame	Time when the L2 loop detection frame was last received	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second - is displayed if no L2 loop detection frames have been received. The time an L2 loop detection frame was received and discarded is not displayed.

Impact on communication

None

Response messages

Table 14-4: List of response messages for the show loop-detection statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Loop Detection program.	Communication with the L2 loop detection program failed. Re-execute the command.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the functionality has not been enabled. Check the configuration.
No corresponding port information.	No port and channel group information for L2 loop detection was found.

Notes

None

show loop-detection logging

Displays the 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

The following figure is an example of displaying log information about the received L2 loop detection frames.

Figure 14-3: Example of displaying log information for received L2 loop detection frames

```
> show loop-detection logging
Date 2008/04/21 12:10:10 UTC
2008/04/21 12:10:10 1/1 Source: 1/3 Vlan: 4090 Inactive
2008/04/21 12:10:09 1/1 Source: 1/3 Vlan: 1
2008/04/21 12:10:08 1/1 Source: 1/3 Vlan: 4090
2008/04/21 12:10:07 1/3 Source: 1/1 Vlan: 4090
2008/04/21 12:10:06 1/3 Source: 1/1 Vlan: 4090
2008/04/20 05:10:10 CH:32 Source: CH:32 Vlan: 4090 Uplink Inactive
2008/04/10 04:10:10 1/20 Source: CH:32 Vlan: 4090
2008/03/21 03:10:10 1/20 Source: 1/12 Vlan: 4095
2008/03/21 02:12:50 1/20 Source: 1/12 Vlan: 4095
2008/03/21 02:12:10 1/20 Source: 1/12 Vlan: 4095
2008/03/21 02:12:09 1/20 Source: 1/12 Vlan: 12
2007/09/05 20:00:00 CH:32 Source: 1/12 Vlan: 12 Uplink
2007/09/05 00:00:00 CH:32 Source: 1/12 Vlan: 12 Uplink
>
```

Display items

Table 14-5: Items displayed for the log information about received L2 loop detection frames

Item	Meaning	Displayed information
yyyy/mm/dd hh:mm:ss	Time when an L2 loop detection frame was received	year/month/day hour:minute:second
<nif no.>/<port no.>	Port number	Displays the number of the port on which the L2 loop detection frame was received.
CH:<channel group number>	Channel group number	Displays the number of the channel group on which the L2 loop detection frame was received.
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. <nif no.>/<port no.>: Indicates the port number. CH: <channel group number>: Indicates the channel group number.
Vlan	VLAN ID	Displays the VLAN ID when an L2 loop detection frame was sent.

Item	Meaning	Displayed information
Uplink	Uplink port	Indicates that an L2 loop detection frame was received on an uplink port.
Inactive	The status is changed to inactive status.	Indicates that the status is changed to inactive status.

Impact on communication

None

Response messages

Table 14-6: List of response messages for the show loop-detection logging command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Loop Detection program.	Communication with the L2 loop detection program failed. Re-execute the command.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the functionality has not been enabled. Check the configuration.

Notes

None

clear loop-detection statistics

Clears the L2 loop detection statistics.

Syntax

```
clear loop-detection statistics [port <port list>] [channel-group-number <channel group list>]
```

Input mode

User mode and administrator mode

Parameters

[port <port list>] [channel-group-number <channel group list>]

Clears the L2 loop detection statistics for the specified ports and channel groups. Ports and channel groups can be specified at the same time. In this case, L2 loop detection statistics related to either the specified ports or the specified channel groups are cleared.

port <port list>

Clears the L2 loop detection statistics for the specified port number. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Clears the L2 loop detection statistics for the channel groups specified in list format in the specified link aggregation. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Clears all L2 loop detection statistics, not limiting them to specific ports or specific channel groups.

Example

The following figure is an example of clearing L2 loop detection statistics.

Figure 14-4: Example of clearing L2 loop detection statistics

```
> clear loop-detection statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 14-7: List of response messages for the clear loop-detection statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Loop Detection program.	Communication with the L2 loop detection program failed. Re-execute the command.

Message	Description
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 acquired by SNMP.

clear loop-detection logging

Clears 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 14-5: 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 14-8: List of response messages for the clear loop-detection statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Loop Detection program.	Communication with the L2 loop detection program failed. Re-execute the command.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the functionality has not been enabled. Check the configuration.

Notes

None

restart loop-detection

Restarts the L2 loop detection program.

Syntax

```
restart loop-detection [-f] [core-file]
```

Input mode

User mode and administrator mode

Parameters

-f

Restarts the L2 loop detection program without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file when the program is restarted.

Operation when this parameter is omitted:

A core file is not output.

Operation when all parameters are omitted:

Restarts the L2 loop detection program after displaying a confirmation message.

Example

The following figure is an example of restarting the L2 loop detection program.

Figure 14-6: Example of restarting the L2 loop detection program

```
> restart loop-detection
L2 Loop Detection program restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Response messages

Table 14-9: List of response messages for the restart loop-detection command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
L2 Loop Detection doesn't seem to be running.	The L2 loop detection program has not been started. Check the configuration.

Notes

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

Storage directory: /usr/var/core/

Core file: `l2ldd.core`

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

dump protocols loop-detection

Outputs detailed event trace information and control table information collected by the L2 loop detection program to a file.

Syntax

```
dump protocols loop-detection
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure is an example of outputting detailed event trace information and control table information to a file.

Figure 14-7: Example of outputting detailed event trace information and control table information

```
> dump protocols loop-detection
>
```

Display items

None

Impact on communication

None

Response messages

Table 14-10: List of response messages for the dump protocols loop-detection command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Loop Detection program.	Communication with the L2 loop detection program failed. Re-execute the command.
File open error.	An attempt to open or access a dump file failed.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the functionality has not been enabled. Check the configuration.

Notes

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

Storage directory: /usr/var/l2ld/

Output file: l2ld_dump.gz

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

Chapter

15. CFM

l2ping
l2traceroute
show cfm
show cfm remote-mep
show cfm fault
show cfm l2traceroute-db
show cfm statistics
clear cfm remote-mep
clear cfm fault
clear cfm l2traceroute-db
clear cfm statistics
restart cfm
dump protocols cfm

I2ping

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 15-1: Example of executing the l2ping command

```
>l2ping remote-mep 1010 domain-level 7 ma 1000 mep 1020 count 3
L2ping to MP:1010(0012.e220.00a3) on Level:7 MA:1000 MEP:1020 VLAN:20
Time:2009/03/10 19:10:24
1: L2ping Reply from 0012.e220.00a3 64bytes Time= 751 ms
2: L2ping Reply from 0012.e220.00a3 64bytes Time= 752 ms
3: L2ping Reply from 0012.e220.00a3 64bytes Time= 753 ms

--- L2ping Statistics ---
Tx L2ping Request : 3 Rx L2ping Reply : 3 Lost Frame : 0%
Round-trip Min/Avg/Max : 751/752/753 ms
>
```

Display items

Table 15-1: Items displayed for the l2ping command

Item	Meaning	Displayed information
L2ping to MP:<remote mp>	The MAC address of the destination remote MEP or MIP.	The MAC address of the destination remote MEP or MIP. <remote mac address>: When the MAC address of the destination remote MEP or MIP is specified. <remote mep id> (<remote mac address>): When the destination remote MEP ID is specified.
Level	Domain level	0 to 7
MA	MA ID number	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	--
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 15-2: List of response messages for the l2ping command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.
No such Remote MEP.	The specified remote MEP is unknown. Make sure the specified parameter is correct, and then try again.
Now another user is using CFM command, please try again.	Another user is using the CFM command. Wait a while, and then retry the operation.
Specified Domain Level is not configured.	The specified domain level has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MA is not configured.	The specified MA ID number or the primary VLAN for the specified MA has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MEP is not configured.	The specified MEP ID has not been configured. Make sure the specified parameter is correct, and then try again.

Notes

- To halt execution of this command, press **Ctrl + C**.
- This command cannot be used concurrently by multiple users.
- If you want to specify 1477 bytes or more for the `framesize` parameter, use the `mtu` or `system mtu` configuration command to set the MTU value for jumbo frames to 1500 bytes or more.
- To verify connectivity, use the MAC address for the remote MP. Even when `remote-mep` is specified, the connectivity is verified by using the MAC address that corresponds to the MEP ID. Therefore, even when the specified MEP ID does not exist, due to a configuration change or another reason, a reply is sent if an MEP or MIP has that MAC address.

l2traceroute

Verifies the route from the Switch's MEP to a remote MEP or MIP.

Syntax

```
l2traceroute {remote-mac <mac address> | remote-mep <mepid>} domain-level
<level> ma <no.> mep <mepid> [timeout <seconds>] [ttl <ttl>]
```

Input mode

User mode and administrator mode

Parameters

```
{remote-mac <mac address> | remote-mep <mepid>}
```

```
remote-mac <mac address>
```

Specify the MAC address of the destination remote MEP or MIP whose route you want to verify.

```
remote-mep <mepid>
```

Specify the destination remote MEP ID 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 15-2: Example of executing the l2traceroute command

```
>l2traceroute remote-mep 1010 domain-level 7 ma 1000 mep 1020 ttl 255
L2traceroute to MP:1010(0012.e220.00a3) on Level:7 MA:1000 MEP:1020 VLAN:20
Time:2009/03/17 10:42:20
254 0012.e220.00c2 Forwarded
253 0012.e210.000d Forwarded
```

```
252  0012.e220.00a3  NotForwarded  Hit
>
```

Display items

Table 15-3: Items displayed for the l2tracert command

Item	Meaning	Displayed information
L2tracert to MP:<remote mp>	The MAC address of the destination remote MEP or MIP.	The MAC address of the destination remote MEP or MIP. <remote mac address>: When the MAC address of the destination remote MEP or MIP is specified. <remote mep id> (<remote mac address>): When the destination remote MEP ID is specified.
Level	Domain level	0 to 7
MA	MA ID number	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 15-4: List of response messages for the l2tracert command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.
No such Remote MEP.	The specified remote MEP is unknown. Make sure the specified parameter is correct, and then try again.
Now another user is using CFM command, please try again.	Another user is using the CFM command. Wait a while, and then retry the operation.

Message	Description
Specified Domain Level is not configured.	The specified domain level has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MA is not configured.	The specified MA ID number or the primary VLAN for the specified MA has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MEP is not configured.	The specified MEP ID has not been configured. Make sure the specified parameter is correct, and then try again.

Notes

- To halt execution of this command, press **Ctrl + C**.
- This command cannot be used concurrently by multiple users.
- If you execute this command multiple times for the same remote MP, only the last execution result is retained in the linktrace database.
- Information about some replies is not displayed if those replies are received after being forwarded by a number of devices that exceeds the number of devices on the routes that can be registered in the linktrace database.
- The MAC address of the remote MP is used to verify the route. Even when `remote-mep` is specified, the route is verified by using the MAC address that corresponds to the MEP ID. Therefore, even when the specified MEP ID does not exist, due to a configuration change or another reason, a reply is sent if an MEP or MIP has that MAC address.

show cfm

Displays the configuration information for domains and MPs, and the CFM information related to detected failures.

Syntax

```
show cfm [{[domain-level <level>] [ma <no.>] [mep <mepid>] | summary}]
```

Input mode

User mode and administrator mode

Parameters

```
{[domain-level <level>] [ma <no.>] [mep <mepid>] | summary}
```

domain-level <level>

Displays CFM information for the specified domain level.

ma <no.>

Displays CFM information for the specified MA ID number.

mep <mepid>

Displays CFM information for the specified MEP ID.

Operation when a 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 15-3: Example of displaying the CFM configuration information

```
>show cfm
Date 2009/03/15 18:32:10 UTC
Domain Level 3 Name(str): ProviderDomain_3
  MA 300   Name(str) : Tokyo_to_Osaka
    Primary VLAN:300   VLAN:10-20,300
    CC:Enable   Interval:1min
    Alarm Priority:2   Start Time: 2500ms   Reset Time:10000ms
    MEP Information
      ID:8012 UpMEP    CH1 (Up)    Enable   MAC:0012.e200.00b2   Status:Timeout
  MA 400   Name(str) : Tokyo_to_Nagoya
    Primary VLAN:400   VLAN:30-40,400
    CC:Enable   Interval:1min
    Alarm Priority:2   Start Time: 2500ms   Reset Time:10000ms
    MEP Information
      ID:8014 DownMEP  1/21(Up)    Disable  MAC:0012.e220.0040   Status:-
  MIP Information
    1/12(Up)    Enable   MAC:0012.e200.0012
    1/22(Down)  Disable  MAC:-
Domain Level 4 Name(str): ProviderDomain_4
```

```

MIP Information
  CH12 (Up)      Enable    MAC:0012.e220.00b2
>

```

Display items in Example 1

Table 15-5: Items displayed for the CFM configuration information

Item	Meaning	Displayed information
Domain Level <level>	Domain level and domain name	<level>: Indicates the domain level. Name : -: Indicates that the domain name is not used. Name (str) : <name>: Indicates that a character string is used for the domain name. Name (dns) : <name>: Indicates that the domain name server name is used for the domain name. Name (mac) : <mac> (<id>): Indicates that the MAC address and ID are used for the domain name.
MA <no.>	MA ID number and MA name	<no.>: Indicates the MA ID number when the configuration was set. Name (str) : <name>: Indicates that a character string is used for the MA name. Name (id) : <id>: Indicates that a numeric value is used for the MA name. Name (vlan) : <vlan id>: Indicates that the VLAN ID is used for the MA name.
Primary VLAN	Primary VLAN ID	The primary VLAN in the VLANs belonging to the MA. - is displayed if the primary VLAN has not been configured.
VLAN	VLAN ID	VLAN ID 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	Interval for sending CCMs	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.
Alarm Priority	Failure detection priority	Priority of failures for which alarms are generated. If a failure whose level is equal to or higher than the priority that has been set is detected, an alarm is reported. <ul style="list-style-type: none"> 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 generated	2500-10000ms: The time elapsed from the detection of a failure until an alarm is generated. - is displayed if CC is disabled.

Item	Meaning	Displayed information
Reset Time	Time from the detection of a failure until an alarm is canceled	2500-10000ms: The time elapsed from the detection of a failure until an alarm is canceled. - is displayed if CC is disabled.
MEP Information	MEP information	--
ID	MEP ID	MEP ID for the Switch
UpMEP	Up MEP	MEP facing the relay side
DownMEP	Down MEP	MEP facing the line
<nif no.> / <port no.>	Port number	MEP port number
CH<channel group number>	Channel group number	MEP channel group number
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
Enable	CFM on a port is enabled.	--
Disable	CFM on a port is disabled.	--
MAC	MEP MAC address	- is displayed if the status of the port to which the MEP belongs is Down.
Status	Status of failure detection on the MEP	The highest-level failure of the failures detected by MEP is displayed. <ul style="list-style-type: none"> • 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 no failure has been detected.
MIP Information	MIP information	--
<nif no.> / <port no.>	Port number	MIP port number
CH<channel group number>	Channel group number	MIP channel group number
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
Enable	CFM on a port is enabled.	--
Disable	CFM on a port is disabled.	--
MAC	MIP MAC address	- is displayed if the status of the port to which the MIP belongs is Down.

Example 2

The following figure is an example of displaying the number of entities accommodated in the CFM configuration.

Figure 15-4: Example of displaying the number of entities accommodated in the CFM configuration

```
>show cfm summary
Date 2009/03/14 18:32:20 UTC
DownMEP Counts      :      2
UpMEP Counts        :      2
MIP Counts           :      5
CFM Port Counts      :      9
>
```

Display items in Example 2

Table 15-6: Items displayed for the number of entities accommodated in the CFM configuration

Item	Meaning	Displayed information
DownMEP Counts	Number of Down MEPs	Number of Down MEPs set in the configuration
UpMEP Counts	Number of Up MEPs	Number of Up MEPs set in the configuration
MIP Counts	Number of MIPs	Number of MIPs set in the configuration
CFM Port Counts	Total number of CFM ports	Total number of VLAN ports to which CFM frames are sent out of primary VLANs for MA (For MA for which only Down MEP is configured, total number of Down MEP's VLAN ports. For MA that contains Up MEPs, total number of all VLAN ports of the primary VLAN).

Impact on communication

None

Response messages

Table 15-7: List of response messages for the show cfm command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.
Specified Domain Level is not configured.	The specified domain level has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MA is not configured.	The specified MA ID 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 monitoring status of connection between the Switch's MEP and the remote MEP.

Syntax

```
show cfm remote-mep [domain-level <level>] [ma <no.>] [mep <mepid>] [remote-mep <mepid>] [detail]
```

Input mode

User mode and administrator mode

Parameters

domain-level <level>

Displays the remote MEP information for the specified domain level.

ma <no.>

Displays the remote MEP information for the specified MA ID number.

mep <mepid>

Displays the remote MEP information for the specified MEP ID.

remote-mep <mepid>

Displays information for the specified remote MEP ID.

Operation when a 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 15-5: Example of displaying remote MEP information

```
>show cfm remote-mep
Date 2009/03/20 18:05:12 UTC
Total RMEP Counts:      4
Domain Level 3 Name(str): ProviderDomain_3
  MA 100  Name(str) : Tokyo_to_Osaka
    MEP ID:101  1/20 (Up)  Enable  Status:Timeout
    RMEP Information Counts: 2
    ID:3      Status:Timeout  MAC:0012.e220.1224  Time:2009/03/20 17:55:20
    ID:15     Status:-      MAC:0012.e200.005a   Time:2009/03/20 18:04:54
  MA 200  Name(str) : Tokyo_to_Nagoya
    MEP ID:8012 CH1 (Up)  Enable  Status:-
    RMEP Information Counts: 2
```

ID:8003 Status:-
ID:8004 Status:-

MAC:0012.e20a.1241 Time:2009/03/20 12:12:20
MAC:0012.e20d.12a1 Time:2009/03/20 12:12:15

>

Display items in Example 1

Table 15-8: Items displayed for remote MEP information

Item	Meaning	Displayed information
Total RMEP Counts	Total number of remote MEPs	--
Domain Level <level>	Domain level and domain name	<level>: Indicates the domain level. Name:-: Indicates that the domain name is not used. Name(str): <name>: Indicates that a character string is used for the domain name. Name(dns): <name>: Indicates that the domain name server name is used for the domain name. Name(mac): <mac> (<id>): Indicates that the MAC address and ID are used for the domain name.
MA <no.>	MA ID number and MA name	<no.>: Indicates the MA ID number when the configuration was set. Name(str): <name>: Indicates that a character string is used for the MA name. Name(id): <id>: Indicates that a numeric value is used for the MA name. Name(vlan): <vlan id>: Indicates that the VLAN ID is used for the MA name.
MEP ID	MEP ID for the Switch	--
<nif no.> / <port no.>	Port number	MEP port number
CH<channel group number>	Channel group number	MEP channel group number
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
Enable	CFM on a port is enabled.	--
Status	The status of failure detection on the Switch's MEP	Displays a failure with the highest priority detected by the Switch's MEP. <ul style="list-style-type: none"> 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 no failure has been detected.
RMEP Information	Remote MEP information	--
Counts	Number of remote MEPs	--
ID	Remote MEP ID	--

Item	Meaning	Displayed information
Status	The status of failure detection in the remote MEP	Displays a remote MEP failure with the highest priority. <ul style="list-style-type: none"> • 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 no failure has been detected.
MAC	MAC address of the remote MEP	--
Time	The time when a CCM was last received	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second

Example 2

The following figure is an example of displaying detailed remote MEP information.

Figure 15-6: Example of displaying detailed remote MEP information

```
> show cfm remote-mep detail
Date 2009/03/20 18:19:03 UTC
Total RMEP Counts:      4
Domain Level 3 Name(str): ProviderDomain_3
  MA 100  Name(str) : Tokyo_to_Osaka
    MEP ID:101  1/20(Up)  Enable  Status:Timeout
      RMEP Information Counts:  2
        ID:3      Status:Timeout  MAC:0012.e220.1224  Time:2009/03/20 17:55:20
          Interface:Up  Port:Forwarding  RDI:On
            Chassis ID Type:MAC  Info: 0012.e220.1220
        ID:15      Status:-  MAC:0012.e200.005a  Time:2009/03/20 18:04:54
          Interface:Up  Port:Forwarding  RDI:-
            Chassis ID Type:MAC  Info: 0012.e200.0050
>
```

Display items in Example 2

Table 15-9: Items displayed for detailed remote MEP information

Item	Meaning	Displayed information
Total RMEP Counts	Total number of remote MEPs	--
Domain Level <level>	Domain level and domain name	<level>: Indicates the domain level. Name:-: Indicates that the domain name is not used. Name(str): <name>: Indicates that a character string is used for the domain name. Name(dns): <name>: Indicates that the domain name server name is used for the domain name. Name(mac): <mac> (<id>): Indicates that the MAC address and ID are used for the domain name.

Item	Meaning	Displayed information
MA <i><no.></i>	MA ID number and MA name	<i><no.></i> : Indicates the MA ID number when the configuration was set. Name (str) : <i><name></i> : Indicates that a character string is used for the MA name. Name (id) : <i><id></i> : Indicates that a numeric value is used for the MA name. Name (vlan) : <i><vlan id></i> : Indicates that the VLAN ID is used for the MA name.
MEP ID	MEP ID for the Switch	--
<i><nif no.>/<port no.></i>	Port number	MEP port number
CH <i><channel group number></i>	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.
Enabled	CFM on a port is enabled.	--
Status	The status of failure detection on the Switch's MEP	Displays a failure with the highest priority detected by the Switch's MEP. <ul style="list-style-type: none"> 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 no failure has been detected.
RMEP Information	Remote MEP information	--
Counts	Number of remote MEPs	--
ID	Remote MEP ID	--
Status	The status of failure detection in the remote MEP	Displays a remote MEP failure with the highest priority. <ul style="list-style-type: none"> 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 no failure has been detected.
MAC	MAC address of the remote MEP	--
Time	The time when a CCM was last received	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second

Item	Meaning	Displayed information
Interface	The status of the remote MEP interface	<p>The status of InterfaceStatus in the CCM that was last received.</p> <ul style="list-style-type: none"> • 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. <p>- is displayed if this information is not found in the received CCM.</p>
Port	The status of the remote MEP port	<p>The status of PortStatus in the CCM that was last received.</p> <ul style="list-style-type: none"> • Forwarding: Indicates Forwarding status. • Blocked: Indicates blocking status. <p>- is displayed if this information is not found in the received CCM.</p>
RDI	The status of failure detection in the remote MEP	<p>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.</p> <ul style="list-style-type: none"> • On: Indicates that a failure is being detected. <p>- is displayed if no failure has been detected.</p>
Chassis ID	Chassis ID of the remote MEP	Displays the chassis ID information in the CCM that was last received.
Type	Subtype for the chassis ID	<p>Type of the information displayed for Info.</p> <ul style="list-style-type: none"> • 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. <p>- is displayed if this information is not found in the received CCM.</p> <p>For this information sent from the Switch, MAC is displayed for Type and the MAC address of the Switch is displayed for Info.</p>
Info	Information about the chassis ID	<p>Information displayed for Type.</p> <p>- is displayed if this information is not found in the received CCM.</p>

Impact on communication

None

Response messages

Table 15-10: List of response messages for the show cfm remote-mep command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.
No such Remote MEP.	The specified remote MEP is unknown. Make sure the specified parameter is correct, and then try again.
Specified Domain Level is not configured.	The specified domain level has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MA is not configured.	The specified MA ID has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MEP is not configured.	The specified MEP ID has not been configured. Make sure the specified parameter is correct, and then try again.

Notes

None

show cfm fault

Displays the type of failure that has been detected by the CC 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 a 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

The following figure is an example of displaying summary information about a CFM failure.

Figure 15-7: Example of displaying failure information

```
>show cfm fault
Date 2009/03/21 10:24:12 UTC
MD:7  MA:1000  MEP:1000  Fault    Time:2009/03/21 10:15:21
MD:7  MA:1010  MEP:1011  Cleared  Time:-
MD:6  MA:100   MEP:600   Cleared  Time:-
>
```

Display items in Example 1

Table 15-11: Items displayed for failure information

Item	Meaning	Displayed 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 when a failure was detected	The time when a failure was detected by the MEP. If multiple failures have been detected, the time each failure was detected is displayed. yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second - is displayed if the failure has been cleared.

Example 2

The following figure is an example of displaying detailed information about a CFM failure.

Figure 15-8: Example of displaying detailed failure information

```
>show cfm fault domain-level 7 detail
Date 2009/03/21 12:00:15 UTC
MD:7 MA:1000 MEP:1000 Fault
  OtherCCM : - RMEP:1001 MAC:0012.e220.11a1 VLAN:1000 Time:2009/03/21 11:22:17
  ErrorCCM : -
  Timeout   : On RMEP:1001 MAC:0012.e220.11a1 VLAN:1000 Time:2009/03/21 11:42:10
  PortState: -
  RDI       : -
MD:7 MA:1010 MEP:1011 Cleared
  OtherCCM : -
  ErrorCCM : -
  Timeout   : - RMEP:1001 MAC:0012.e220.22a1 VLAN:200 Time:2009/03/21 10:22:17
  PortState: -
  RDI       : -
>
```

Display items in Example 2

Table 15-12: Items displayed for detailed failure information

Item	Meaning	Displayed 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.	--
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.

Item	Meaning	Displayed information
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 was detected on the remote MEP.	Indicates that a CCM reporting detection of a failure was received from the remote MEP. On: A failure was found. -: No failures were found.
RMEP	Remote MEP ID	Indicates the remoter MEP ID of the CCM that triggered failure detection.
MAC	MAC address of the remote MEP	--
VLAN	VLAN that received a CCM	--
Time	Time when a failure was detected	The time when a failure was detected. yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second

Impact on communication

None

Response messages

Table 15-13: List of response messages for the show cfm fault command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.
Specified Domain Level is not configured.	The specified domain level has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MA is not configured.	The specified MA ID has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MEP is not configured.	The specified MEP ID has not been configured. Make sure the specified parameter is correct, and then try again.

Notes

If the interface for which Down MEP is configured goes down, failure information of the corresponding MEP is deleted.

show cfm l2traceroute-db

Displays route information acquired by the `l2traceroute` command and information about the MP on the route. The information registered in the linktrace database is displayed.

Syntax

```
show cfm l2traceroute-db [{remote-mac <mac address> | remote-mep <mepid>}
domain-level <level> ma <no.>] [detail]
```

Input mode

User mode and administrator mode

Parameters

{remote-mac <mac address> | remote-mep <mepid>}

remote-mac <mac address>

Specify the MAC address of the destination remote MEP or MIP on the route that will be displayed.

remote-mep <mepid>

Specify the destination remote MEP ID 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 route information is displayed.

Operation when all parameters are omitted:

All route information in the linktrace database is displayed.

Example 1

The following figure is an example of displaying route information in the linktrace database.

Figure 15-9: Example of displaying linktrace database information

```
> show cfm l2traceroute-db
Date 2009/03/15 10:05:30 UTC
L2traceroute to MP:0012.e220.00a3 on Level:7 MA:1000 MEP:1020 VLAN:1000
Time:2009/03/14 17:42:20
254 0012.e220.00c0 Forwarded
253 0012.e210.000d Forwarded
252 0012.e220.00a3 NotForwarded Hit

L2traceroute to MP:2010(0012.e220.1040) on Level:7 MA:2000 MEP:2020 VLAN:20
Time:2009/03/14 17:37:55
63 0012.e220.10a9 Forwarded
62 0012.e220.10c8 NotForwarded
>
```

Display items in Example 1

Table 15-14: Items displayed for linktrace database information

Item	Meaning	Displayed information
L2traceroute to MP:<remote mp>	The MAC address of the destination remote MEP or MIP.	The MAC address of the destination remote MEP or MIP. <remote mac address>: When the MAC address of the destination remote MEP or MIP is specified. <remote mep id> (<remote mac address>): When the destination remote MEP ID is specified.
Level	Domain level	0 to 7
MA	MA ID number	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 15-10: Example of displaying detailed linktrace database information

```
> show cfm l2traceroute-db remote-mep 2010 domain-level 7 ma 2000 detail
Date 2009/03/15 10:30:12 UTC
L2traceroute to MP:2010(0012.e220.1040) on Level:7 MA:2000 MEP:2020 VLAN:20
Time:2009/03/14 17:37:55
63 0012.e220.10a9 Forwarded
  Last Egress : 0012.e210.2400 Next Egress : 0012.e220.10a0
  Relay Action: MacAdrTbl
  Chassis ID   Type: MAC           Info: 0012.e228.10a0
  Ingress Port MP Address: 0012.e220.10a9 Action: OK
  Egress Port  MP Address: 0012.e220.10aa Action: OK
62 0012.e228.aa38 NotForwarded
  Last Egress : 0012.e220.10a0 Next Egress : 0012.e228.aa30
  Relay Action: MacAdrTbl
  Chassis ID   Type: MAC           Info: 0012.e228.aa30
  Ingress Port MP Address: 0012.e228.aa38 Action: OK
  Egress Port  MP Address: 0012.e228.aa3b Action: Down
>
```


Display items in Example 2

Table 15-15: Items displayed for the detailed linktrace database information

Item	Meaning	Displayed information
L2tracroute to MP:<remote mp>	The MAC address of the destination remote MEP or MIP.	The MAC address of the destination remote MEP or MIP. <remote mac address>: When the MAC address of the destination remote MEP or MIP is specified. <remote mep id> (<remote mac address>): When the destination remote MEP ID is specified.
Level	Domain level	0 to 7
MA	MA ID number	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 found in the received linktrace reply.
Next Egress	ID of the device that received a linktrace message	The MAC address that identifies the device that received a linktrace message. - is displayed if this information is not found in the received linktrace reply. The device MAC address is used for sending this information from the Switch to another device.
Relay Action	The processing method for forwarding a linktrace message	The processing method for forwarding a linktrace message <ul style="list-style-type: none"> • RlyHit: A linktrace message was not forwarded because it had reached the destination (the destination remote MEP or MIP). • MacAddrTbl: A linktrace message was forwarded by using the MAC address table. • MPCCMDB: A linktrace message was forwarded by using the MIPCCM database. - is displayed if a linktrace message was not forwarded for a response from a destination other than the MP.
Chassis ID	Chassis ID of the replying MP	The chassis ID of the MP that sent a linktrace reply.

Item	Meaning	Displayed information
Type	Subtype of the chassis ID	<p>Type of the information displayed for Info.</p> <ul style="list-style-type: none"> 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. <p>- is displayed if this information is not found in the received linktrace reply.</p> <p>For this information sent from the Switch, MAC is displayed for Type and the MAC address of the Switch is displayed for Info.</p>
Info	Information about the chassis ID	<p>Information displayed for Type.</p> <p>- is displayed if this information is not found in the received linktrace reply.</p>
Ingress Port	Information about MP ports that received a linktrace message	--
MP Address	MAC address of the MP that received a linktrace message	<p>The MAC address of the MP that received a linktrace message.</p> <p>- is displayed if this information is not found in the received linktrace reply.</p>
Action	Status of the port that received a linktrace message	<p>Displays the status of the MP port that received the linktrace message of each device.</p> <ul style="list-style-type: none"> OK: Indicates normal status. Down: Indicates Down status. Blocked: Indicates Blocked status. NOVLAN: Indicates that there is no VLAN setting for linktrace messages. <p>- is displayed if this information is not found in the received linktrace reply.</p>
Egress Port	Port information for the MP that forwarded a linktrace message	--
MP Address	MAC address of the port used to forward the linktrace message	<p>The MAC address of the port used to send a linktrace message.</p> <p>- is displayed if this information is not found in the received linktrace reply.</p>
Action	Status of the port used to forward a linktrace message	<p>The status of the MP port used to forward each device's linktrace message.</p> <ul style="list-style-type: none"> OK: Indicates normal status. Down: Indicates Down status. Blocked: Indicates Blocked status. NOVLAN: Indicates that there is no VLAN setting for linktrace messages. <p>- is displayed if this information is not found in the received linktrace reply.</p>

Impact on communication

None

Response messages

Table 15-16: List of response messages for the show cfm l2traceroute-db command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.

Notes

Information about some replies is not displayed if those replies are received after being forwarded by a number of devices that exceeds the number of devices on the routes that can be registered in the linktrace database.

show cfm statistics

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 a 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 15-11: Example of displaying CFM statistics

```
>show cfm statistics domain-level 3
Date 2009/03/15 18:32:10 UTC
Domain Level 3 Name(str): ProviderDomain_3
MA 300 Name(str) : Tokyo_to_Osaka_300
MEP ID:10 1/47 (Up) CFM:Disable
  CCM Tx:      80155 Rx:      784 RxDiscard:      6
  LBM Tx:       2 Rx:       11 RxDiscard:      1
  LBR Tx:      12 Rx:       2 RxDiscard:      0
  LTM Tx:       0 Rx:       0 RxDiscard:      0
  LTR Tx:       0 Rx:       0 RxDiscard:      0
                        Other RxDiscard:      0

MIP Information
1/48 (Up) CFM:Enable
  CCM Tx:      - Rx:      - RxDiscard:      -
  LBM Tx:      - Rx:      0 RxDiscard:      1
  LBR Tx:       0 Rx:      - RxDiscard:      -
  LTM Tx:      - Rx:      3 RxDiscard:      0
  LTR Tx:       3 Rx:      - RxDiscard:      -
                        Other RxDiscard:      0
>
```

Display items

Table 15-17: Items displayed for CFM statistics

Item		Meaning	Displayed information
Domain Level <level>		Domain level and domain name	<level>: Indicates the domain level. Name: -: Indicates that the domain name is not used. Name (str): <name>: Indicates that a character string is used for the domain name. Name (dns): <name>: Indicates that the domain name server name is used for the domain name. Name (mac): <mac> (<id>): Indicates that the MAC address and ID are used for the domain name.
MA <no.>		MA ID number and MA name	<no.>: Indicates the MA ID number when the configuration was set. Name (str): <name>: Indicates that a character string is used for the MA name. Name (id): <id>: Indicates that a numeric value is used for the MA name. Name (vlan): <vlan id>: Indicates that the VLAN ID is used for the MA name.
MEP ID		MEP ID for the Switch	--
<nif no.> / <port no.>		Port number	MEP port number
CH<channel group number>		Channel group number	MEP channel group number
Up		The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down		The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
CFM		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	--
<nif no.> / <port no.>		Port number	MIP port number
CH<channel group number>		Channel group number	MIP channel group number
Up		The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down		The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
CFM		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.

Item		Meaning	Displayed information
	Rx	Number of CCM receptions	- is displayed for MIP.
	RxDiscard	Number of discarded CCMs	For an MEP, the following CCMs are discarded: <ul style="list-style-type: none"> • 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 - 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: <ul style="list-style-type: none"> • A loopback message with an invalid format • A loopback message whose destination MAC address is not the MAC address for the receiving MP or the multicast address for CC • A loopback message whose source MAC address is the multicast address for a CC or a linktrace • A loopback message whose destination MAC address is not the MAC address for the receiving MIP (for an MIP)
LBR	Tx	Number of loopback replies that have been sent	--
	Rx	Number of loopback replies that have been received	- is displayed for MIP.
	RxDiscard	Number of loopback replies that have been discarded	For an MEP, the following loopback replies are discarded: <ul style="list-style-type: none"> • A loopback reply with an invalid format • A loopback reply whose destination MAC address is different from the MAC address of the MEP • A loopback reply whose source MAC address is the multicast address or broadcast address • A loopback reply whose Loopback Transaction Identifier value is different from that in the loopback message that was sent • A loopback reply that was received after the wait time for a response that was set by an operation command expired - is displayed for MIP.
LTM	Tx	Number of linktrace messages that have been sent	- is displayed for MIP.
	Rx	Number of linktrace messages that have been received	--

Item		Meaning	Displayed information
	RxDiscard	Number of linktrace messages that have been discarded	The following linktrace messages are discarded: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • A linktrace reply with an invalid format • A linktrace reply whose destination MAC address is different from the MAC address of the receiving MEP • A linktrace reply whose LTR Transaction Identifier value is different from the value in the linktrace message • A linktrace reply that was received after the wait time for a response that was set by an operation command expired - is displayed for MIP.
Other RxDiscard		Number of other CFM PDUs that have been discarded	The following CFM PDUs are counted: <ul style="list-style-type: none"> • Unsupported CFM PDUs • Loopback replies and linktrace replies received by MIP

Impact on communication

None

Response messages

Table 15-18: List of response messages for the show cfm statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.
Specified Domain Level is not configured.	The specified domain level has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MA is not configured.	The specified MA ID 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.

15. CFM

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 a 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 15-12: Example of clearing remote MEP information

```
> clear cfm remote-mep
>
```

Display items

None

Impact on communication

None

Response messages

Table 15-19: List of response messages for the clear cfm remote-mep command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.

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 a 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 15-13: Example of clearing CFM failure information

```
> clear cfm fault
>
```

Display items

None

Impact on communication

None

Response messages

Table 15-20: List of response messages for the clear cfm fault command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.

15. CFM

Notes

None

clear cfm l2tracroute-db

Clears CFM linktrace database information.

Syntax

```
clear cfm l2tracroute-db
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure is an example of clearing CFM linktrace database information.

Figure 15-14: Example of clearing CFM linktrace database information

```
> clear cfm l2tracroute-db
>
```

Display items

None

Impact on communication

None

Response messages

Table 15-21: List of response messages for the clear cfm l2tracroute-db command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.

Notes

None

clear cfm statistics

Clears the CFM statistics.

Syntax

```
clear cfm statistics [domain-level <level> [ma <no.> [mep <mepid>]]]
clear cfm statistics [domain-level <level> [mip] [port <port list>]
[channel-group-number <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 a 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 15-15: Example of clearing CFM statistics

```
> clear cfm statistics
>
```

Display items

None

Impact on communication

None

Response messages*Table 15-22:* List of response messages for the clear cfm statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.

Notes

None

restart cfm

Restarts the CFM program.

Syntax

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

Input mode

User mode and administrator mode

Parameters

-f

Restarts the CFM program without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file when the program is restarted.

Operation when this parameter is omitted:

A core file is not output.

Operation when all parameters are omitted:

Restarts the CFM program after displaying a confirmation message.

Example

The following figure is an example of restarting the CFM program.

Figure 15-16: Example of restarting the CFM program

```
> restart cfm
CFM program restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Response messages

Table 15-23: List of response messages for the restart cfm command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
CFM doesn't seem to be running.	The CFM program is not running. Check the configuration.

Notes

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

Storage directory: `/usr/var/core/`

Core file: `cfmd.core`

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

dump protocols cfm

Dumps detailed event trace information and control table information collected by the CFM program to a file.

Syntax

```
dump protocols cfm
```

Input mode

User mode and administrator mode

Parameters

None

Example

The following figure is an example for collecting dump information of the CFM program.

Figure 15-17: Example of collecting dump information of the CFM program

```
> dump protocols cfm
>
```

Display items

None

Impact on communication

None

Response messages

Table 15-24: List of response messages for the dump protocols cfm command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.
File open error.	An attempt to open or access a dump file failed.

Notes

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

Storage directory: `/usr/var/cfm/`

Output file: `cfmd_dump.gz`

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

Chapter

16. SNMP

```
show snmp
show snmp pending
snmp lookup
snmp get
snmp getnext
snmp walk
snmp getif
snmp getroute
snmp getarp
snmp getforward
snmp rget
snmp rgetnext
snmp rwalk
snmp rgetroute
snmp rgetarp
```

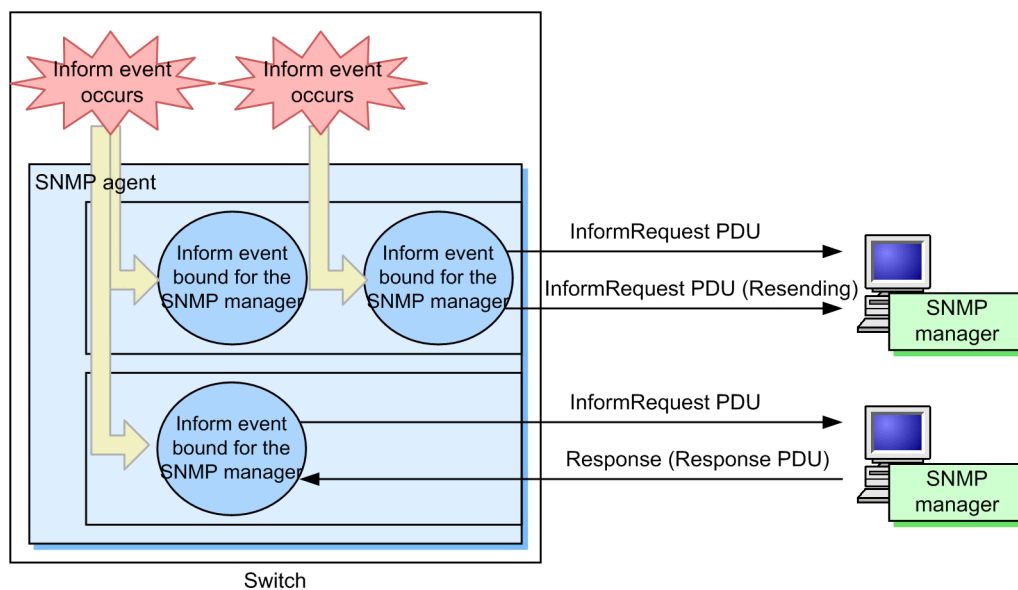
show snmp

Displays SNMP information.

For inform requests, information is displayed for each of the following units:

- Inform event
- Inform event bound for the SNMP manager
- InformRequest PDU

Figure 16-1: InformRequest information



Syntax

```
show snmp
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 16-2: Example of executing the show snmp command

```
> show snmp
Date 2011/12/27 15:06:08 UTC
Contact: Suzuki@example.com
Location: ServerRoom
SNMP packets input : 137      (get:417 set:2)
  Get-request PDUs   : 18
  Get-next PDUs     : 104
  Get-bulk PDUs      : 0
  Set-request PDUs   : 6
  Response PDUs      : 3      (with error 0)
  Error PDUs         : 7
    Bad SNMP version errors: 1
    Unknown community name : 5
    Illegal operation       : 1
    Encoding errors         : 0
```

```

SNMP packets output : 185
  Trap PDUs          : 4
  Inform-request PDUs : 53
  Response PDUs      : 128    (with error 4)
    No errors         : 124
    Too big errors    : 0
    No such name errors : 3
    Bad values errors : 1
    General errors    : 0
  Timeouts           : 49
  Drops              : 0

[TRAP]
  Host: 192.168.0.1, sent:1
  Host: 192.168.0.2, sent:3

[INFORM]
  Timeout(sec)       : 10
  Retry              : 5
  Pending informs    : 1/25 (current/max)
  Host: 192.168.0.3
    sent      :8          retries:26
    response:2          pending:1          failed:5          dropped:0
  Host: 192.168.0.4
    sent      :3          retries:15
    response:0          pending:0          failed:3          dropped:0
  Host: 2001:db8::10
    sent      :1          retries:0
    response:1          pending:0          failed:0          dropped:0

```

Display items

Table 16-1: Items displayed when the show snmp command is executed

Item	Meaning	Displayed information
Contact	Indicates the contact information of the Switch.	Value set by the snmp-server contact configuration command
Location	Indicates the name of the location where the Switch is installed.	Value set by the snmp-server location configuration command
SNMP packets input	Indicates the snmpInPkts value (total number of received SNMP messages).	
get	Indicates the snmpInTotalReqVars value (total number of MIB objects for which a MIB was successfully collected).	--
set	Indicates the snmpInTotalSetVars value (total number of MIB objects for which a MIB was successfully configured.).	--
Get-request PDUs	Indicates the snmpInGetRequests value (total number of received GetRequestPDUs).	--
Get-next PDUs	Indicates the snmpInGetNexts value (total number of received GetNextRequest PDUs).	--
Get-bulk PDUs	Indicates the total number of received GetBulkRequest PDUs.	0 to 4294967295
Set-request PDUs	Indicates the snmpInSetRequests value (total number of received SetRequest PDUs).	--
Response PDUs	Indicates the snmpInGetResponses value (total number of received GetResponse PDUs).	--

Item	Meaning	Displayed information
with error	Indicates the number of PDUs of the received GetResponse PDUs whose error status is not <code>noError</code> .	0 to 4294967295
Error PDUs	Indicates the total number of errors that occurred in PDU reception processing.	0 to 4294967295
Bad SNMP version errors	Indicates the <code>snmpInBadVersions</code> value (total number of received messages whose version is not supported).	--
Unknown community name	Indicates the <code>snmpInBadCommunityNames</code> value (total number of received SNMP messages from unknown communities).	--
Illegal operation	Indicates the <code>snmpInBadCommunityUses</code> value (total number of received messages that indicate operations that are not permitted by the specified community).	--
Encoding errors	Indicates the <code>snmpInASNParseErrs</code> value (total number of ASN.1 error messages).	--
SNMP packets output	Indicates the <code>snmpOutPkts</code> value (total number of sent SNMP messages).	
Trap PDUs	Indicates the <code>snmpOutTraps</code> value (total number of sent Trap PDUs).	--
Inform-request PDUs	Indicates the total number of sent Inform-request PDUs.	0 to 4294967295
Response PDUs	Indicates the <code>snmpOutGetResponses</code> value (total number of sent GetResponse PDUs).	--
with error	Indicates the number of PDUs of the sent GetResponse PDUs whose error status is not <code>noError</code> .	0 to 4294967295
No errors	Indicates the total number of sent PDUs whose error status is <code>noError</code> .	0 to 4294967295
Too big errors	Indicates the <code>snmpOutTooBigs</code> value (total number of sent PDUs whose error status is <code>tooBig</code>).	--
No such name errors	Indicates the <code>snmpOutNoSuchNames</code> value (total number of sent PDUs whose error status is <code>noSuchName</code>).	--
Bad values errors	Indicates the <code>snmpOutBadValues</code> value (total number of sent PDUs whose error status is <code>badValue</code>).	--
General errors	Indicates the <code>snmpOutGenErrs</code> value (total number of sent PDUs whose error status is <code>genErr</code>).	--
Timeouts	Indicates the total number of InformRequest PDUs for which a timeout occurred.	0 to 4294967295
Drops	Indicates the total number of inform events that were bound for the SNMP manager but were discarded because, for example, the maximum number of inform events that can wait for a response was exceeded.	0 to 4294967295
[TRAP]	Indicates trap information.	

Item	Meaning	Displayed information
Host	Indicates the host for which the trap is issued.	Value set by the <i><manager address></i> parameter of the <code>snmp-server host</code> configuration command
VRF [OP-NPAR]	Indicates the VRF ID.	Value set by the <code>vrf</code> parameter of the <code>snmp-server host</code> configuration command
sent	Indicates the number of times a trap was sent.	0 to 4294967295
[INFORM]	Indicates inform event information.	
Timeout(sec)	Indicates the timeout value (in seconds).	Value set by the <code>timeout</code> parameter of the <code>snmp-server informs</code> configuration command
Retry	Indicates the number of resending attempts that has been set.	Value set by the <code>retries</code> parameter of the <code>snmp-server informs</code> configuration command
Pending informs : <i><current></i> / <i><max></i>	Indicates the number of inform events that are held and the maximum number of inform events that can be held. If the SNMP manager does not respond, an inform event is held.	<i><current></i> : The number of inform events that are currently held. <i><max></i> : Value set by the <code>pending</code> parameter of the <code>snmp-server informs</code> configuration command.
Host	Indicates the inform event destination.	Value set by the <i><manager address></i> parameter of the <code>snmp-server host</code> configuration command
VRF [OP-NPAR]	Indicates the VRF ID.	Value set by the <code>vrf</code> parameter of the <code>snmp-server host</code> configuration command
sent	Indicates the number of inform events bound for the SNMP manager that sent InformRequest PDUs.	0 to 4294967295
retries	Indicates the number of resent InformRequest PDUs.	0 to 4294967295
response	Indicates the number of responses from the SNMP manager for inform events bound for the SNMP manager.	0 to 4294967295
pending	Indicates the number of inform events bound for the SNMP manager that is waiting for a response from another SNMP manager.	0 to 21000
failed	Indicates the number of times sending of an inform event bound for the SNMP manager failed. Sending fails if there is no response after repeated resend attempts.	0 to 4294967295
dropped	Indicates the number of inform events that were bound for the SNMP manager but were discarded because, for example, the maximum number of inform events that can wait for a response was exceeded.	0 to 4294967295

Impact on communication

None

Response messages

Table 16-2: List of response messages for the show snmp command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to SNMP program.	Communication with the SNMP program failed. Re-execute the command.

Notes

1. The Switch support the snmp operation commands that have the functionality equivalent to the SNMP agent and the SNMP manager. The statistics displayed by this command pertain to only the SNMP agent, and do not pertain to SNMP operation commands.
2. In the statistics displayed by this command, the number of messages and PDUs are counted in the same way as when MIBs are acquired from a network SNMP manager. This is true even when MIBs are acquired by using SNMP operation commands.
3. If inform events bound for the SNMP manager occur after a `coldStart` inform event is issued due to startup of the switch, issuance of inform events for the SNMP manager is suppressed until the response to the `coldStart` inform event is received. The inform events that are bound for SNMP manager and that have not yet been issued are counted as `sent` and `pending`.

show snmp pending

Displays inform events bound for the SNMP manager that is waiting for a response from another SNMP manager.

Syntax

```
show snmp pending
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 16-3: Example of executing the show snmp pending command

```
> show snmp pending
Date 2011/12/27 15:06:10 UTC
Req ID: 48, Dest: 192.168.0.1, Remaining Retry: 2, Expires in seconds: 3
Req ID: 49, Dest: 192.168.0.2, Remaining Retry: 4, Expires in seconds: 3
Req ID: 50, Dest: 192.168.0.3, Remaining Retry: 2, Expires in seconds: 7
Req ID: 51, Dest: 192.168.0.4, Remaining Retry: 4, Expires in seconds: 7
Req ID: 52, Dest: 2001:db8::10, Remaining Retry: 10, Expires in seconds: 30
```

Display items

Table 16-3: Items displayed when the show snmp pending command is executed

Item	Meaning	Displayed information
Req ID	Request ID	--
Dest	Destination SNMP manager	Value set by the <i><manager address></i> parameter of the <i>snmp-server host</i> configuration command
VRF [OP-NPAR]	VRF ID of the SNMP manager	Value set by the <i><vrfid></i> parameter of the <i>snmp-server host</i> configuration command
Remaining Retry	Remaining number of retries	0 to 100 If the value of this item is 0, whether a response is made is checked, but no resend attempts are performed.
Expires in seconds	Remaining time before the session times out	0 to 21474835 (seconds)

Impact on communication

None

Response messages

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

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to SNMP program.	Communication with the SNMP program failed. Re-execute the command.
no entries.	There are no inform events bound for the SNMP manager.

Notes

If this command is executed when inform events bound for the SNMP manager time out simultaneously, the command might display 0 for all sessions as the remaining time before a timeout (as shown in the following example).

Example

```
> show snmp pending
Date 2011/12/27 17:06:10 UTC
Req ID: 88, Dest: 192.168.0.1, Remaining Retry: 0, Expires in seconds: 0
Req ID: 89, Dest: 192.168.0.2, Remaining Retry: 0, Expires in seconds: 0
Req ID: 90, Dest: 192.168.0.3, Remaining Retry: 0, Expires in seconds: 0
```

snmp lookup

Displays supported MIB object names and object IDs.

Syntax

```
snmp lookup [<variable name>]
```

Input mode

User mode and administrator mode

Parameters

<variable name>

Specify an object name or an object in dot notation.

A list of object names that follow the specified object or objects in dot notation are displayed.

Operation when this parameter is omitted:

All object names are listed in dot notation.

Example

Figure 16-4: Example of executing the snmp lookup command

```
> snmp lookup sysDescr
sysDescr                                = 1.3.6.1.2.1.1.1

> snmp lookup
iso                                     = 1
org                                     = 1.3
dod                                     = 1.3.6
internet                               = 1.3.6.1
mgmt                                    = 1.3.6.1.2
```

Display items

Supported MIB object names and object IDs are displayed in the <object name> = <object ID> format.

Impact on communication

None

Response messages

Table 16-5: List of response messages for the snmp lookup command

Message	Description
No match found for <MIB object name>	The applicable <MIB object name> cannot be found by using this command.

Notes

None

snmp get

Displays the specified MIB value.

Syntax

```
snmp get <variable name>
```

Input mode

User mode and administrator mode

Parameters

<variable name>

Specify an object name or an object in dot notation.

Searches for and displays management information for the specified object instance.

Example

Figure 16-5: Example of executing the snmp get command

```
> snmp get sysDescr.0

Name: sysDescr.0
Value: ALAXALA AX6300S xxxx Ver. 10.2
> snmp get 1.3.6.1.2.1.1.1.0

Name: sysDescr.0
Value: ALAXALA AX6300S xxxx Ver. 10.2
```

Display items

Table 16-6: Items displayed when the snmp get command is executed

Item	Meaning	Displayed information
Name	Object instance	--
Value	Object instance value	--

Impact on communication

None

Response messages

Table 16-7: List of response messages for the snmp get command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Cannot translate variable class: <MIB Object Name>	The object name <MIB Object Name> is invalid.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>. The object ID specified at the following position is not managed: <Number>.

Message	Description
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
make_obj_id_from_dot, bad character : x,y,z	An object ID specified in dot notation contains invalid characters, such as x, y, and z.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
receive error.	A receive error occurred.
request ID mismatch. Got: <ID1>, expected: <ID2>	A frame whose request ID number of the SNMP frame is <ID2> was expected, but an SNMP frame whose request ID number is <ID1> was received.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

Notes

1. For five minutes immediately after the power is turned on or the `copy` command is used to copy the backup configuration file to the startup configuration file, the `No response` message appears because the SNMP agent is being initialized.
2. If the `snmp-server community` configuration command is not set, the `No response` message appears and the MIB cannot be acquired.

snmp getnext

Displays the MIB value following the specified one.

Syntax

```
snmp getnext <variable name>
```

Input mode

User mode and administrator mode

Parameters

<variable name>

Specify an object name or an object in dot notation.

Searches for and displays the management information following the specified object instance.

Example

Figure 16-6: Example of executing the snmp getnext command

```
> snmp getnext sysObjectID.0

Name: sysUpTime.0
Value: 45300
> snmp getnext 1.3.6.1.2.1.1.2.0

Name: sysUpTime.0
Value: 47300
```

Display items

Table 16-8: Items displayed when the snmp getnext command is executed

Item	Meaning	Displayed information
Name	Object instance following the specified one	--
Value	Object instance value following the specified one	--

Impact on communication

None

Response messages

Table 16-9: List of response messages for the snmp getnext command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Cannot translate variable class: <MIB Object Name>	The object name <MIB Object Name> is invalid.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.

Message	Description
Error code set in packet - No such variable name. Index: <i><Number></i> .	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <i><Number></i> . The object ID specified at the following position is not managed: <i><Number></i> .
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <i><Code></i>	An SNMP frame containing response status code <i><Code></i> , which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
make_obj_id_from_dot, bad character : x,y,z	An object ID specified in dot notation contains invalid characters, such as x, y, and z.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
receive error.	A receive error occurred.
request ID mismatch. Got: <i><ID1></i> , expected: <i><ID2></i>	A frame whose request ID number of the SNMP frame is <i><ID2></i> was expected, but an SNMP frame whose request ID number is <i><ID1></i> was received. Alternatively, a timeout occurred while searching the MIB.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

Notes

1. For five minutes immediately after the power is turned on or the `copy` command is used to copy the backup configuration file to the startup configuration file, the `No response` message appears because the SNMP agent is being initialized.
2. If there are too many interfaces on a Switch, it takes time for searching IP-related MIB information, and a timeout might occur. If that happens, use the `snmp get` command to acquire the information, or use the `snmp getnext` command to set the instance value and then acquire the information.
3. If the `snmp-server community` configuration command is not set, the `No response` message appears and the MIB cannot be acquired.

snmp walk

Displays the specified MIB tree.

Syntax

`snmp walk <variable name>`

Input mode

User mode and administrator mode

Parameters

<variable name>

Specify an object name or an object in dot notation.

Searches the management information following the specified object instance, and then displays all instances of the applicable object.

Example

Figure 16-7: Example of executing the snmp walk command

```
> snmp walk interfaces

Name: ifNumber.0
Value: 3

Name: ifIndex.1
Value: 1

Name: ifIndex.2
Value: 2

Name: ifIndex.3
Value: 3

Name: ifDescr.1
Value: loopback

Name: ifDescr.10
Value: Gigabitether 0/1
```

Display items

Table 16-10: Items displayed when the snmp walk command is executed

Item	Meaning	Displayed information
Name	Object instance	--
Value	Object instance value	--

Impact on communication

None

Response messages

Table 16-11: List of response messages for the snmp walk command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.

Message	Description
Cannot translate variable class: <i><MIB Object Name></i>	The object name <i><MIB Object Name></i> is invalid.
Error code set in packet - General error: <i><Number></i> .	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <i><Number></i> .
Error code set in packet - No such variable name. Index: <i><Number></i> .	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <i><Number></i> . The object ID specified at the following position is not managed: <i><Number></i> .
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <i><Code></i>	An SNMP frame containing response status code <i><Code></i> , which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
make_obj_id_from_dot, bad character : x,y,z	An object ID specified in dot notation contains invalid characters, such as x, y, and z.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
receive error.	A receive error occurred.
request ID mismatch. Got: <i><ID1></i> , expected: <i><ID2></i>	A frame whose request ID number of the SNMP frame is <i><ID2></i> was expected, but an SNMP frame whose request ID number is <i><ID1></i> was received. Alternatively, a timeout occurred while searching the MIB.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

Notes

1. For five minutes immediately after the power is turned on or the `copy` command is used to copy the backup configuration file to the startup configuration file, the `No response` message appears because the SNMP agent is being initialized.
2. If there are too many interfaces on a Switch, it takes time for searching IP-related MIB information, and a timeout might occur. If that happens, use the `snmp get` command to acquire the information, or use the `snmp getnext` command to set the instance value and then acquire the information.
3. If the `snmp-server community` configuration command is not set, the `No response` message appears and the MIB cannot be acquired.

snmp getif

Displays MIB information for the interface group.

Syntax

```
snmp getif
```

Input mode

User mode and administrator mode

Parameters

None

Searches management information for the interface group and then displays interface information.

Example

Figure 16-8: Example of executing the snmp getif command

```
> snmp getif
#  Type      PhysAddr      Adm  Opr  InOctets  OutOctets  InPkts  OutPkts
1  loopback  0012.e200.0000  up   up    18426     18575     290     292
2  Ethernet  0012.e2c0.d161  up   up    24591     3417      377     52
3  Ethernet  0012.e2c0.d162  up   dwn    601       854       6       7
```

Display items

Table 16-12: Items displayed when the snmp getif command is executed

Item	Meaning	Displayed information
#	Indicates the ifIndex number.	--
Type	Indicates the interface type (ifType).	other (A type other than the following types)
		Ethernet
		loopback (local loopback)
		l2vlan
		LA
PhysAddr	Indicates a physical address of an interface (ifPhysAddress).	--
Adm	Indicates the interface status of the configuration (ifAdminStatus).	up (enabled)
		down (disabled)
Opr	Indicates the current interface status (ifOperStatus).	up (enabled)
		dwn (disabled)
		test (being tested)
InOctets	Indicates the number of octets received on an interface (ifInOctets).	--
OutOctets	Indicates the number of octets sent from an interface (ifOutOctets).	--

Item	Meaning	Displayed information
InPkts	Indicates the number of packets received on an interface (ifInUcastPkts+ifInNUcastPkts).	--
OutPkts	Indicates the number of packets sent from an interface (ifOutUcastPkts+ifOutNUcastPkts).	--

Impact on communication

None

Response messages

Table 16-13: List of response messages for the snmp getif command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
receive error.	A receive error occurred.
request ID mismatch. Got: <ID1>, expected: <ID2>	A frame whose request ID number of the SNMP frame is <ID2> was expected, but an SNMP frame whose request ID number is <ID1> was received.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

Notes

1. For five minutes immediately after the power is turned on or the `copy` command is used to copy the backup configuration file to the startup configuration file, the `No response` message appears because the SNMP agent is being initialized.
2. If the `snmp-server community` configuration command is not set, the `No response` message appears and the MIB cannot be acquired.

snmp getroute

Displays the IP routing table (ipRouteTable).

Syntax

```
snmp getroute
```

Input mode

User mode and administrator mode

Parameters

None

Searches management information for ipRouteTable and then displays routing information.

Example

Figure 16-9: Example of executing the snmp getroute command

```
> snmp getroute
Index  Destination      NextHop      Metric1      Type      Proto      Age
  2    10.0.0.0         10.1.1.1         0    direct    local      720
  2    10.1.1.0         10.1.1.1         0    direct    local      720
  2    10.1.1.1         10.1.1.1         0    direct    local      720
  0    127.0.0.0         0.0.0.0         0    other     local      720
  1    127.0.0.1         127.0.0.1        0    direct    local      720
>
```

Display items

Table 16-14: Items displayed when the snmp getroute command is executed

Item	Meaning	Displayed information
Index	Indicates the interface number used for reaching the next hop on this route (ipRouteIfIndex).	--
Destination	Indicates the destination IP address on this route (ipRouteDest).	--
NextHop	Indicates the IP address of the next hop for the destination of this route (ipRouteNextHop).	--
Metric1	Indicates the primary routing metric for this route (ipRouteMetric1).	--
Type	Indicate the type of this route (ipRouteType).	direct (direct route)
		indirect (indirect route)
		invalid (invalid route)
		other (others)
Proto	Indicates the routing protocol (ipRouteProto).	rip (RIP)
		ospf (OSPF)
		bgp (bgp)
		local (static routing)
		netmgmt (static routing)
		other (others)

Item	Meaning	Displayed information
Age	Indicates the number of seconds elapsed after this route was last updated or confirmed (ipRouteAge).	--

Impact on communication

None

Response messages

Table 16-15: List of response messages for the snmp getroute command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
No routing information available.	There were no routing table entries.
receive error.	A receive error occurred.
request ID mismatch. Got: <ID1>, expected: <ID2>	A frame whose request ID number of the SNMP frame is <ID2> was expected, but an SNMP frame whose request ID number is <ID1> was received. Alternatively, a timeout occurred while searching the MIB.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

Notes

1. For five minutes immediately after the power is turned on or the `copy` command is used to copy the backup configuration file to the startup configuration file, the `No response` message appears because the SNMP agent is being initialized.
2. If there are too many interfaces on a Switch, it takes time for searching MIB information for `ipRouteTable`, and a timeout might occur. If that happens, use the `snmp getnext` command to acquire the `ipRouteTable` information.
3. If the `snmp-server community` configuration command is not set, the `No response` message

appears and the MIB cannot be acquired.

snmp getarp

Displays the IP address translation table (ipNetToMediaTable).

Syntax

snmp getarp

Input mode

User mode and administrator mode

Parameters

None

Searches ipNetToMediaTable management information and displays ARP information.

Example

Figure 16-10: Example of executing the snmp getarp command

```
> snmp getarp
Index      Network Address      Physical Address      Type
   4        12.1.1.99          0012.e2c0.d162      static
>
```

Display items

Table 16-16: Items displayed when the snmp getarp command is executed

Item	Meaning	Displayed information
Index	Indicates the interface number that has this ARP information (ipNetToMediaIfIndex).	--
Network Address	Indicates the IP address corresponding to a physical address (ipNetToMediaNetAddress).	--
Physical Address	Indicates a physical address (ipNetToMediaPhysAddress).	--
Type	Indicates the type of mapping (ipNetToMediaType).	other (Mapping other than the following types)
		invalid (invalid mapping)
		dynamic (dynamic mapping)
		static (static mapping)

Impact on communication

None

Response messages

Table 16-17: List of response messages for the snmp getarp command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.

Message	Description
Error code set in packet - No such variable name. Index: <i><Number></i> .	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <i><Number></i> . The object ID specified at the following position is not managed: <i><Number></i> .
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <i><Code></i>	An SNMP frame containing response status code <i><Code></i> , which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
No ARP information available.	There were no ARP table entries.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
receive error.	A receive error occurred.
request ID mismatch. Got: <i><ID1></i> , expected: <i><ID2></i>	A frame whose request ID number of the SNMP frame is <i><ID2></i> was expected, but an SNMP frame whose request ID number is <i><ID1></i> was received. Alternatively, a timeout occurred while searching the MIB.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

Notes

1. For five minutes immediately after the power is turned on or the `copy` command is used to copy the backup configuration file to the startup configuration file, the `No response` message appears because the SNMP agent is being initialized.
2. If there are too many interfaces on a Switch, it takes time for searching MIB information for `ipNetToMediaTable`, and a timeout might occur. If that happens, use the `snmp getnext` command to acquire the `ipNetToMediaTable` information.
3. If the `snmp-server community` configuration command is not set, the `No response` message appears and the MIB cannot be acquired.

snmp getforward

Displays ipForwardTable and axsVrflpForwardTable (IP forwarding table).

Syntax

snmp getforward

Input mode

User mode and administrator mode

Parameters

None

Searches management information for ipForwardTable and axsVrflpForwardTable, and then displays forwarding information.

Example

Figure 16-11: Example of executing the snmp getforward command

```
> snmp getforward
Index  Destination      NextHop      Metric1  Type      Proto      Age  NH-AS
  2    0.0.0.0/0        192.168.0.1      0  remote  netmgmt    855  0
  0    127.0.0.0/8      0.0.0.0          0  other   local      974  0
  1    127.0.0.1/32     127.0.0.1        0  local   local      974  0
  2    192.168.0.0/24   192.168.0.34     0  local   local      855  0
  2    192.168.0.34/32  192.168.0.34     0  local   local      855  0

VRF 3
Index  Destination      NextHop      Metric1  Type      Proto      Age  NH-AS
 1210  10.10.10.0/24     10.10.10.1      0  local   local      855  0

VRF 4
Index  Destination      NextHop      Metric1  Type      Proto      Age  NH-AS
 1211  20.1.1.0/24       20.1.1.1        0  local   local      855  0
 1212  20.20.20.0/24     20.20.20.1      0  local   local      855  0
>
```

Display items

Table 16-18: Items displayed when the snmp getforward command is executed

Item	Meaning	Displayed information
Index	Indicates the identifier of the local interface connected to the next hop on this route (ipForwardIfIndex).	--
Destination	Indicates the destination address of this route (ipForwardDest) and the mask for logical conjunction with the destination (ipForwardMask) displayed in mask length.	--
NextHop	Indicates the address of the next system on the route (ipForwardNextHop).	--
Metric1	Indicates the metric for this route (ipForwardMetric1).	--
Type	Indicates the type of the route (ipForwardType).	local (local)
		remote (remote)
		invalid (invalid)
		other (others)
Proto	Indicates the protocol that learned this route (ipForwardProto).	rip (RIP)

Item	Meaning	Displayed information
		ospf (OSPF)
		bgp (bgp)
		local (static routing)
		netmgmt (static routing)
		other (others)
Age	Indicates the time (in seconds) elapsed since this route was learned or updated (ipForwardAge).	--
NH-AS	Indicates the autonomous system number of the next hop (ipForwardNextHopAS).	--

Table 16-19: Items displayed when the snmp getforward command is executed (by VRF) [OP-NPAR]

Item	Meaning	Displayed information
VRF	Indicates the VRF index (axsVrfIpFwVRFIndex).	--
Index	Indicates the identifier of the local interface connected to the next hop on this route (axsVrfIpFwIfIndex).	--
Destination	Indicates the destination address of this route (axsVrfIpFwDest) and the mask for ANDing with the destination (axsVrfIpFwMask) displayed as a mask length.	--
NextHop	Indicates the address of the next system on this route (axsVrfIpFwNextHop).	--
Metric1	Indicates the metric for this route (axsVrfIpFwMetric1).	--
Type	Indicates the type of the route (axsVrfIpFwType).	local (local)
		remote (remote)
		invalid (invalid)
		other (others)
Proto	Indicates the protocol that learned this route (axsVrfIpFwProto).	rip (RIP)
		ospf (OSPF)
		bgp (bgp)
		local (static routing)
		netmgmt (static routing)
Age	Indicates the time (in seconds) elapsed since this route was learned or updated (axsVrfIpFwAge).	--
		--
NH-AS	Indicates the autonomous system number of the next hop (axsVrfIpFwNextHopAS).	--

Impact on communication

None

Response messages

Table 16-20: List of response messages for the snmp getforward command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
No forwarding information available.	There were no forwarding table entries.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
receive error.	A receive error occurred.
request ID mismatch. Got: <ID1>, expected: <ID2>	A frame whose request ID number of the SNMP frame is <ID2> was expected, but an SNMP frame whose request ID number is <ID1> was received. Alternatively, a timeout occurred while searching the MIB.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

Notes

1. For five minutes immediately after the power is turned on or the `copy` command is used to copy the backup configuration file to the startup configuration file, the `No response` message appears because the SNMP agent is being initialized.
2. If there are too many interfaces on a Switch, it takes time for searching MIB information for `ipForwardTable`, and a timeout might occur. If that happens, use the `snmp getNext` command to acquire the `ipForwardTable` information.
3. If the `snmp-server community` configuration command is not set, the `No response` message appears and the MIB cannot be acquired.

snmp rget

Displays the MIB value for the specified remote device.

Syntax

```
snmp rget [version { 1 | 2 }] <ip address> <community> <variable name>
```

Input mode

User mode and administrator mode

Parameters

Remotely accesses an SNMP agent, acquires and displays management information of the specified object instance.

version { 1 | 2 }

Specify the SNMP version.

Operation when this parameter is omitted:

1 is specified.

<ip address>

Specify the IP address of the device which is remotely accessed.

<community>

Specify the community name of the remote device.

<variable name>

Specify an object name of MIB or an object in dot notation.

Example

Figure 16-12: Example of executing the snmp rget command

```
> snmp rget version 2 192.168.11.35 public sysObjectID.0
```

Name: sysObjectID.0

Value: ax6300s

Display items

Table 16-21: Items displayed when the snmp rget command is executed

Item	Meaning	Displayed information
Name	Object instance following the specified one	--
Value	Object instance value following the specified one	--

Impact on communication

None

Response messages

Table 16-22: List of response messages for the snmp rget command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Cannot translate variable class: <MIB Object Name>	The object name <MIB Object Name> is invalid.

Message	Description
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
make_obj_id_from_dot, bad character : x,y,z	An object ID specified in dot notation contains invalid characters, such as x, y, and z.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
receive error.	A receive error occurred.
request ID mismatch. Got: <ID1>, expected: <ID2>	A frame whose request ID number of the SNMP frame is <ID2> was expected, but an SNMP frame whose request ID number is <ID1> was received.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

Notes

None

snmp rgetnext

Displays the MIB value following the specified remote device.

Syntax

```
snmp rgetnext [version { 1 | 2 }] <ip address> <community> <variable name>
```

Input mode

User mode and administrator mode

Parameters

Remotely accesses an SNMP agent, acquires and displays the management information following the specified object instance.

version { 1 | 2 }

Specify the SNMP version.

Operation when this parameter is omitted:

1 is specified.

<ip address>

Specify the IP address of the device which is remotely accessed.

<community>

Specify the community name of the remote device.

<variable name>

Specify an object name of MIB or an object in dot notation.

Example

Figure 16-13: Example of executing the snmp rgetnext command

```
> snmp rgetnext version 2 192.168.11.35 public sysObjectID.0
```

Name: sysUpTime.0

Value: 27603450

Display items

Table 16-23: Items displayed when the snmp rgetnext command is executed

Item	Meaning	Displayed information
Name	Object instance following the specified one	--
Value	Object instance value following the specified one	--

Impact on communication

None

Response messages

Table 16-24: List of response messages for the snmp rgetnext command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Cannot translate variable class: <MIB Object Name>	The object name <MIB Object Name> is invalid.

Message	Description
Error code set in packet - General error: <i><Number></i> .	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <i><Number></i> .
Error code set in packet - No such variable name. Index: <i><Number></i> .	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <i><Number></i> . The object ID specified at the following position is not managed: <i><Number></i> .
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <i><Code></i>	An SNMP frame containing response status code <i><Code></i> , which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
make_obj_id_from_dot, bad character : x,y,z	An object ID specified in dot notation contains invalid characters, such as x, y, and z.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
receive error.	A receive error occurred.
request ID mismatch. Got: <i><ID1></i> , expected: <i><ID2></i>	A frame whose request ID number of the SNMP frame is <i><ID2></i> was expected, but an SNMP frame whose request ID number is <i><ID1></i> was received. Alternatively, a timeout occurred while searching the MIB.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

Notes

If there are too many interfaces on the target Switch, it takes time for searching IP-related MIB information, and a timeout might occur. If that happens, use the `snmp rget` command to acquire the information, or use the `snmp rgetnext` command to set the instance value, and then acquire the information.

snmp rwalk

Displays information about the MIB tree for the specified remote device.

Syntax

```
snmp rwalk [version { 1 | 2 }] <ip address> <community> <variable name>
```

Input mode

User mode and administrator mode

Parameters

Remotely accesses an SNMP agent, and acquires the management information following the specified object instance, and then displays all instances of the applicable object.

version { 1 | 2 }

Specify the SNMP version.

Operation when this parameter is omitted:

1 is specified.

<ip address>

Specify the IP address of the device which is remotely accessed.

<community>

Specify the community name of the remote device.

<variable name>

Specify an object name of MIB or an object in dot notation.

Example

Figure 16-14: Example of executing the snmp rwalk command

```
> snmp rwalk version 2 192.168.11.35 public ifDescr
```

```
Name: ifDescr.1
```

```
Value: loopback
```

```
Name: ifDescr.10
```

```
Value: 1000BASE-X 0/1 giga01
```

Display items

Table 16-25: Items displayed when the snmp rwalk command is executed

Item	Meaning	Displayed information
Name	Object instance following the specified one	--
Value	Object instance value following the specified one	--

Impact on communication

None

Response messages

Table 16-26: List of response messages for the snmp rwalk command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Cannot translate variable class: <MIB Object Name>	The object name <MIB Object Name> is invalid.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
make_obj_id_from_dot, bad character : x,y,z	An object ID specified in dot notation contains invalid characters, such as x, y, and z.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
receive error.	A receive error occurred.
request ID mismatch. Got: <ID1>, expected: <ID2>	A frame whose request ID number of the SNMP frame is <ID2> was expected, but an SNMP frame whose request ID number is <ID1> was received. Alternatively, a timeout occurred while searching the MIB.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

Notes

If there are too many interfaces on the target Switch, it takes time for searching IP-related MIB information, and a timeout might occur. If that happens, use the `snmp rget` command to acquire the information, or use the `snmp rgetnext` command to set the instance value, and then acquire the information.

snmp rgetroute

Displays the IP routing table (ipRouteTable) of the specified remote device.

Syntax

```
snmp rgetroute <ip address> <community>
```

Input mode

User mode and administrator mode

Parameters

Remotely accesses an SNMP agent and displays routing information from management information of ipRouteTable.

<ip address>

Specify the IP address of the device which is remotely accessed.

<community>

Specify the community name of the remote device.

Example

Figure 16-15: Example of executing the snmp rgetroute command

```
> snmp rgetroute 20.1.30.101 public
No response - retrying...
             - retrying...
             - try again.
```

```
> snmp rgetroute 20.1.30.101 public
Index      Destination      NextHop      Metric1      Type      Proto      Age
  2         20.0.0.0         20.1.1.1         0    direct    local      180
  2         20.1.1.0         20.1.1.1         0    direct    local      720
```

Display items

Table 16-27: Items displayed when the snmp rgetroute command is executed

Item	Meaning	Displayed information
Index	Indicates the interface number used for reaching the next hop on this route (ipRouteIfIndex).	--
Destination	Indicates the destination IP address on this route (ipRouteDest).	--
NextHop	Indicates the IP address of the next hop for the destination of this route (ipRouteNextHop).	--
Metric1	Indicates the primary routing metric for this route (ipRouteMetric1).	--
Type	Indicate the type of this route (ipRouteType).	direct (direct route)
		indirect (indirect route)
		invalid (invalid route)
		other (others)
Proto	Indicates the routing protocol (ipRouteProto).	rip (RIP)
		ospf (OSPF)

Item	Meaning	Displayed information
		bgp (bgp)
		local (static routing)
		netmgmt (static routing)
		other (others)
Age	Indicates the number of seconds elapsed after this route was last updated or confirmed (ipRouteAge).	--

Impact on communication

None

Response messages

Table 16-28: List of response messages for the snmp rgetroute command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
No routing information available.	There were no routing table entries.
receive error.	A receive error occurred.
request ID mismatch. Got: <ID1>, expected: <ID2>	A frame whose request ID number of the SNMP frame is <ID2> was expected, but an SNMP frame whose request ID number is <ID1> was received. Alternatively, a timeout occurred while searching the MIB.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

Notes

- For AUX-port related information, -1 is displayed as a value for Index.

2. If there are too many interfaces on the target Switch, it takes time for searching MIB information for ipRouteTable, and a timeout might occur. If that happens, use the `snmp rgetnext` command to acquire the ipRouteTable information.

snmp rgetarp

Displays the IP address translation table (ipNetToMediaTable) of the specified remote device.

Syntax

```
snmp rgetarp <ip address> <community>
```

Input mode

User mode and administrator mode

Parameters

Remotely accesses an SNMP agent and displays ARP information from management information of ipNetToMediaTable.

<ip address>

Specify the IP address of the device which is remotely accessed.

<community>

Specify the community name of the remote device.

Example

Figure 16-16: Example of executing the snmp rgetarp command

```
> snmp rgetarp 20.1.30.101 public
Index      Network Address      Physical Address      Type
  4         12.1.1.99         0012.e258.8860       static
  1         112.1.1.99         0012.e258.8870       static
```

Display items

Table 16-29: Items displayed when the snmp rgetarp command is executed

Item	Meaning	Displayed information
Index	Indicates the interface number that has this ARP information (ipNetToMediaIfIndex).	--
Network Address	Indicates the IP address corresponding to a physical address (ipNetToMediaNetAddress).	--
Physical Address	Indicates a physical address (ipNetToMediaPhysAddress).	--
Type	Indicates the type of mapping (ipNetToMediaType).	other (Mapping other than the following types)
		invalid (invalid mapping)
		dynamic (dynamic mapping)
		static (static mapping)

Impact on communication

None

Response messages

Table 16-30: List of response messages for the snmp rgetarp command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
No ARP information available.	There were no ARP table entries.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
receive error.	A receive error occurred.
request ID mismatch. Got: <ID1>, expected: <ID2>	A frame whose request ID number of the SNMP frame is <ID2> was expected, but an SNMP frame whose request ID number is <ID1> was received. Alternatively, a timeout occurred while searching the MIB.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

Notes

If there are too many interfaces on the target Switch, it takes time for searching MIB information for ipNetToMediaTable, and a timeout might occur. If that happens, use the `snmp rgetnext` command to acquire the ipNetToMediaTable information.

Chapter

17. sFlow

show sflow
clear sflow statistics
restart sflow
dump sflow

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 17-1: Example of displaying the setting status and the operating status of sFlow statistics

```
> show sflow
Date 2006/10/21 20:04:01 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared: 8:00:05
sFlow agent data :
  sFlow service version : 4
  CounterSample interval rate: 60 seconds
  Default configured rate: 1 per 2048 packets
  Default actual rate : 1 per 2048 packets
  Configured sFlow ingress ports : 1/2-4
  Configured sFlow egress ports : 5/9-11
  Received sFlow samples : 37269  Dropped sFlow samples(Dropped Queue) : 2093 (
2041)
  Exported sFlow samples : 37269  Couldn't export sFlow samples : 0
sFlow collector data :
  Collector IP address: 192.168.4.199  UDP:6343  Source IP address: 130.130.130
.1
  Send FlowSample UDP packets : 12077  Send failed packets: 0
  Send CounterSample UDP packets: 621  Send failed packets: 0
  Collector IP address: 192.168.4.203  UDP:65535  Source IP address: 130.130.13
0.1
  Send FlowSample UDP packets : 12077  Send failed packets: 0
  Send CounterSample UDP packets: 621  Send failed packets: 0
```

Figure 17-2: Example of displaying detailed information about the setting status and the operating status of sFlow statistics

```
> show sflow detail
Date 2006/10/21 20:04:01 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared: 8:00:05
sFlow agent data :
  sFlow service version : 4
  CounterSample interval rate: 60 seconds
  Default configured rate: 1 per 2048 packets
  Default actual rate : 1 per 2048 packets
  Configured sFlow ingress ports : 1/2-4
  Configured sFlow egress ports : 5/9-11
  Received sFlow samples : 37269  Dropped sFlow samples(Dropped Queue) : 2093 (
2041)
  Exported sFlow samples : 37269  Couldn't export sFlow samples : 0
sFlow collector data :
  Collector IP address: 192.168.4.199  UDP:6343  Source IP address: 130.130.130
```



```

.1
  Send FlowSample UDP packets    : 12077  Send failed packets:    0
  Send CounterSample UDP packets:   621  Send failed packets:    0
  Collector IP address: 192.168.4.203  UDP:65535  Source IP address: 130.130.13
0.1
  Send FlowSample UDP packets    : 12077  Send failed packets:    0
  Send CounterSample UDP packets:   621  Send failed packets:    0
Detail data :
  Max packet size: 1400 bytes
  Packet information type: header
  Max header size: 128 bytes
  Extended information type: switch,router,gateway,user,url
  Url port number: 80,8080
  Sampling mode: random-number
  Sampling rate to collector: 1 per 2163 packets
  Target ports for CounterSample: 1/ 2-4 , 5/ 9-11

```

Display items

Table 17-1: 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 <code>clear sflow statistics</code> 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 <code>sflow ingress</code> is set in the configuration and on which sFlow statistics are collected
Configured sFlow egress ports	Ports for which <code>sflow egress</code> 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 accumulated in the sFlow statistics queue for the hardware is not included.)
(Dropped Queue)	Number of packets discarded without being accumulated in a queue. This value is also cleared when the <code>clear qos queueing</code> command is executed.
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

Item	Displayed information
Source IP address	Address used as an agent IP when packets are sent to the collector
Send FlowSample UDP packets	Number of UDP packets for flow samples sent to the collector
Send failed packets	Number of UDP packets that could not be sent to the collector
Send CounterSample UDP packets	Number of UDP packets for counter samples sent to the collector
Max packet size	Maximum sFlow packet size
Packet information type	Basic data format for flow samples
Max header size	Maximum header length 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. Note that if the sampling interval is changed, execute the <code>clear sflow statistics</code> command first. Otherwise, a correct value might not be displayed.
Target ports for CounterSample	Target port for counter samples

Impact on communication

None

Response messages

Table 17-2: List of response messages for the show sflow command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
sflow doesn't seem to be running.	This command failed because the flow statistics program is not started. If this message appears when sFlow statistics are enabled, wait until the sFlow statistics program is restarted, and then re-execute the command.

Notes

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 17-3: List of response messages for the clear sflow statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
sflow doesn't seem to be running.	This command failed because the flow statistics program is not started. If this message appears when sFlow statistics are enabled, wait until the sFlow statistics program is restarted, and then re-execute the command.

Notes

The 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.

restart sflow

Restarts the flow statistics program.

Syntax

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

Input mode

User mode and administrator mode

Parameters

-f

Restarts the flow statistics program without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file of the flow statistics program (`flowd.core`) when the program is restarted.

Operation when this parameter is omitted:

A core file is not output.

Example

```
>restart sflow
sflow program restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Response messages

Table 17-4: List of response messages for the restart sflow command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
sflow doesn't seem to be running.	This command failed because the flow statistics program is not started. If this message appears when sFlow statistics are enabled, wait until the sFlow statistics program is restarted, and then re-execute the command.

Notes

- The counter value for statistics is cleared when the flow statistics program is restarted.
- The storage directory and the name of the core file are as follows:

Storage directory: `/usr/var/core/`

Core file: `flowd.core`

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

dump sflow

Dumps debug information collected in the flow statistics program to a file.

Syntax

```
dump sflow
```

Input mode

User mode and administrator mode

Parameters

None

Example

```
>dump sflow
>
```

Display items

None

Impact on communication

None

Response messages

Table 17-5: List of response messages for the dump sflow command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
sflow doesn't seem to be running.	This command failed because the flow statistics program is not started. If this message appears when sFlow statistics are enabled, wait until the sFlow statistics program is restarted, and then re-execute the command.

Notes

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

Storage directory: /usr/var/flowd/

File: sflow.trc

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

Chapter

18. LLDP

```
show lldp
show lldp statistics
clear lldp
clear lldp statistics
restart lldp
dump protocols lldp
```

show lldp

Displays LLDP configuration information and neighboring device information.

Syntax

```
show lldp [port <port list>] [detail]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Displays LLDP information for the specified port.

For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

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.

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 18-1: Example of displaying the LLDP configuration information and neighboring device information in a simplified format

```
> show lldp
Date 2006/03/09 19:16:20 UTC
Status: Enabled Chassis ID: Type=MAC Info=0012.e268.2c21
Interval Time: 30 Hold Count: 4 TTL: 120
Port Counts=3
  1/1 (CH:10) Link: Up Neighbor Counts: 2
  1/2 Link: Down Neighbor Counts: 0
  1/3 Link: Down Neighbor Counts: 0
>
```

Display items in Example 1

Table 18-1: Items displayed for LLDP configuration information and neighboring device information in a simplified format

Item	Meaning	Displayed information
Status	Status of the LLDP functionality on the Switch	Enabled: The LLDP functionality is enabled. Disabled: The LLDP functionality is disabled.

Item	Meaning	Displayed 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	Information about the chassis ID	MAC address of the Switch
Interval Time	Interval for sending LDPDUs that has been set on the Switch (in seconds)	5 to 32768
Hold Count	Multiplier for Interval Time, used for calculating the LDPDU retention time to be reported to neighboring devices	2 to 10
TTL	LDPDU retention time to be reported to neighboring devices	10 to 65535
Port Counts	Number of ports	Number of ports that has been set for enable-port
<nif no.>/<port no.>	Port number	The NIF number and the port number of the port whose information is to be displayed
CH	Channel group number	This item is displayed if the applicable port belongs to the 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 device information items that is retained by the applicable port

Example 2

The following is an example of displaying LLDP information when the `detail` parameter is specified.

Figure 18-2: Example of displaying detailed LLDP configuration information and neighboring device information

```

> show lldp detail
Date 2006/03/09 19:16:34 UTC
Status: Enabled Chassis ID: Type=MAC Info=0012.e268.2c21
Interval Time: 30 Hold Count: 4 TTL: 120
System Name: LLDP1
System Description: ALAXALA AX6300S AX-6300-S04 [AX6304S] Switching software Ver. 10.2 [OS-SE]
Total Neighbor Counts=2
Port Counts=3
Port 1/1 (CH:10) Link: Up Neighbor Counts: 2
  Port ID: Type=MAC Info=0012.e298.5cc0
  Port Description: GigabitEthernet 1/1
  Tag ID: Tagged=1,10-20,4094
  IPv4 Address: Tagged: 10 192.168.248.240
  IPv6 Address: Tagged: 20 3ffe:501:811:ff01:200:8798:5cc0:e7f4
  1 TTL: 110 Chassis ID: Type=MAC Info=0012.e268.2505
    System Name: LLDP2
    System Description: ALAXALA AX6300S AX-6300-S04 [AX6304S] Switching software Ver. 10.2 [OS-SE]
    Port ID: Type=MAC Info=0012.e298.dc20
    Port Description: GigabitEthernet 1/5
    Tag ID: Tagged=1,10-20,4094
    IPv4 Address: Tagged: 10 192.168.248.220
    2 TTL: 100 Chassis ID: Type=MAC Info=0012.e268.2c2d
      System Name: LLDP3
      System Description: ALAXALA AX6300S AX-6300-S08 [AX6308S] Switching software Ver. 10.2 [OS-SE]

```

```

Port ID: Type=MAC          Info=0012.e298.7478
Port Description: GigabitEthernet 1/24
Tag ID: Tagged=1,10-20,4094
IPv4 Address: Tagged: 10    192.168.248.200
IPv6 Address: Tagged: 20    3ffe:501:811:ff01:200:8798:7478:e7f4
Port 1/2          Link: Down Neighbor Counts: 0
Port 1/3          Link: Down Neighbor Counts: 0
>

```

3

1. Information about the Switch's port
2. Information about neighboring devices
3. Information about neighboring devices

Display items in Example 2

Table 18-2: Items displayed for detailed LLDP configuration information and neighboring device information

Item	Meaning	Displayed information
Status	Status of the LLDP functionality on the Switch	Enabled: The LLDP functionality is enabled. Disabled: The LLDP functionality is disabled.
Chassis ID	Chassis ID of the Switch	--
Type	Subtype for the chassis ID	MAC: Indicates that a MAC address is displayed for Info.
Info	Information about the chassis ID	MAC address of the Switch
Interval Time	Interval for sending LDPDUs that has been set on the Switch (in seconds)	5 to 32768
Hold Count	Multiplier for Interval Time, used for calculating the LDPDU retention time to be reported to neighboring devices	2 to 10
TTL	LDPDU retention time to be reported to neighboring devices	10 to 65535
System Name	System name of the Switch	A character string set by using the <code>name</code> parameter of the <code>system</code> command. This item is not displayed if the information has not been set in the configuration.
System Description	System description of the Switch	The same character string as the string used for the MIB (<code>sysDescr</code>)
Total Neighbor Counts	Total number of neighboring devices connected to the Switch	Number of neighboring devices whose information is retained by the Switch. 0 to 192
Port Counts	Number of ports	Number of ports that has been set for enable-port
Port	Applicable port number	<nif no.> / <port no.>
CH	Channel group number	This item is displayed if the applicable port belongs to the 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.
Neighbor Counts	Number of neighboring devices	Number of neighboring device information items that is retained by the applicable port

Item	Meaning	Displayed information
Port ID	Port ID of the applicable port	--
Type	Subtype for the port ID	MAC: Indicates that a MAC address is displayed for Info.
Info	Information about the port ID	MAC address of the port
Port Description	Port description for the applicable port	The same character string as the string used for the MIB (ifDescr). GigabitEthernet: Indicates a 1 Gbit/s or slower Ethernet. TenGigabitEthernet: Indicates a 10 Gbit/s Ethernet.
Tag ID	List of VLANs to which the applicable port belongs	VLAN ID list This item is not displayed if the information has not been set in the configuration.
IPv4 Address	IP address of the applicable port (IPv4)	This item is not displayed if the information has not been set in the configuration.
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	IP address of the applicable port (IPv6)	This item is not displayed if the information has not been set in the configuration.
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.
TTL	Remaining LDPDU retention time (in seconds)	0 to 65535
Chassis ID	Chassis ID of the neighboring device	--
Type	Subtype for the chassis ID	CHAS-COMP: Indicates that entPhysicalAlias of the Entity MIB is displayed for Info. CHAS-IF: Indicates that ifAlias of the interface MIB is displayed for Info. PORT: Indicates that portEntPhysicalAlias of the Entity MIB is displayed for Info. BACK-COMP: Indicates that backplaneEntPhysicalAlias of the Entity MIB is displayed for Info. MAC: Indicates that macAddress of the LLDP MIB is displayed for Info. NET: Indicates that networkAddress of the LLDP MIB is displayed for Info. LOCL: Indicates that local of the LLDP MIB is displayed for Info.
Info	Information about the chassis ID	Information displayed for the subtype
System Name	System name of the neighboring device	This item is not displayed if it has not been reported.
System Description	System description of the neighboring device	This item is not displayed if it has not been reported.

Item	Meaning	Displayed information
Port ID	Port ID for the neighboring device	--
Type	Subtype for the port ID	PORT: Indicates that ifAlias of the InterfaceMIB is displayed for Info. ENTRY: Indicates that portEntPhysicalAlias of the Entity MIB is displayed for Info. BACK-COMP: Indicates that backplaneEntPhysicalAlias of the Entity MIB is displayed for Info. MAC: Indicates that macAddr of the LLDP MIB is displayed for Info. NET: Indicates that networkAddr of the LLDP MIB is displayed for Info. LOCL: Indicates that local of the LLDP MIB is displayed for Info.
Info	Information about the port ID	Information displayed for the subtype
Port Description	Port description of the neighboring device	This item is not displayed if it has not been reported.
Tag ID	List of 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.
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	IP address assigned to the neighboring device (IPv6)	This item is not displayed if it has not been reported.
Tagged	ID for the VLAN that has the IP address described in the previous item	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.

Impact on communication

None

Response messages

Table 18-3: List of response messages for the show lldp command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to LLDP program.	Communication with the LLDP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart lldp</code> command to restart the LLDP program.
LLDP is not configured.	LLDP has not been configured. Check the configuration.

Notes

None

show lldp statistics

Displays LLDP statistics.

Syntax

```
show lldp statistics [port <port list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Displays LLDP statistics for the specified ports in list format.

For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Displays statistics for all LLDP frames by port.

Example

Figure 18-3: Example of displaying LLDP statistics

```
> show lldp statistics
Date 2006/03/09 23:09:59 UTC
Port Counts: 3
Port 1/1   LDPDUs      : Tx   =      1300 Rx   =      1294 Invalid=      0
           Discard TLV: TLVs=      0 LDPDUs=      0
Port 1/2   LDPDUs      : Tx   =      890 Rx   =      547 Invalid=      0
           Discard TLV: TLVs=      0 LDPDUs=      0
Port 1/3   LDPDUs      : Tx   =      0 Rx   =      0 Invalid=      0
           Discard TLV: TLVs=      0 LDPDUs=      0
>
```

Display items

Table 18-4: Items displayed for LLDP statistics

Item	Meaning	Displayed information
Port counts	Number of ports subject to this statistics	--
Port	Port number	<nif no.> / <port no.>
LDPDUs	Statistics for frames	0 is displayed for the disabled ports.
Tx	Number of LDPDUs that have been sent	0 to 4294967295
Rx	Number of LDPDUs that have been received	0 to 4294967295
Invalid	Number of invalid LDPDUs	0 to 4294967295
Discard TLV	TLV statistics	0 is displayed for the disabled ports.
TLVs	Number of TLVs that have been discarded	0 to 4294967295
LDPDUs	Number of LDPDUs that contain discarded TLVs	0 to 4294967295

Impact on communication

None

Response messages*Table 18-5:* List of response messages for the show lldp statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to LLDP program.	Communication with the LLDP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart lldp</code> command to restart the LLDP program.
LLDP is not configured.	LLDP has not been configured. Check the configuration.

Notes

None

clear lldp

Clears LLDP neighboring device information.

Syntax

```
clear lldp [port <port list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Clears neighboring device information of the specified port.

For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Information about all neighboring devices retained on the Switch is cleared.

Example

Figure 18-4: Example of executing the clear lldp command

```
> clear lldp
>
```

Display items

None

Impact on communication

None

Response messages

Table 18-6: List of response messages for the clear lldp command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to LLDP program.	Communication with the LLDP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart lldp</code> command to restart the LLDP program.
LLDP is not configured.	LLDP has not been configured. Check the configuration.

Notes

None

clear lldp statistics

Clears LLDP statistics.

Syntax

```
clear lldp statistics [port <port list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Clears LLDP statistics for the specified port.

For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Clears all LLDP statistics for the Switch.

Example

Figure 18-5: Example of executing the clear lldp statistics command

```
> clear lldp statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 18-7: List of response messages for the clear lldp statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to LLDP program.	Communication with the LLDP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart lldp</code> command to restart the LLDP program.
LLDP is not configured.	LLDP has not been configured. Check the configuration.

Notes

None

restart lldp

Restarts the LLDP program.

Syntax

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

Input mode

User mode and administrator mode

Parameters

-f

Restarts the LLDP program without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file when the program is restarted.

Operation when this parameter is omitted:

A core file is not output.

Operation when all parameters are omitted:

Restarts the LLDP program after displaying a confirmation message.

Example

Figure 18-6: Example of restarting the LLDP program

```
> restart lldp
LLDP restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Response messages

Table 18-8: List of response messages for the restart lldp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
LLDP doesn't seem to be running.	This command failed because the LLDP program is not started. Wait until the LLDP program restarts, and then re-execute the command.

Notes

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

Storage directory: /usr/var/core/

Core file: lldpd.core

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

dump protocols lldp

Dumps detailed event trace information and control table information collected by the LLDP program to a file.

Syntax

```
dump protocols lldp
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 18-7: Example of specifying LLDP dump

```
> dump protocols lldp
>
```

Display items

None

Impact on communication

None

Response messages

Table 18-9: List of response messages for the dump protocols lldp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to LLDP program.	Communication with the LLDP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart lldp</code> command to restart the LLDP program.
File open error.	An attempt to open or access a dump file failed. Re-execute the command later.
LLDP is not configured.	LLDP has not been configured. Check the configuration.

Notes

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

Storage directory: `/usr/var/lldp/`

File: `lldpd_dump.gz`

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

Chapter

19. OADP

show oadp
show oadp statistics
clear oadp
clear oadp statistics
restart oadp
dump protocols oadp

show oadp

Displays OADP/CDP configuration information and neighboring device information.

Syntax

```
show oadp [port <port list>] [channel-group-number <channel group list>] [device-id <device id>] [detail]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Displays neighboring device information for the specified port.

For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

The neighboring device information for all ports is displayed.

channel-group-number <channel group list>

Displays neighboring device information for the specified channel group in list format.

For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

The neighboring device information for all channel groups is displayed.

device-id <device id>

Displays neighboring device information for the specified device ID.

Operation when this parameter is omitted:

All neighboring device information is displayed.

detail

Displays OADP/CDP configuration information for the Switch and neighboring device information in detail.

Operation when this parameter is omitted:

OADP/CDP configuration information for the Switch and neighboring device information are displayed in a simplified format.

Operation when all parameters are omitted:

OADP/CDP 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 OADP/CDP configuration information in a simplified format.

Figure 19-1: Example of displaying OADP configuration information and neighboring device information in a simplified format

```
> show oadp
Date 2006/03/09 19:50:20 UTC
OADP/CDP status: Enabled/Disabled   Device ID: OADP-1
```

```
Interval Time: 60   Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 1/1-5,16,20
CH 10
```

```
Total Neighbor Counts=2
```

Local	VID	Holdtime	Remote	VID	Device ID	Capability	Platform
1/1	0	35	1/8	0	OADP-2	RS	AX6304S
1/16	0	9	1/1	0	OADP-3	RS	AX6308S

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
```

```
>
```

```
> show oadp port 1/1
```

```
Date 2006/03/09 19:50:30 UTC
```

```
OADP/CDP status: Enabled/Disabled   Device ID: OADP-1
```

```
Interval Time: 60   Hold Time: 180
```

```
ignore vlan: 2-4,10
```

```
Enabled Port: 1/1-5,16,20
```

```
CH 10
```

```
Total Neighbor Counts=1
```

Local	VID	Holdtime	Remote	VID	Device ID	Capability	Platform
1/1	0	35	1/8	0	OADP-2	RS	AX6304S

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
```

```
>
```

```
> show oadp device-id OADP-3
```

```
Date 2006/03/09 19:50:40 UTC
```

```
OADP/CDP status: Enabled/Disabled   Device ID: OADP-1
```

```
Interval Time: 60   Hold Time: 180
```

```
ignore vlan: 2-4,10
```

```
Enabled Port: 1/1-5,16,20
```

```
CH 10
```

```
Total Neighbor Counts=1
```

Local	VID	Holdtime	Remote	VID	Device ID	Capability	Platform
1/16	0	9	1/1	0	OADP-3	RS	AX6308S

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
```

```
>
```

Display items in Example 1

Table 19-1: Items displayed for OADP configuration information and neighboring device information in a simplified format

Item	Meaning	Displayed information
OADP/CDP status	Status of the OADP/CDP functionality on the Switch	Enabled: The OADP/CDP functionality is enabled. Disabled: The OADP/CDP functionality is disabled. Paused: The OADP/CDP functionality is being paused.
Interval Time	Interval for sending OADP frames that has been set on the Switch (in seconds)	5 to 254
Hold Time	OADP frame retention time to be reported to neighboring devices (in seconds)	10 to 255

Item	Meaning	Displayed information
ignore vlan	VLANs that ignore OADP PDUs	VLAN ID list
Enabled Port	Information about ports where the OADP functionality is enabled on the Switch	NIF number/port number, channel group number
Total Neighbor Counts	Number of neighboring devices whose information is retained by the Switch.	0 to 250
Local	Received port number	NIF number/port number, channel group number
VID	VLAN ID of the IEEE802.1Q VLAN Tag attached to the receive frame	VLAN ID
Holdtime	Remaining retention time for neighboring device information (in seconds)	OADP: 0 to 255 CDP: Time set for a Cisco switch on the sending side
Remote	Port number sent from a neighboring device	NIF number/port number, channel group number
VID	VLAN ID set for the VLAN ID TLV sent from a neighboring device	VLAN ID
Device ID	Device ID of the neighboring device	Device identifier
Capability	Functionality of neighboring devices	R: Indicates a router. T: Indicates a transparent bridge. B: Indicates a source-route bridge. S: Indicates a switch. H: Indicates a host. I: Indicates that no IGMP reports are sent. r: Indicates a repeater.
Platform	Name of the neighboring device	Device name

Example 2

The following figure is an example of displaying OADP information when the `detail` parameter is specified.

Figure 19-2: Example of displaying detailed OADP configuration information and neighboring device information

```

> show oadp detail
Date 2006/03/09 19:55:52 UTC
OADP/CDP status: Enabled/Disabled   Device ID: OADP-1
Interval Time: 60   Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 1/1-5,16,20
Total Neighbor Counts=2
-----
Port: 1/1      VLAN ID: 0
Holdtime      : 6(sec)
Port ID       : 1/8   VLAN ID(TLV): 0
Device ID     : OADP-2
Capabilities   : Router,Switch
Platform      : AX6304S
Entry address(es):
  IP address   : 192.16.170.87
  IPv6 address: fe80::200:4cff:fe71:5d1c
IfSpeed       : 1G    Duplex   : FULL
Version       : ALAXALA AX6300S AX-6300-S04 [AX6304S] Switching soft
ware Ver. 10.2 [OS-SE]

```



```

-----
Port: 1/16      VLAN ID: 0
Holdtime       : 10(sec)
Port ID        : 1/1  VLAN ID(TLV): 0
Device ID      : OADP-3
Capabilities    : Router,Switch
Platform       : AX6308S
Entry address(es):
    IP address  : 192.16.170.100
IfSpeed        : 1G   Duplex      : FULL
Version        : ALAXALA AX6300S AX-6300-S08 [AX6308S] Switching software Ver. 10.2 [OS-SE]
-----
>

```

1. Configuration information of the Switch
2. Information about the Switch's port
3. Information about neighboring devices

Display items in Example 2

Table 19-2: Items displayed for detailed OADP configuration information and neighboring device information

Item	Meaning	Displayed information
OADP/CDP status	Status of the OADP/CDP functionality on the Switch	Enabled: The OADP/CDP functionality is enabled. Disabled: The OADP/CDP functionality is disabled. Paused: The OADP/CDP functionality is being paused.
Interval Time	Interval for sending OADP frames that has been set on the Switch (in seconds)	5 to 254
Hold Time	OADP frame retention time to be reported to neighboring devices (in seconds)	10 to 255
ignore vlan	VLANs that ignore OADP PDUs	VLAN ID list
Enabled Port	Information about ports where the OADP functionality is enabled on the Switch	NIF number/port number, channel group number
Total Neighbor Counts	Number of neighboring devices whose information is retained by the Switch.	0 to 250
Port	Received port number	NIF number/port number, channel group number
VLAN ID	VLAN ID of the IEEE802.1Q VLAN Tag attached to the receive frame	VLAN ID
Holdtime	Remaining retention time for neighboring device information (in seconds)	OADP: 0 to 255 CDP: Time set for a Cisco switch on the sending side
Port ID	Port number sent from a neighboring device	NIF number/port number, channel group number

Item	Meaning	Displayed information
VLAN ID(TLV)	VLAN ID set for the VLAN ID TLV sent from a neighboring device	VLAN ID
Device ID	Device ID of the neighboring device	Device identifier
Capability	Functionality of neighboring devices	Functionality
Platform	Name of the neighboring device	Device name
Entry address	Addresses related to ports sent from neighboring devices	IPv4 address, IPv6 address
ifSpeed	Line speed of a port sent from a neighboring device	Example: 10M: 10Mbit/s, 1G: 1Gbit/s
Duplex	Duplex information for a port sent from a neighboring device	FULL or HALF
Version	Version information about neighboring devices	Version information

Impact on communication

None

Response messages

Table 19-3: List of response messages for the show oadp command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to OADP.	Communication with the OADP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart oadp</code> command to restart the OADP program.
OADP is not configured.	OADP has not been configured. Check the configuration.

Notes

None

show oadp statistics

Displays OADP/CDP statistics.

Syntax

```
show oadp statistics [port <port list>] [channel-group-number <channel group list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Displays the OADP statistics for the specified ports in list format.

For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

OADP statistics for all ports are displayed.

channel-group-number <channel group list>

Displays OADP statistics for the specified channel group numbers in list format.

For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

OADP statistics for all channel groups are displayed.

Operation when all parameters are omitted:

Statistics for all OADP/CDP frames are displayed by port.

Example

Figure 19-3: Example of displaying OADP/CDP statistics

```
> show oadp statistics
Date 2006/03/09 23:12:23 UTC
Port Counts: 3
Port 1/6   OADP PDUs   : Tx   =          9 OADP/CDP PDUs   : Rx   =          14
           RX PDUs    : OADP=          6 CDPv1 =          0 CDPv2 =          8
           Discard/ERR: Head=          0 cksum =          0 capacity=          0
Port 1/7   OADP PDUs   : Tx   =         10 OADP/CDP PDUs   : Rx   =          18
           RX PDUs    : OADP=          9 CDPv1 =          0 CDPv2 =          9
           Discard/ERR: Head=          0 cksum =          0 capacity=          0
Port 1/8   OADP PDUs   : Tx   =          0 OADP/CDP PDUs   : Rx   =          0
           RX PDUs    : OADP=          0 CDPv1 =          0 CDPv2 =          0
           Discard/ERR: Head=          0 cksum =          0 capacity=          0
>
```

Display items

Table 19-4: Items displayed for OADP/CDP statistics

Item	Meaning	Displayed information
Port counts	Number of ports subject to this statistics	--
Port	Port number	The NIF number and the port number of the port whose information is to be displayed

Item	Meaning	Displayed information
OADP PDUs Tx	Number of sent OADP PDUs	0 to 4294967295
OADP/CDP PDUs Rx	Number of received OADP/CDP PDUs	0 to 4294967295
Rx PDUs	Statistics for receive frames	--
OADP	Number of OADP PDUs	0 to 4294967295
CDPv1	Number of CDP version 1 PDUs	0 to 4294967295
CDPv2	Number of CDP version 2 PDUs	0 to 4294967295
Discard/ERR	Statistics for error frames	--
Head	Number of header error PDUs	0 to 4294967295
cksum	Number of checksum error PDUs	0 to 4294967295
capacity	Number of PDUs exceeding the accommodation limit	0 to 4294967295

Impact on communication

None

Response messages

Table 19-5: List of response messages for the show oadp statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to OADP.	Communication with the OADP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart oadp</code> command to restart the OADP program.
OADP is not configured.	OADP has not been configured. Check the configuration.

Notes

None

clear oadp

Clears OADP neighboring device information.

Syntax

```
clear oadp [port <port list>] [channel-group-number <channel group list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Clears neighboring device information of the specified port.

For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Clears neighboring device information for all ports.

channel-group-number <channel group list>

Clears neighboring device information for the specified channel group number in list format.

For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

The neighboring device information for all channel group numbers is cleared.

Operation when all parameters are omitted:

Information about all neighboring devices retained on the Switch is cleared.

Example

Figure 19-4: Example of executing the clear oadp command

```
> clear oadp
>
```

Display items

None

Impact on communication

None

Response messages

Table 19-6: List of response messages for the clear oadp command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to OADP.	Communication with the OADP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart oadp</code> command to restart the OADP program.

Message	Description
OADP is not configured.	OADP has not been configured. Check the configuration.

Notes

None

clear oadp statistics

Clears OADP/CDP statistics.

Syntax

```
clear oadp statistics [port <port list>] [channel-group-number <channel group list>]
```

Input mode

User mode and administrator mode

Parameters

port <port list>

Clears OADP/CDP statistics for the specified port.

For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

OADP/CDP statistics for all ports are cleared.

channel-group-number <channel group list>

Clears OADP/CDP statistics for the specified channel group numbers in list format.

For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

OADP/CDP statistics for all channel groups are cleared.

Operation when all parameters are omitted:

All OADP/CDP statistics for the Switch are cleared.

Example

Figure 19-5: Example of executing the clear oadp statistics command

```
> clear oadp statistics
>
```

Display items

None

Impact on communication

None

Response messages

Table 19-7: List of response messages for the clear oadp statistics command

Message	Description
Can't execute this command in standby system.	This command cannot be executed on a standby system.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to OADP.	Communication with the OADP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart oadp</code> command to restart the OADP program.

Message	Description
OADP is not configured.	OADP has not been configured. Check the configuration.

Notes

None

restart oadp

Restarts the OADP program.

Syntax

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

Input mode

User mode and administrator mode

Parameters

-f

Restarts the OADP program without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the core file when the program is restarted.

Operation when this parameter is omitted:

A core file is not output.

Operation when all parameters are omitted:

Restarts the OADP program after displaying a confirmation message.

Example

Figure 19-6: Example of restarting the OADP program

```
> restart oadp
OADP restart OK? (y/n): y
>
```

Display items

None

Impact on communication

None

Response messages

Table 19-8: List of response messages for the restart oadp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
OADP doesn't seem to be running.	This command failed because the OADP program is not started. Wait until the OADP program restarts, and then re-execute the command.

Notes

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

Storage directory: /usr/var/core/

Core file: `oadpd.core`

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

dump protocols oadp

Dumps detailed event trace information and control table information collected by the OADP program to a file.

Syntax

```
dump protocols oadp
```

Input mode

User mode and administrator mode

Parameters

None

Example

Figure 19-7: Example of specifying OADP dump

```
> dump protocols oadp
>
```

Display items

None

Impact on communication

None

Response messages

Table 19-9: List of response messages for the dump protocols oadp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to OADP.	Communication with the OADP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart oadp</code> command to restart the OADP program.
File open error.	An attempt to open or access a dump file failed. Re-execute the command later.
OADP is not configured.	OADP has not been configured. Check the configuration.

Notes

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

Storage directory: `/usr/var/oadp/`

File: `oadpd_dump.gz`

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

Index

A

activate standby 282

C

clear access-filter 16
clear access-log 22
clear access-log flow 28
clear cfm fault 423
clear cfm l2traceroute-db 425
clear cfm remote-mep 421
clear cfm statistics 426
clear dot1x auth-state 114
clear dot1x logging 131
clear dot1x statistics 112
clear efmoam statistics 370
clear fense logging 244
clear fense statistics 243
clear gsrp 304
clear gsrp forced-shift 311
clear gsrp port-up-delay 309
clear ip arp inspection statistics 260
clear ip dhcp snooping binding 253
clear ip dhcp snooping logging 274
clear ip dhcp snooping statistics 257
clear lldp 484
clear lldp statistics 485
clear loop-detection logging 386
clear loop-detection statistics 384
clear mac-authentication auth-state 208
clear mac-authentication logging 210
clear mac-authentication statistics 211
clear oadp 497
clear oadp statistics 499
clear qos queueing 55
clear qos queueing distribution 65
clear qos queueing interface 72
clear qos queueing to-cpu 79
clear qos-flow 42
clear sflow statistics 471
clear shaper 87
clear shaper <port list> 94
clear vrrpstatus (IPv4) 331
clear vrrpstatus (IPv6) 349
clear web-authentication auth-state 175
clear web-authentication html-files 183
clear web-authentication logging 167
clear web-authentication statistics 168
command description format 2
commit mac-authentication 216
commit web-authentication 169

D

debug access-log 32
dump access-log 29
dump protocols cfm 430
dump protocols dhcp snooping 277
dump protocols dot1x 121
dump protocols efmoam 373
dump protocols gsrp 315
dump protocols lldp 488
dump protocols loop-detection 389
dump protocols mac-authentication 225
dump protocols oadp 503
dump protocols vaa 247
dump protocols web-authentication 179
dump sflow 473

I

inactivate standby 280

L

l2ping 392
l2traceroute 395
load mac-authentication 222
load web-authentication 173

N

no debug access-log 34

R

reauthenticate dot1x 117
redundancy force-switchover 283
remove mac-authentication mac-address 214
remove web-authentication user 139
restart access-log 30
restart cfm 428
restart dhcp snooping 275
restart dot1x 119
restart efmoam 371
restart gsrp 313
restart lldp 486
restart loop-detection 387
restart mac-authentication 224
restart oadp 501
restart sflow 472
restart vaa 245
restart web-authentication 177

S

set gsrp master 307

set mac-authentication mac-address 212
set web-authentication html-files 180
set web-authentication passwd 136
set web-authentication user 134
set web-authentication vlan 138
show access-filter 10
show access-log 20
show access-log flow 23
show cfm 398
show cfm fault 408
show cfm l2traceroute-db 411
show cfm remote-mep 402
show cfm statistics 416
show dot1x 103
show dot1x logging 122
show dot1x statistics 98
show efmoam 364
show efmoam statistics 367
show fense logging 240
show fense server 228
show fense statistics 233
show gsrp 290
show gsrp aware 302
show ip arp inspection statistics 258
show ip dhcp snooping binding 250
show ip dhcp snooping logging 261
show ip dhcp snooping statistics 255
show lldp 476
show lldp statistics 482
show loop-detection 376
show loop-detection logging 382
show loop-detection statistics 379
show mac-authentication 203
show mac-authentication logging 190
show mac-authentication login 188
show mac-authentication mac-address 218
show mac-authentication statistics 206
show oadp 490
show oadp statistics 495
show qos queueing 44
show qos queueing distribution 57
show qos queueing interface 68
show qos queueing to-cpu 74
show qos-flow 36
show sflow 468
show shaper 81
show shaper <port list> 88
show snmp 432
show snmp pending 437
show track (IPv4) 354
show track (IPv6) 358
show vrrpstatus (IPv4) 318
show vrrpstatus (IPv6) 336
show web-authentication 160
show web-authentication html-files 184
show web-authentication logging 145
show web-authentication login 143
show web-authentication statistics 164
show web-authentication user 141
snmp get 440
snmp getarp 451
snmp getforward 453
snmp getif 446
snmp getnext 442
snmp getroute 448
snmp lookup 439
snmp rget 456
snmp rgetarp 465
snmp rgetnext 458
snmp rgetroute 462
snmp rwalk 460
snmp walk 444
store mac-authentication 220
store web-authentication 171
swap vrrp (IPv4) 333
swap vrrp (IPv6) 351
synchronize 285