

---

*AX3800S/AX3650S Software Manual*

**Operation Command Reference Vol.1**  
**For Version 11.10**

AX38S-S006X-40

**Alaxala**

## ■ Relevant products

This manual applies to the models in the AX3800S and AX3650S series of switches. It also describes the functionality of version 11.10 of the software. The described functionality is that supported by the software OS-L3SA-A/OS-L3SA and OS-L3SL-A/OS-L3SL, and by 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.

RSA and RSA SecurID are trademarks or registered trademarks of RSA Security Inc. in the United States and other countries.

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

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

VitalQIP and VitalQIP Registration Manager are trademarks of Alcatel-Lucent.

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

December 2012 (Edition 5) AX38S-S006X-40

## ■ Copyright

All Rights Reserved, Copyright(C), 2011, 2012, ALAXALA Networks, Corp.

## History of Amendments

[For version 11.10]

### Summary of amendments

Location and title	Changes
5 Stack	<ul style="list-style-type: none"><li>Stack was supported by AX3800S series switches.</li></ul>

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

[For version 11.9]

### Summary of amendments

Item	Changes
Stack	<ul style="list-style-type: none"><li>The execution example and items displayed by the <code>show switch</code> command were changed.</li></ul>
Checking software versions and device statuses	<ul style="list-style-type: none"><li>The items displayed by the <code>show version</code> command were changed.</li></ul>
Ethernet	<ul style="list-style-type: none"><li>The <code>show interfaces</code> (40GBASE-R) command was added.</li><li>A description related to QSFP+ was added.</li></ul>

[For version 11.8]

The section *Operation when a stack configuration is used* was added to all command descriptions.

### Summary of amendments

Item	Changes
Stack	<ul style="list-style-type: none"><li>This chapter was added.</li></ul>

[For version 11.7]

### Summary of amendments

Item	Changes
Checking software versions and device statuses	<ul style="list-style-type: none"><li>The items displayed by the <code>show version</code> command were changed.</li><li>The execution example and items displayed by the <code>show system</code> command were changed.</li><li>The execution example and items displayed by the <code>show environment</code> command were changed.</li></ul>
SNMP	<ul style="list-style-type: none"><li>The following commands were added: <code>show snmp</code> <code>show snmp pending</code></li></ul>

[For version 11.6]

This manual contains descriptions of the AX3650S series switches that were in the *AX3600S Software Manual for Ver. 11.5*.

### Summary of amendments

Item	Changes
Terminals and remote operations	<ul style="list-style-type: none"><li>A parameter was added to the <code>tftp</code> command.</li></ul>
Checking software versions and device statuses	<ul style="list-style-type: none"><li>A description about AX3800S series switches was added to the displayed detailed information of <code>Current selected unicast multipath number</code> for the <code>show system</code> command.</li></ul>

Item	Changes
Ethernet	<ul style="list-style-type: none"><li>• The execution example and items displayed by the <code>show interfaces</code> command were changed.</li></ul>

---

# Preface

---

## Applicable products and software versions

This manual applies to the models in the AX3800S and AX3650S series of switches. It also describes the functionality of version 11.10 of the software. The described functionality is that supported by the software OS-L3SA-A/OS-L3SA and OS-L3SL-A/OS-L3SL, and by 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 the functions applicable to both the AX3800S and AX3650S series of switches, and functionalities common to each software package. For functionalities that are not common to both AX3800S and AX3650S series switches, and functionalities not common to OS-L3SA-A/OS-L3SA and OS-L3SL-A/OS-L3SL are indicated as follows:

[AX3800S]:

The description applies to AX3800S switches.

[AX3650S]:

The description applies to AX3650S switches.

[OS-L3SA]:

The description applies to OS-L3SA-A/OS-L3SA for the AX3800S and AX3650S series of switches.

The functions supported by optional licenses are indicated as follows:

[OP-DH6R]:

The description applies to the OP-DH6R optional license.

[OP-OTP]:

The description applies to the OP-OTP 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**

Quick Start Guide  
(AX36S-Q001X)

- **Determining the hardware installation conditions and how to handle the hardware**

Hardware Instruction Manual  
(AX36S-H001X)

- **Understanding the software functions, configuration settings, and use of the operation commands**

Configuration Guide  
Vol.1  
(AX38S-S001X)  
Vol.2  
(AX38S-S002X)  
Vol.3  
(AX38S-S003X)

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

Configuration  
Command Reference  
Vol. 1  
(AX38S-S004X)  
Vol.2  
(AX38S-S005X)

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

Operation Command Reference  
Vol. 1  
(AX38S-S006X)  
Vol.2  
(AX38S-S007X)

- **Understanding messages and logs**

Message and Log Reference  
(AX38S-S008X)

- **Understanding the MIB**

MIB Reference  
(AX38S-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:

AX3800S series switch

AX3650S 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
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second (can also appear as bps)
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4

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

RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SElector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SFP+	Enhanced Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
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
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 1024<sup>2</sup> bytes. 1 GB (gigabyte) is 1024<sup>3</sup> bytes. 1 TB (terabyte) is 1024<sup>4</sup> bytes.



---

# Contents

---

<b>Preface</b>	<b>i</b>
Applicable products and software versions .....	i
Corrections to the manual .....	i
Intended readers .....	i
Manual URL .....	i
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**

<b>1. Reading the Manual</b>	<b>1</b>
Command description format .....	2
Specifiable values for parameters .....	4
List of character codes .....	7
Error messages displayed by the entry-error location detection functionality .....	8

## **PART 2: Basic Operation**

<b>2. Switching the Command Input Mode</b>	<b>9</b>
enable .....	10
disable .....	11
quit .....	12
exit .....	13
logout .....	14
configure (configure terminal) .....	15
<b>3. Terminals and Remote Operations</b>	<b>17</b>
set exec-timeout .....	18
set terminal help .....	20
set terminal pager .....	22
show history .....	24
telnet .....	25
ftp .....	28
tftp .....	34
<b>4. Configurations and File Operations</b>	<b>39</b>
show running-config (show configuration) .....	40
show startup-config .....	41
copy .....	42
erase configuration .....	45
show file .....	46
cd .....	49
pwd .....	50
ls .....	51
dir .....	53
cat .....	56
cp .....	57

mkdir .....	60
mv .....	62
rm .....	64
rmdir .....	66
delete .....	68
undelete .....	70
squeeze .....	72
zmodem .....	74
<b>5. Stack</b> .....	<b>77</b>
remote command .....	78
show switch .....	81
set switch .....	84
dump stack .....	85
<b>6. Login Security and RADIUS or TACACS+</b> .....	<b>87</b>
adduser .....	88
rmuser .....	91
password .....	93
clear password .....	95
show sessions (who) .....	97
show whoami (who am i) .....	99
killuser .....	102
show accounting .....	104
clear accounting .....	108
restart accounting .....	109
dump protocols accounting .....	111
<b>7. Time Settings and NTP</b> .....	<b>113</b>
show clock .....	114
set clock .....	115
show ntp associations .....	117
restart ntp .....	120
<b>8. Utilities</b> .....	<b>121</b>
diff .....	122
grep .....	124
more .....	125
less .....	126
tail .....	127
hexdump .....	128

## PART 3: Operating Devices

<b>9. Checking Software Versions and Device Statuses</b> .....	<b>129</b>
show version .....	130
show system .....	134
clear control-counter .....	147
show environment .....	148
reload .....	154
show tech-support .....	156
show tcpdump (tcpdump) .....	161
backup .....	173
restore .....	176

<b>10. Power Saving Functionality</b>	179
show power-control schedule .....	180
show power .....	182
clear power .....	184
set power-control schedule .....	185
show power-control port .....	186
<b>11. Checking Internal Memory and Memory Cards</b>	189
show mc .....	190
format mc .....	192
show flash .....	194
<b>12. Log</b>	197
show logging .....	198
clear logging .....	200
show logging console .....	201
set logging console .....	202
<b>13. Software Management</b>	203
ppupdate .....	204
set license .....	207
show license .....	209
erase license .....	210
<b>14. Resource Information</b>	211
show cpu .....	212
show processes .....	215
show memory .....	218
df .....	220
du .....	221
<b>15. Dump Information</b>	223
erase dumpfile .....	224
show dumpfile .....	225
 <b>PART 4: Network Interfaces</b>	
<b>16. Ethernet</b>	227
show interfaces (10BASE-T/100BASE-TX/1000BASE-T) .....	228
show interfaces (100BASE-FX) [AX3650S] .....	243
show interfaces (1000BASE-X) .....	251
show interfaces (10GBASE-R) .....	267
show interfaces (40GBASE-R) [AX3800S] .....	275
clear counters .....	283
show port .....	285
activate .....	303
inactivate .....	305
test interfaces .....	307
no test interfaces .....	311
<b>17. Link Aggregation</b>	315
show channel-group .....	316
show channel-group statistics .....	327
clear channel-group statistics lacp .....	335

restart link-aggregation .....	337
dump protocols link-aggregation .....	339

## PART 5: Layer 2 Switching

<b>18. MAC Address Table</b> .....	341
show mac-address-table .....	342
clear mac-address-table .....	346
<b>19. VLAN</b> .....	349
show vlan .....	350
show vlan mac-vlan .....	363
restart vlan .....	366
dump protocols vlan .....	368
<b>20. Spanning Tree Protocols</b> .....	369
show spanning-tree .....	370
show spanning-tree statistics .....	397
clear spanning-tree statistics .....	404
clear spanning-tree detected-protocol .....	406
show spanning-tree port-count .....	408
restart spanning-tree .....	411
dump protocols spanning-tree .....	413
<b>21. Ring Protocol</b> .....	415
show axrp .....	416
clear axrp .....	423
clear axrp preempt-delay .....	425
restart axrp .....	427
dump protocols axrp .....	429
<b>22. IGMP/MLD Snooping</b> .....	431
show igmp-snooping .....	432
clear igmp-snooping .....	438
show mld-snooping .....	440
clear mld-snooping .....	446
restart snooping .....	448
dump protocols snooping .....	450

## PART 6: Filters

<b>23. Filters</b> .....	453
show access-filter .....	454
clear access-filter .....	459

## PART 7: QoS

<b>24. QoS</b> .....	461
show qos-flow .....	462
clear qos-flow .....	466
show qos queueing .....	468
clear qos queueing .....	476

## **PART 8: Layer 2 Authentication**

<b>25. IEEE 802.1X</b>	<b>479</b>
show dot1x statistics .....	480
show dot1x .....	485
clear dot1x statistics .....	495
clear dot1x auth-state .....	497
reauthenticate dot1x .....	500
restart dot1x .....	502
dump protocols dot1x .....	504
show dot1x logging .....	506
clear dot1x logging .....	516
<b>26. Web Authentication</b>	<b>517</b>
set web-authentication user .....	518
set web-authentication passwd .....	520
set web-authentication vlan .....	522
remove web-authentication user .....	524
show web-authentication user .....	526
show web-authentication login .....	528
show web-authentication logging .....	530
show web-authentication .....	546
show web-authentication statistics .....	551
clear web-authentication logging .....	554
clear web-authentication statistics .....	555
commit web-authentication .....	556
store web-authentication .....	558
load web-authentication .....	560
clear web-authentication auth-state .....	562
restart web-authentication .....	564
dump protocols web-authentication .....	566
set web-authentication html-files .....	567
clear web-authentication html-files .....	570
show web-authentication html-files .....	571
clear web-authentication dead-interval-timer .....	573
<b>27. MAC-based Authentication</b>	<b>575</b>
show mac-authentication login .....	576
show mac-authentication logging .....	578
show mac-authentication .....	591
show mac-authentication statistics .....	595
clear mac-authentication auth-state .....	598
clear mac-authentication logging .....	600
clear mac-authentication statistics .....	601
set mac-authentication mac-address .....	602
remove mac-authentication mac-address .....	604
commit mac-authentication .....	606
show mac-authentication mac-address .....	608
store mac-authentication .....	610
load mac-authentication .....	612
restart mac-authentication .....	614
dump protocols mac-authentication .....	616
clear mac-authentication dead-interval-timer .....	617
<b>28. Authentication VLANs [OP-VAA]</b>	<b>619</b>
show fense server [OP-VAA] .....	620

show fense statistics [OP-VAA] .....	625
show fense logging [OP-VAA] .....	632
clear fense statistics [OP-VAA] .....	635
clear fense logging [OP-VAA] .....	637
restart vaa [OP-VAA] .....	638
dump protocols vaa [OP-VAA] .....	640

## **PART 9: Security**

### **29. DHCP Snooping** 641

show ip dhcp snooping binding .....	642
clear ip dhcp snooping binding .....	645
show ip dhcp snooping statistics .....	647
clear ip dhcp snooping statistics .....	649
show ip arp inspection statistics .....	650
clear ip arp inspection statistics .....	652
show ip dhcp snooping logging .....	653
clear ip dhcp snooping logging .....	666
restart dhcp snooping .....	667
dump protocols dhcp snooping .....	669

## **PART 10: High Reliability Based on Redundant Configurations**

### **30. GSRP** 671

show gsrp .....	672
show gsrp aware .....	684
clear gsrp .....	686
set gsrp master .....	689
clear gsrp port-up-delay .....	691
clear gsrp forced-shift .....	693
restart gsrp .....	695
dump protocols gsrp .....	697

### **31. VRRP** 699

show vrrpstatus (IPv4) .....	700
clear vrrpstatus (IPv4) .....	710
swap vrrp (IPv4) .....	712
show vrrpstatus (IPv6) .....	715
clear vrrpstatus (IPv6) .....	724
swap vrrp (IPv6) .....	726
show track (IPv4) .....	729
show track (IPv6) .....	733

### **32. Uplink Redundancy** 737

show switchport-backup .....	738
set switchport-backup active .....	743
restart uplink-redundant .....	745
dump protocols uplink-redundant .....	747
show switchport-backup statistics .....	748
clear switchport-backup statistics .....	750

## **PART 11: High Reliability Based on Network Failure Detection**

<b>33. IEEE 802.3ah/UDLD</b>	<b>753</b>
show efmoam .....	754
show efmoam statistics .....	757
clear efmoam statistics .....	760
restart efmoam .....	761
dump protocols efmoam .....	763
<b>34. L2 Loop Detection</b>	<b>765</b>
show loop-detection .....	766
show loop-detection statistics .....	769
show loop-detection logging .....	772
clear loop-detection statistics .....	774
clear loop-detection logging .....	776
restart loop-detection .....	777
dump protocols loop-detection .....	779
<b>35. CFM</b>	<b>781</b>
l2ping .....	782
l2traceroute .....	785
show cfm .....	788
show cfm remote-mep .....	793
show cfm fault .....	799
show cfm l2traceroute-db .....	802
show cfm statistics .....	807
clear cfm remote-mep .....	811
clear cfm fault .....	813
clear cfm l2traceroute-db .....	815
clear cfm statistics .....	816
restart cfm .....	818
dump protocols cfm .....	820

## **PART 12: Remote Network Management**

<b>36. SNMP</b>	<b>821</b>
show snmp .....	822
show snmp pending .....	827
snmp lookup .....	829
snmp get .....	830
snmp getnext .....	832
snmp walk .....	834
snmp getif .....	836
snmp getroute .....	839
snmp getarp .....	842
snmp getforward .....	844
snmp rget .....	847
snmp rgetnext .....	849
snmp rwalk .....	851
snmp rgetroute .....	853
snmp rgetarp .....	856
<b>37. sFlow</b>	<b>859</b>
show sflow .....	860
clear sflow statistics .....	863

restart sflow .....	864
dump sflow .....	866

## **PART 13: Management of Neighboring Device Information**

### **38. LLDP** 867

show lldp .....	868
show lldp statistics .....	874
clear lldp .....	876
clear lldp statistics .....	877
restart lldp .....	878
dump protocols lldp .....	880

### **39. OADP** 881

show oadp .....	882
show oadp statistics .....	887
clear oadp .....	889
clear oadp statistics .....	891
restart oadp .....	893
dump protocols oadp .....	895

### **Appendix** 897

A List of operation commands supported by the remote command command .....	898
--	-----

### **Index** 901

## **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*.

### Operation when a stack configuration is used

Describes the functionality of the command used in a stack configuration for member switches other than the master switch. This section describes the format for entering an operation command when the operation command is executed for a member switch other than the master switch and the `remote command` command is used to execute the operation command. For details on the input mode and general notes on the `remote command` command, see the description for the `remote command` command.

### Example

Provides examples of appropriate command usage.

### Display items

Describes the display items generated by the example.

The following table describes the 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 <i>timezone</i> 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 <i>&lt;interface name&gt;</i>
interface gigabitethernet	geth1/0/1 The numeric values represent <i>&lt;switch no.&gt;/&lt;nif no.&gt;/&lt;port no.&gt;</i> .
interface tengigabitethernet	tengeth1/0/24 The numeric values represent <i>&lt;switch no.&gt;/&lt;nif no.&gt;/&lt;port no.&gt;</i> .
interface fortygigabitethernet [AX3800S]	ftygeth1/0/52 The numeric values represent <i>&lt;switch no.&gt;/&lt;nif no.&gt;/&lt;port no.&gt;</i> .
interface vlan <i>&lt;vlan id&gt;</i>	VLAN0002 The last four digits represent <i>&lt;vlan id&gt;</i> .
interface loopback 0	loopback0
interface null 0	null0

## 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
IPv6 address	Specify this item in hexadecimal format, separating 2-byte hexadecimal values by colons (:).	3ffe:501:811:ff03::87ff:fed0:c7e0 fe80::200:87ff:fe5a:13c7
IPv6 address with an interface name (for a link-local address only)	Specify a percent (%) between an IPv6 address and an interface name. Only link-local IPv6 addresses can be used as this parameter type.	fe80::200:87ff:fe5a:13c7%VLAN0001

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

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

Table 1-4: Range of <switch no.>, <nif no.> and <port no.> values for AX3830S series switches (for commands applicable to a stack configuration) [AX3800S]

Model	Range of values		
	<switch no.>	<nif no.>	<port no.>
AX3830S-44XW	1 to 2	0	1 to 48
AX3830S-44X4QW			1 to 52

Table 1-5: Range of <nif no.> and <port no.> values for AX3830S series switches (for commands not applicable to a stack configuration) [AX3800S]

Model	Range of values	
	<nif no.>	<port no.>
AX3830S-44XW	0	1 to 48
AX3830S-44X4QW		1 to 52

Table 1-6: Range of <switch no.>, <nif no.> and <port no.> values for AX3650S series switches (for commands applicable to a stack configuration) [AX3650S]

Model	Range of values		
	<switch no.>	<nif no.>	<port no.>
AX3650S-24T6XW AX3650S-20S6XW	1 to 2	0	1 to 30
AX3650S-48T4XW			1 to 52

Table 1-7: Range of <nif no.> and <port no.> values for AX3650S series switches (for commands not applicable to a stack configuration) [AX3650S]

Model	Range of values	
	<nif no.>	<port no.>
AX3650S-24T6XW AX3650S-20S6XW	0	1 to 30
AX3650S-48T4XW		1 to 52

## 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 <switch no.>/<nif no.>/<port no.> format to specify multiple ports. You can also specify one port, as when <switch no.>/<nif no.>/<port no.> is written as the parameter input format. The range of permitted values is the same as the range of <switch no.>, <nif no.> and <port no.> values in the above tables.

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

For a command applicable to a stack configuration:

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

For a command not applicable to a stack configuration:

0/1-3,5

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

For a command applicable to a stack configuration:

1/\*/\*: Specify all ports on a switch. Note that an asterisk (\*) cannot be specified in a switch number.

For a command not applicable to a stack configuration:

\*/\*: Specify all ports on a switch

## 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 1-8:* 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 11.10*).

Table 1-9: 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	A parameter entered at '^' is an invalid format.	When the input format of the parameter is invalid
11	% Permission denied	This command cannot be executed in user mode.	When a command that can be executed only in administrator mode is executed in user mode.
12	% internal program error	A program is faulty. Contact maintenance personnel.	When an invalid action other than described above occurs
13	% Command not authorized.	The executed command is not authorized.	When the executed command is not authorized by the RADIUS/TACACS+ server via RADIUS/TACACS+ command authorization
14	% illegal parameter at '<word>' word	An invalid character '<word>' is entered. <word>: Invalid word	When '<word>' is entered at positions where a character cannot be entered
15	% illegal switch number at '^' marker	An invalid switch number is entered at '^'.	When an invalid switch number is entered

## Chapter

---

# 2. Switching the Command Input Mode

---

enable  
disable  
quit  
exit  
logout  
configure (configure terminal)

---

## enable

---

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

### Syntax

`enable`

### Input mode

User mode

### Parameters

None

### Operation when a stack configuration is used

The command can be executed only on the master switch.

### Example

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

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

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

### Display items

None

### Impact on communication

None

### Response messages

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

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Login timed out after 60 seconds.	A timeout occurred because no password was entered within 60 seconds.
Sorry	The mode cannot be changed to administrator mode because a password entry error occurred.

### Notes

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

---

## disable

---

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

### Syntax

disable

### Input mode

Administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

### Example

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

```
# disable
>
```

### Display items

None

### Impact on communication

None

### Response messages

None

### Notes

None

---

## quit

---

Ends the current command input mode as follows:

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

For details about operations in configuration command mode, see the manual *Configuration Command Reference*.

### Syntax

quit

### Input mode

User mode, administrator mode, and configuration command mode

### Parameters

None

### Operation when a stack configuration is used

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

### Example

Ends administrator mode and returns to user mode.

```
# quit
>
```

### Display items

None

### Impact on communication

None

### Response messages

None

### Notes

None

---

## exit

---

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

For details about operations in configuration command mode, see the manual *Configuration Command Reference*.

### Syntax

exit

### Input mode

User mode, administrator mode, and configuration command mode

### Parameters

None

### Operation when a stack configuration is used

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

### Example

Ends administrator mode and logs out from the device.

```
# exit
```

### Display items

None

### Impact on communication

None

### Response messages

None

### Notes

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

---

## logout

---

Logs out from the device.

### Syntax

logout

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

### Example

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

```
# logout  
login:
```

### Display items

None

### Impact on communication

None

### Response messages

None

### Notes

None

---

## configure (configure terminal)

---

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

### Syntax

```
configure [terminal]
```

### Input mode

Administrator mode

### Parameters

terminal

Enables editing of the running configuration stored in memory.

### Operation when a stack configuration is used

The command can edit a configuration only on the master switch.

### Example

Changes the command input mode to configuration command mode.

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

### Display items

None

### Impact on communication

None

### Response messages

For details about error messages displayed during configuration editing, see *41.1.2 Editing configurations and operation information* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.

### Notes

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

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

## 2. Switching the Command Input Mode

configuration command mode.

## Chapter

---

# 3. Terminals and Remote Operations

---

set exec-timeout  
set terminal help  
set terminal pager  
show history  
telnet  
ftp  
tftp

---

## set exec-timeout

---

Sets the idle time (in minutes) for auto-logout (see 4.3(3) *Auto-logout* in the manual *Configuration Guide Vol. 1 For Version 11.10*). This setting can be configured for each user.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

<minutes>

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

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

### Operation when a stack configuration is used

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

```
remote command {<switch no.> | all} set exec-timeout <minutes>
```

### Example

Sets the auto-logout value to 30 minutes.

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

### Display items

None

### Impact on communication

None

### Response messages

None

### Notes

- If an account added by the `adduser` command with the `no-flash` parameter specified configures the settings using this command, they revert to the default (60 minutes) when the device is restarted.
- If any of `exec-timeout`, `terminal-pager`, or `terminal-help` is set for the `username` configuration command, the corresponding user operates with the `exec-timeout` setting value (specified value, or default value when the parameter is omitted) in the configuration.
- A user operating with the settings of the `username` configuration command can also temporarily change operations only in the target session by executing this command after login.
- When the Switch uses the sleep mode functionality, if you execute a command that configures the CLI environment information (`set exec-timeout`, `set terminal help`, or `set terminal pager`) immediately before or after the log message "E3 SOFTWARE 01910405 1001:000000000000 System is going to sleep soon.", which indicates the start of the sleep mode, the already set CLI environment information (any or all of auto-logout, paging,

and help) might return to the default settings.

To restore the settings, delete `.clirc` under the home directory of the user in this status, and then again set the CLI environment information.

Note that if the home directory does not contain `.clirc`, again set the CLI environment information without performing anything else.

---

## set terminal help

---

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

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

all

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

no-utility

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

### Operation when a stack configuration is used

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

```
remote command {<switch no.> | all} set terminal help { all | no-utility }
```

### Example

- Enables help messages for all permissible operation commands to be displayed.  
 > set terminal help all
  
- Enables help messages for all permissible operation commands except for utility commands and file operation commands to be displayed.  
 > set terminal help no-utility

### Display items

None

### Impact on communication

None

### Response messages

None

### Notes

- If an account added by the `adduser` command with the `no-flash` parameter specified configures the settings using this command, they revert to the default (all) when the device is restarted.
- If any of `exec-timeout`, `terminal-pager`, or `terminal-help` is set for the `username` configuration command, the corresponding user operates with the `terminal-help` setting value (specified value or default value for when the parameter is omitted) in the configuration.
- A user operating with the settings of the `username` configuration command can also temporarily change operations only in the target session by executing this command after login.

- When the Switch uses the sleep mode functionality, if you execute a command that configures the CLI environment information (`set exec-timeout`, `set terminal help`, or `set terminal pager`) immediately before or after the log message "E3 SOFTWARE 01910405 1001:000000000000 System is going to sleep soon.", which indicates the start of the sleep mode, the already set CLI environment information (any or all of auto-logout, paging, and help) might return to the default settings.

To restore the settings, delete `.clirc` under the home directory of the user in this status, and then again set the CLI environment information.

Note that if the home directory does not contain `.clirc`, again set the CLI environment information without performing anything else.

---

## set terminal pager

---

Specifies whether to perform paging (see 5.2.8 *Paging* in the manual *Configuration Guide Vol. 1 For Version 11.10*). This setting can be configured for each user.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

{ enable | disable }

enable

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

disable

Paging is not performed.

Operation when this parameter is omitted:

Paging is performed.

### Operation when a stack configuration is used

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

```
remote command {<switch no.> | all} set terminal pager [{ enable | disable }]
```

### Example

- Paging is not performed.  
> set terminal pager disable
  
- Paging is performed.  
> set terminal pager enable

### Display items

None

### Impact on communication

None

### Response messages

None

### Notes

- If an account added by the `adduser` command with the `no-flash` parameter specified configures the settings using this command, they revert to the default (enable) when the device is restarted.
- If any of `exec-timeout`, `terminal-pager`, or `terminal-help` is set for the `username` configuration command, the corresponding user operates with the `terminal-pager` setting value (specified value or default value for when the parameter is omitted) in the configuration.
- A user operating with the settings of the `username` configuration command can also

temporarily change operations only in the target session by executing this command after login.

- When the Switch uses the sleep mode functionality, if you execute a command that configures the CLI environment information (`set exec-timeout`, `set terminal help`, or `set terminal pager`) immediately before or after the log message "E3 SOFTWARE 01910405 1001:000000000000 System is going to sleep soon.", which indicates the start of the sleep mode, the already set CLI environment information (any or all of auto-logout, paging, and help) might return to the default settings.

To restore the settings, delete `.clirc` under the home directory of the user in this status, and then again set the CLI environment information.

Note that if the home directory does not contain `.clirc`, again set the CLI environment information without performing anything else.

---

## show history

---

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

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

### Syntax

`show history`

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

### Example

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

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

### Display items

None

### Impact on communication

None

### Response messages

None

### Notes

None

---

## telnet

---

Connects a virtual terminal to the remote operation terminal that has the specified IP address.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

<host>

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

When `/vrf <vrf id>` is specified, the destination host name cannot be specified to <host>. [OS-L3SA]

{/ipv4 | /ipv6}

/ipv4

Establishes a connection via IPv4 only.

/ipv6

Establishes a connection via IPv6 only.

Operation when this parameter is omitted:

Establishes a connection via IPv4 or IPv6.

/source-interface <source address>

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

Operation when this parameter is omitted:

The source IP address selected by the Switch is used.

/vrf <vrf id> [OS-L3SA]

Connects to the specified VRF. For <vrf id>, specify a VRF ID that was set in the configuration.

Operation when this parameter is omitted:

Displays the information for the global network.

<port>

Specifies a port number.

Operation when this parameter is omitted:

23 is used for the port number.

Operation when all parameters are omitted:

Connects to specified <host> in global networks.

## Operation when a stack configuration is used

The command can be executed only on the master switch.

### Example

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

```
> telnet 192.168.0.1
```

After the `telnet` command is executed, the following message indicating that you will need to wait for the connection with the remote operation terminal to be established is displayed.  
 Trying 192.168.0.1 ...

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

```
Connected to 192.168.0.1
Escape character is '^]'.
```

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

```
login: username
Password: *****
```
3. Accesses the remote operation terminal whose IPv6 address is 3ffe:1:100::250 via Telnet.  

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

### Display items

None

### Impact on communication

None

### Response messages

Table 3-1: List of response messages for the telnet command

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

Message	Description
Connected to <i>&lt;host&gt;</i> .	A connection to <i>&lt;host&gt;</i> was established. <i>&lt;host&gt;</i> : Remote host
Connection closed by foreign host.	The connection was closed from the host.
Trying <i>&lt;host&gt;</i> ...	Trying to connect to <i>&lt;host&gt;</i> . <i>&lt;host&gt;</i> : Remote host
Unable to connect to remote host	The connection to the host could not be established.
Unable to connect to remote host: Connection refused	The host rejected the connection.
Unable to connect to remote host: Operation timed out	The connection timed out.

## Notes

- To interrupt the processing while `Trying...` is displayed, press the **Ctrl + C** keys.
- After a connection is established, to halt execution of this command while the login prompt is displayed, press the **Ctrl + D** keys.
- This command sends the input key codes to the login destination remote device without making any modifications. Therefore, the key code output by the terminal on which this command is entered must be the same as the key code required by the destination terminal. If they are different, the command will not operate correctly. For example, as the input key code for the carriage return control code (the **Enter** key), some terminals generate 0x0D or 0x0D0A, whereas other terminals need to receive 0x0D or 0x0A to recognize a carriage return control code from the login destination terminal. Check key code compatibility beforehand.
- When the escape character `^]` (**Ctrl + ]** keys) is entered while a connection is being established, the mode switches to `telnet>` mode. In this mode, inputting `quit` ends the `telnet` command (If a connection is established, it is closed). To exit from `telnet>` mode, enter just a line feed without any other character.

---

**ftp**


---

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

**Syntax**

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

**Input mode**

User mode and administrator mode

**Parameters**

<host>

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

Operation when this parameter is omitted:

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

{/ipv4 | /ipv6}

/ipv4

Establishes a connection via IPv4 only.

/ipv6

Establishes a connection via IPv6 only.

Operation when this parameter is omitted:

Establishes a connection via IPv4 or IPv6.

/source-interface <source address>

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

Operation when this parameter is omitted:

The source IP address selected by the Switch is used.

/vrf <vrf id> [OS-L3SA]

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

Operation when this parameter is omitted:

Connects to global network.

Operation when all parameters are omitted:

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

**Operation when a stack configuration is used**

The command can be executed only on the master switch.

## Example

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

```
> ftp 192.168.0.1
```

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

1. Entering the login name:

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

Name :

2. Entering the password:

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

Password:

3. Entering a file transfer command:

The following prompt is displayed on the command line.

ftp>

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

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

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

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

`mget <remote-files>`

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

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

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

`mput <local-files>`

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

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

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

`ascii`

Sets ASCII as the transfer format of the file.

`binary`

Sets binary as the transfer format of the file.

`[ bye | quit | exit ]`

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

`cd <remote-directory>`

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

*cdup*

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

*chmod <mode> <remote-file>*

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

*close*

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

*debug*

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

*delete <remote-file>*

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

*hash*

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

*{help | ?} [<command>]*

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

*lcd [<directory>]*

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

*lols [<local-directory>]*

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

*[ lopwd | lpwd ]*

Displays the current directory of the Switch.

*lpage <local-file>*

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

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

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

*mdelete [<remote-files>]*

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

*mkdir <directory-name>*

Creates a directory on the remote operation terminal.

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

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

*open <host> [<port>]*

Establishes a connection to the FTP server with the specified address. When a port

number (option) is specified, the `ftp` command tries to connect to the FTP server on the specified port.

**passive**

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

**progress**

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

**prompt**

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

**pwd**

Displays the current directory on the remote operation terminal.

**rename** *<from-name>* *<to-name>*

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

**rmdir** *<directory-name>*

Deletes a directory on the remote operation terminal.

**status**

Displays the current FTP status.

**verbose**

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

## Display items

None

## Impact on communication

None

## Response messages

Table 3-2: List of response messages for the `ftp` command

Message	Description
?Ambiguous command	Multiple commands contain the specified characters.
?Ambiguous help command <i>&lt;command&gt;</i>	Multiple help commands correspond to the specified characters. <i>&lt;command&gt;</i> : Command name
?Invalid command	The specified command could not be found.
<i>&lt;file name&gt;</i> : No such file OR directory	The specified file or directory could not be found. <i>&lt;file name&gt;</i> : The specified file name or directory name

### 3. Terminals and Remote Operations

Message	Description
<host>: bad port number -- <port>usage: open host-name [port]	An invalid port number was input. <port>: Port number
<host>: Host name lookup failure	An unknown host name was input. <host>: Remote host
<host>: hostname nor servname provided, or not known	The address specified for the host and the connection method specified by option are invalid or inconsistent. <host>: Remote host
<host>: Unknown host	An unknown host name was input. <host>: Remote host IP address
Already connected to <host>, use close first.	Communication with the remote device has already been established. To connect to another host, use the (ftp) <code>close</code> command or (ftp) <code>quit</code> command to stop the communication. <host>: Remote host IP address
bind: Can't assign requested address	An invalid source IP address has been set.
bind: Invalid argument	An invalid source IP address has been set.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot specify hostname with VRF	VRF and a host name cannot be specified at the same time.
connect to address <host>: Connection refused	The host rejected the connection. <host>: Remote host
connect to address <host>: No route to host	The connection to the host cannot be established because no route exists. <host>: Remote host
connect to address <host>: Operation timed out	The connection timed out. <host>: Remote host
connect: Connection refused	Connection has failed.
connect: No route to host	A connection cannot be established because the routing table to the remote host does not exist.
connect: Operation timed out	The connection timed out.
Connected to <host>.	A connection to <host> was established. <host>: Remote host
Login failed.	A login attempt has failed.
No address associated with hostname	The connection to the host could not be established because the address could not be resolved.
No control connection for command: Bad file descriptor	The command could not be executed because the control connection with the remote host was lost.
Not connected.	No remote communication.
quit for Ctrl+Z pushed.	The ftp command was ended by pressing the <b>Ctrl + Z</b> keys.
Service not available, remote server has closed connection	The command could not be executed because the connection was closed on the remote host.
Trying <host>...	Trying to connect to <host>. <host>: Remote host

## Notes

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

---

## tftp

---

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

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

<host>

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

Operation when this parameter is omitted:

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

{/ipv4 | /ipv6}

/ipv4

Establishes a connection via IPv4 only.

/ipv6

Establishes a connection via IPv6 only.

Operation when this parameter is omitted:

Establishes a connection via IPv4 or IPv6.

/source-interface <source address>

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

Operation when this parameter is omitted:

The source IP address selected by the Switch is used.

/vrf <vrf id> [OS-L3SA]

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

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

Operation when this parameter is omitted:

Connects to global network.

<port>

Specifies the port number of the connection destination.

Operation when this parameter is omitted:

69 is used for the port number.

Operation when all parameters are omitted:

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

### Operation when a stack configuration is used

The command can be executed only on the master switch.

### Example

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

```
> tftp 192.168.0.1
```

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

1. Entering a file transfer command:

The following prompt is displayed on the command line.

```
tftp>
```

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

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

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

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

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

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

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

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

```
connect <host> [port]
```

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

```
mode
```

Checks the current file transfer format.

```
quit
```

Ends the `tftp` command.

```
trace
```

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

```
status
```

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

```
binary
```

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

```
ascii
```

Sets ascii (netascii) as the file transfer format.

? [*<command>*]

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

## Display items

None

## Impact on communication

None

## Response messages

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

Message	Description
?Invalid command	The specified command could not be found.
?Invalid help command <i>&lt;command&gt;</i>	The help command applicable to the specified characters could not be found. <i>&lt;command&gt;</i> : Command name
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot specify hostname with VRF	VRF and a host name cannot be specified at the same time.
Error code <i>&lt;number&gt;</i> : <i>&lt;message&gt;</i>	Displaying other TFTP error messages: <i>&lt;number&gt;</i> : Error code <i>&lt;message&gt;</i> : Error description
Error code 1: File not found	The specified file could not be found.
Error code 2: Access violation	The specified file could not be accessed.
Error code 3: Disk full or allocation exceeded	The disk is full or allocation exceeds the limit.
Error code 6: File already exists	The file already exists.
getting from <i>&lt;host&gt;</i> : <i>&lt;remote file&gt;</i> to <i>&lt;local file&gt;</i> [ <i>&lt;mode&gt;</i> ]	Receiving <i>&lt;remote file&gt;</i> on <i>&lt;host&gt;</i> as <i>&lt;local file&gt;</i> (the transfer mode is <i>&lt;mode&gt;</i> ). <i>&lt;host&gt;</i> : Remote host <i>&lt;remote file&gt;</i> : Remote file name <i>&lt;local file&gt;</i> : Local file name <i>&lt;mode&gt;</i> : File transfer mode
No target machine specified, Use connect command.	The connection destination has not been set. Use the connect command to set it.
putting <i>&lt;local file&gt;</i> to <i>&lt;host&gt;</i> : <i>&lt;remote file&gt;</i> [ <i>&lt;mode&gt;</i> ]	Sending <i>&lt;local file&gt;</i> to <i>&lt;host&gt;</i> as <i>&lt;remote file&gt;</i> (the transfer mode is <i>&lt;mode&gt;</i> ). <i>&lt;local file&gt;</i> : Local file name <i>&lt;host&gt;</i> : Remote host <i>&lt;remote file&gt;</i> : Remote file name <i>&lt;mode&gt;</i> : File transfer mode
quit for Ctrl+Z pushed.	The tftp command was ended by pressing the <b>Ctrl + Z</b> keys.
tftp: <i>&lt;file name&gt;</i> : Is a directory	The specified file is a directory. <i>&lt;file name&gt;</i> : File name
tftp: <i>&lt;file name&gt;</i> : Permission denied	Access permission for the specified file does not exist. <i>&lt;file name&gt;</i> : File name
tftp: bind: Can't assign requested address	An invalid source IP address has been set.

Message	Description
tftp: bind: Invalid argument	An invalid source IP address has been set.
tftp: No address associated with hostname	The connection to the host could not be established because the address could not be resolved.
tftp: sendto: No route to host	The connection to the remote host cannot be established because no route exists.
tftp: servname not supported for ai_socktype	An invalid port number was input.
Transfer timed out.	Transfer timed out. Check the route to the server or the server settings.

## Notes

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



## Chapter

---

# 4. Configurations and File Operations

---

show running-config (show configuration)  
show startup-config  
copy  
erase configuration  
show file  
cd  
pwd  
ls  
dir  
cat  
cp  
mkdir  
mv  
rm  
rmdir  
delete  
undelete  
squeeze  
zmodem

---

## show running-config (show configuration)

---

Displays the running configuration.

### Syntax

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

### Input mode

Administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

### Example and display items

None

### Impact on communication

None

### Response messages

For details about error messages displayed during configuration editing, see *41.1.2 Editing configurations and operation information* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.

### Notes

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

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

---

## show startup-config

---

Displays the startup configuration used at device startup.

### Syntax

```
show startup-config
```

### Input mode

Administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

### Example and display items

None

### Impact on communication

None

### Response messages

For details about error messages displayed during configuration editing, see *41.1.2 Editing configurations and operation information* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.

### Notes

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

---

## copy

---

Copies a configuration.

### Syntax

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

### Input mode

Administrator mode

### Parameters

*<source file>*

Specifies the copy-source configuration file or configuration.

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

*<file name>*

- Specifying a local configuration file  
Specify the name of the file in a switch.
- Specify a remotely-stored configuration file.

The following URL formats can be specified:

FTP

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

TFTP

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

HTTP

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

*<user name>*: User name on the remote server

*<password>*: Password for the remote server

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

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

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

*<port>*: Specifies a port number.

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

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

running-config: Running configuration

startup-config: Startup configuration file

*<target file>*

Specifies the copy-destination configuration file or configuration.

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

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

When the stack is configured, *running-config* cannot be specified.

#### debug

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

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

Operation when this parameter is omitted:

Details about communication status are not displayed.

### Operation when a stack configuration is used

The command can be executed only on the master switch.

#### Example

- Copy the running configuration to the startup configuration.  

```
# copy running-config startup-config
Configuration file copy to startup-config? (y/n):y
```
- Save the running configuration to a file on a remote server.  

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

Authentication for 2001:240:400::101.
User: staff
Password: xxx (Enter the password stored on the remote server for the user
account "staff".)
transferring

Data transfer succeeded.
#
```

#### Display items

None

#### Impact on communication

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

#### Response messages

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

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't set stack enable in running-config because stack is not active.	The <i>stack enable</i> configuration command cannot be set in the running configuration because the stack is not active.

Message	Description
Can't specify running-config for <i>&lt;target file&gt;</i> because stack is active.	When the stack is active, the running configuration cannot be specified in the <i>&lt;target file&gt;</i> parameter. To change the operation mode, execute this command with the startup configuration file specified in the <i>&lt;target file&gt;</i> parameter, and then restart all the switches.
Configuration file already exist. Configuration file copy to <i>&lt;target file&gt;?</i> (y/n):	That copy-destination file name already exists. This message asks for confirmation on whether or not to overwrite the file. Entering <i>y</i> performs the copy. Entering <i>n</i> aborts the copy.
Configuration file copy to <i>&lt;target file&gt;?</i> (y/n):	This message asks for confirmation on whether or not to copy a file to the copy-destination file name. Entering <i>y</i> performs the copy. Entering <i>n</i> aborts the copy.

For details about error messages displayed during configuration editing, see *41.1.2 Editing configurations and operation information* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.

## Notes

1. You cannot copy to a running configuration while the running configuration is being edited. Execute the copy command after the edit is completed.
2. When the running configuration is updated, the edited contents of the configuration are also updated.
3. Editing the startup configuration has no effect on the running configuration or communication.
4. If you do not have writing permission for the save destination file, your edits cannot be saved to the file. To save edits to a file on a remote server, change the settings to allow you to write on the remote server.
5. If you copy a configuration to the running configuration, the specified configuration becomes the running configuration. Note that if you were logged in via the network, the operating port is restarted.
6. If you copy a configuration file created using an editor or a different device model, operation might be unstable even if the copy command completes normally. Before copying, confirm that the configuration file contents and interface definitions to be applied are appropriate for the capacity limit of the device and that there is sufficient space for the new configuration file. If you perform a copy by mistake, use the `erase configuration` command to reset the configuration, and then edit it again.
7. If there is insufficient free space for storing files, a configuration cannot be copied. Use the `show mc` command to check the free space in the user area. The necessary space required for copying a configuration is the total size of the new configuration in the copy source and the existing configuration in the copy destination. About 2 MB of free capacity is required for a maximum-size configuration file.
8. When specifying the URL format, we recommend that you omit *<password>* when executing the command. The executed command is recorded in operation logs, and might be referenced by other users. To ensure security, we recommend that you omit *<password>* and input the password by using the inquiry prompt.
9. In the URL notation, a single `/` located between the *<host>* specification and the *<filepath>* specification is not included as a path component. For example, to specify `/usr/home/staff/a.cnf` on the FTP remote server, specify `ftp://<host>/usr/home/staff/a.cnf`.
10. When the copy source is a running configuration, and the copy destination is a startup configuration, the same processing as that for the `save` command is performed.

---

## erase configuration

---

Resets startup configuration and running configuration to the defaults.

### Syntax

```
erase configuration
```

### Input mode

Administrator mode

### Parameters

None

### Operation when a stack configuration is used

This command is not supported.

### Example

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

### Display items

None

### Impact on communication

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

### Response messages

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

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

For details about error messages displayed during configuration editing, see *41.1.2 Editing configurations and operation information* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.

### Notes

1. This command cannot be used while the configuration is being edited. Use this command to reset the configuration file to the default, after the configuration edit is completed.
2. When this command is executed, the operating ports stop all operations. You need to be careful if you logged in via a network because the session is terminated by executing this command.

---

## show file

---

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

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

<file name>

Specifies the following items as file names to be displayed.

- Local file specification  
Specify the name of the file to be stored in the flash memory of a switch.

- Remote file specification  
Specifies the following types of URLs:

FTP

```
ftp://[<user name>[:<password>]@]<host>[:<port>]/<filepath>
```

TFTP

```
tftp://<host>[:<port>]/<filepath>
```

HTTP

```
http://[<user name>[:<password>]@]<host>[:<port>]/[<filepath>]
```

<user name>: User name on the remote server

<password>: Password for the remote server

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

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

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

<port>: Specifies a port number.

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

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

debug

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

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

Operation when this parameter is omitted:

Details about communication status are not displayed.

## Operation when a stack configuration is used

The command can display information only for the master switch.

### Example

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

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

Authentication for 2001:240:400::101.
User: staff
Password: xxx (Enter the password stored on the remote server for the user
account "staff".)
transferring...

interface gigabitethernet 0/1
  switchport mode access
!

### Total 3 lines.
>
```

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

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

Authentication for 2001:240:400::101.
User: staff
Password: xxx (Enter the password stored on the remote server for the user
account "staff".)
transferring...

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

### Display items

None

### Impact on communication

None

### Response messages

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

Message	Description
### List of remote directory.	Gets and displays the list of the specified directory.
### Total <number> lines.	The number of lines of the displayed file is <number> lines.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.

Message	Description
Data transfer failed. (<reason>)	File transfer from the remote server failed. <reason>: Additional information Re-execute the command with the <code>debug</code> parameter specified for checking.

## Notes

1. Specify ASCII text files as the files to be displayed. Do not specify files that cannot be displayed by terminals, such as binary-format files. If such files are specified, the display might be distorted or display invalid characters. In this case, log in to the Switch again, or reset the terminal.  
  
For HTTP transfers, such files might be discarded part way through the transfer, the transfer might result in the error `Data transfer failed.`, and download might not be performed.
2. When specifying the URL format with <file name>, we recommend that you omit the <password> when executing the command. The executed command is recorded in operation logs, and they might be checked by other users. To ensure security, we recommend that you omit <password> and input the password by using the inquiry prompt.
3. For access via FTP, specify a directory with / specified at the end of the file path to get and display the directory list.
4. In the URL notation, a single / located between the <host> specification and the <filepath> specification is not included as a path component. For example, to specify `/usr/home/staff/a.cnf` on the FTP remote server, specify `ftp://<host>/usr/home/staff/a.cnf`.

---

**cd**

---

Changes the directory.

**Syntax**

`cd [<directory>]`

**Input mode**

User mode and administrator mode

**Parameters**

*<directory>*

Specifies the name of the destination directory.

Operation when this parameter is omitted:

Moves to the home directory of the current login user.

**Operation when a stack configuration is used**

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

**Example and display items**

None

**Impact on communication**

None

**Response messages**

None

**Notes**

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

---

## **pwd**

---

Shows the path to the current directory.

### **Syntax**

pwd

### **Input mode**

User mode and administrator mode

### **Parameters**

None

### **Operation when a stack configuration is used**

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

### **Example and display items**

None

### **Impact on communication**

None

### **Response messages**

None

### **Notes**

None

---

## ls

---

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

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

*<option>*

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

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

Operation when this parameter is omitted:

Hidden files and detailed information are not displayed.

*<names>*

Specifies a file name or directory name.

Operation when this parameter is omitted:

Shows a list of the contents of the current directory.

mc-dir

Show the list of files on a memory card.

### Operation when a stack configuration is used

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

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

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

### Example

Show the list of files on a memory card.

```
>ls mc-dir
```

### Display items

None

### Impact on communication

None

### Response messages

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

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

Message	Description
MC not found.	A memory card was not inserted. Make sure that a memory card is inserted into the device properly. Make sure there is no dust in the memory card slot. If there is dust, remove it with a dry cloth and then insert the memory card again.

## Notes

1. The `mc-dir` parameter cannot be used when a memory card is not inserted.
2. When the `mc-dir` parameter is specified, the ACC LED is on while the command is being executed. Do not remove or insert the memory card while the ACC LED is on.
3. If this command is executed by the `remote command` command, one file is displayed per line as the execution result of a backup switch.

---

## dir

---

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

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

`/all`

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

`summary`

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

Operation when this parameter is omitted:

Shows a list of files including detailed information.

`/deleted`

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

### Operation when a stack configuration is used

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

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

### Example

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

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

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

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

*Figure 4-2: Displayed file when only /all is specified*

```
> dir /all
Directory of ./:
- -rw-r--r-- user      user      123117 Jan 27 14:18 userfile1
```

```

- -rw-r--r-- user      user      344 Jan 27 14:55 userfile2
6 -rw-r--r-- user      user      16 Jan 27 17:57 [userfile3]
>

```

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

*Figure 4-3: Displayed deleted files*

```

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

```

## Display items

*Table 4-5: Display contents when the /all option is specified*

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

*Table 4-6: Display contents when the /deleted option is specified*

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

Location (digit)	Item	Description
27 to 38	File modification date	Indicates the file modification date.
40 to	Deleted file name	Indicates the deleted file name.

### Impact on communication

None

### Response messages

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

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

### Notes

None

---

## cat

---

Shows the contents of a specified file.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

*<option>*

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

Operation when this parameter is omitted:

Shows the contents of a specified file without any modification.

*<file name>*

Specifies a file name to be displayed.

### Operation when a stack configuration is used

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

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

### Example and display items

None

### Impact on communication

None

### Response messages

None

### Notes

None

---

## cp

---

Copies a file.

### Syntax

```
cp [<option>] <file name1> <file name2>
cp <file name1> mc-file <mc file name2>
    (Copies a file on the internal flash memory to a memory card.)
cp mc-file <mc file name1> <file name2>
    (Copies a file on a memory card to the internal flash memory.)
cp <file name1> switch <switch no.> <switch file name2>
    (Copies the file in internal flash memory to the member switch having the
    specified switch number)
cp switch <switch no.> <switch file name1> <file name2>
    (Copies the file in the member switch having the specified switch number to
    the internal flash memory)
```

### Input mode

User mode and administrator mode

### Parameters

<option>

-r: Copies a directory.

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

Operation when this parameter is omitted:

Copies the specified file without asking for confirmation of overwriting.

<file name1>

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

<file name2>

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

mc-file <mc file name2>

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

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

mc-file <mc file name1>

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

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

switch <switch no.>

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

<switch file name2>

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

<switch file name1>

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

### Operation when a stack configuration is used

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

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

```
remote command {<switch no.> | all} cp <file name1> mc-file <mc file name2>
```

(Copies the file in internal flash memory of the member switch to the memory card of the member switch)

```
remote command {<switch no.> | all} cp mc-file <mc file name1> <file name2>
```

(Copies the file in the memory card of the member switch to the internal flash memory of the member switch)

### Example

- Copy file1 from the internal flash memory to the memory card and name as file2.  
`>cp file1 mc-file file2`
- Copy file1 from the memory card to the internal flash memory and name as file2.  
`>cp mc-file file1 file2`
- Copy `/var/tmp/file1` from the current member switch to the `/var/tmp` directory of the member switch having the switch number 2, and name the file as file2.  
`>cp /var/tmp/file1 switch 2 /var/tmp/file2`

### Display items

None

### Impact on communication

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

### Response messages

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

Message	Description
Can't create file.	The file could not be copied. Check the state such as free capacity, and then re-execute the command.
Can't execute.	The command could not be executed. Re-execute the command.
copy error	The file could not be read from or written to the memory card. Check the state of the destination such as the free capacity of the memory card and internal flash memory, and then re-execute the command.
MC is busy.	Another process is accessing the memory card. Wait a while, and then re-execute the command.
MC is write protected.	Make sure the memory card's protect switch is not set to ▼ Lock. If the switch is set to ▼ Lock, slide the switch, and then insert the memory card again. Make sure there is no dust in the memory card slot. If there is dust, remove it with a dry cloth and then insert the memory card again.

Message	Description
MC not found.	A memory card was not inserted. Make sure that a memory card is inserted into the device properly. Make sure there is no dust in the memory card slot. If there is dust, remove it with a dry cloth and then insert the memory card again.
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. <switch no.>: Switch number

## Notes

1. The `mc-file` parameter cannot be used when a memory card is not inserted.
2. When the `mc-file` parameter is specified, the ACC LED is on while the command is being executed. Do not remove or insert the memory card while the ACC LED is on.
3. Accessing a memory card increases load on the device. Before specifying `mc-file`, if monitoring time and sending interval of the Layer 2 or Layer 3 protocol, which are settings for maintaining connection with neighboring devices, are set shorter than the initial value, reset the monitoring time and sending interval to longer values.
4. The `switch <switch no.>` parameter can be specified only on the master switch when the stack is configured.
5. If this command is executed by the `remote command` command, the current directory of the other member switch becomes the home directory of the user who executes this command.

---

## mkdir

---

Creates a new directory.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

*<option>*

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

Operation when this parameter is omitted:

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

*<directory>*

Specifies the name of the directory to be created.

mc-dir *<directory>*

Creates a directory on a memory card.

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

### Operation when a stack configuration is used

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

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

### Example

Creates a directory `newdir` on a memory card.

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

### Display items

None

### Impact on communication

None

### Response messages

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

Message	Description
Can't create directory.	A directory could not be created in the memory card. Check the state of the memory card such as free capacity, and then re-execute the command.
Can't execute.	The command could not be executed. Re-execute the command.

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

## Notes

1. The `mc-dir` parameter cannot be used when a memory card is not inserted. In addition, the parameter cannot be used with the `-p` option.
2. When the `mc-dir` parameter is specified, the ACC LED is on while the command is being executed. Do not remove or insert the memory card while the ACC LED is on.

---

## mv

---

Moves or renames a file.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

*<option>*

-f

Forcibly performs a move without requesting confirmation.

Operation when this parameter is omitted:

Displays a confirmation message, and then moves or renames a file.

*<file name1>*

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

*<file name2>*

Specifies the name of the file after moving or renaming.

*<directory1>*

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

*<directory2>*

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

*<names>*

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

*<dir>*

Indicates the name of the destination directory.

### Operation when a stack configuration is used

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

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

### Example and display items

None

### Impact on communication

None

### Response messages

None

## Notes

None

---

## rm

---

Deletes a specified file.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

*<option>*

-r: Deletes all files in the specified directory and the directories below it.

Operation when this parameter is omitted:

Deletes only the specified file.

*<file name>*

Specifies a file name or directory name to be deleted.

mc-file *<mc file name>*

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

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

### Operation when a stack configuration is used

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

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

### Example

Delete a file called `file1` on the memory card.

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

### Display items

None

### Impact on communication

None

### Response messages

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

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

Message	Description
MC is write protected.	Make sure the memory card's protect switch is not set to ▼ Lock. If the switch is set to ▼ Lock, slide the switch, and then insert the memory card again. Make sure there is no dust in the memory card slot. If there is dust, remove it with a dry cloth and then insert the memory card again.
MC not found.	A memory card was not inserted. Make sure that a memory card is inserted into the device properly. Make sure there is no dust in the memory card slot. If there is dust, remove it with a dry cloth and then insert the memory card again.

## Notes

1. The `mc-file` parameter cannot be used when a memory card is not inserted. In addition, the parameter cannot be used with the `-r` option.
2. When the `mc-file` parameter is specified, the ACC LED is on while the command is being executed. Do not remove or insert the memory card while the ACC LED is on.
3. If file names or directory names include special characters, an error such as a command invalid error might occur. In this case, specify an asterisk wildcard (\*) for `<file name>`, and individually confirm target files, to delete files named with special characters. Special characters are characters other than alphanumeric characters listed in *List of character codes* in 1. *Reading the Manual*.

---

## rmdir

---

Deletes a specified directory.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

<directory>

Specifies the name of the directory to be deleted.

mc-dir <directory>

Deletes a directory on the memory card.

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

### Operation when a stack configuration is used

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

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

### Example

Delete a directory `deldir` on the memory card.

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

### Display items

None

### Impact on communication

None

### Response messages

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

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

Message	Description
MC not found.	A memory card was not inserted. Make sure that a memory card is inserted into the device properly. Make sure there is no dust in the memory card slot. If there is dust, remove it with a dry cloth and then insert the memory card again.

**Notes**

1. The `mc-dir` parameter cannot be used when a memory card is not inserted.
2. When the `mc-dir` parameter is specified, the ACC LED is on while the command is being executed. Do not remove or insert the memory card while the ACC LED is on.

---

## delete

---

Recoverably deletes files on the internal flash memory used by the Switch. Note that the maximum number of files that can be deleted is 64 files.

### Syntax

```
delete <file name>
```

### Input mode

User mode and administrator mode

### Parameters

<file name>

Specifies the name of a file to be deleted.

### Operation when a stack configuration is used

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

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

### Example

Recoverably deletes a file.

*Figure 4-4: Executing delete for a file*

```
> delete userfile
>
```

### Display items

None

### Impact on communication

None

### Response messages

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

Message	Description
delete: Delete command can not be used this flash. (<code>)	This command cannot be used for internal flash memory (<internal code>).
delete: Directory is specified.	A directory has been specified.
delete: No flash file is specified.	The specified file does not exist.
delete: No such file or directory.	The specified file does not exist. or the current directory is not valid.
delete: Not enough flash space.	There is not enough free space on the internal flash memory to execute this command.
delete: Permission denied.	No deletion permission for the specified file exists.
delete: Specify file name.	Specify a file name.

### Notes

1. This command can operate only on files in internal flash memory. Files on RAM disk (memory) cannot be deleted.

2. If there is not enough free space on internal flash memory to recoverably store files, this command cannot be used for deletion.
3. To recover files deleted by this command, use the `undelete` command.
4. To completely erase files deleted by this command, use the `squeeze` command.
5. To list files deleted by this command, use the `dir` command.

---

## undelete

---

Recovers recoverably deleted files on the internal flash memory used by the Switch.

### Syntax

```
undelete <index>
```

### Input mode

User mode and administrator mode

### Parameters

<index>

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

### Operation when a stack configuration is used

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

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

### Example

Recover files deleted by the `delete` command.

*Figure 4-5: File recovery*

```
> dir /all

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

### Display items

None

### Impact on communication

None

### Response messages

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

Message	Description
undelete: Current directory is not flash.	The current directory is not the internal flash memory. Move to an appropriate directory.
undelete: Directory is not found for undelete file.	No directory found for restoring undeleted files to. Create a directory for storing the file.
undelete: Exist same name file or directory.	A file or directory that has the same name as that of the specified file already exists in the directory for executing the <code>undelete</code> command.
undelete: Invalid index value.	Specify decimal values for the index value.
undelete: No such file or directory.	The current directory is not valid.

Message	Description
undelete: Not found undelete file.	The specified file does not exist.
undelete: Permission denied.	You do not have access permission for the current directory or specified file.
undelete: Permission denied of directory for undelete file.	You do not have write permission for the directory where the specified file is to be stored.
undelete: Specify correct deleted index number.	Specify a proper index number for the deleted file.
undelete: Specify correct index number [1-64].	Specify a numeric value between 1 and 64 for the index value.
undelete: Specify index number.	Specify an index number.
undelete: Undelete command can not be used this flash. (<code>)	This command cannot be used for internal flash memory (<internal code>).

## Notes

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

---

## squeeze

---

Completely erases files on internal flash memory used by the Switch that have been recoverably deleted by the `delete` command.

### Syntax

`squeeze`

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

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

### Example

Completely erase files deleted by the `delete` command.

*Figure 4-6: Executing squeeze for a file*

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

### Display items

None

### Impact on communication

None

### Response messages

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

Message	Description
Canceled	The squeeze command has been canceled.
Deleted files will be erased. OK ? (y/n):	Erases deleted files. Enter <code>y</code> to erase, otherwise <code>n</code> to abort.
Done	The erasure has been completed.
squeeze: Current directory is not flash.	The current directory is not internal flash memory.
squeeze: No such file or directory.	The current directory is not valid. Move to an appropriate directory.
squeeze: Permission denied.	You do not have access permission for the current directory. Move to an appropriate directory.
squeeze: Squeeze command can not be used this flash.( <code>&lt;code&gt;</code> )	This command cannot be used for internal flash memory ( <code>&lt;internal code&gt;</code> ).
Squeezing	Erasing the file.

## Notes

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

---

## zmodem

---

Transfers files between the Switch and console connected by RS232C.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

get

Transfers files from the console to the Switch.

put <file name>

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

### Operation when a stack configuration is used

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

### Example

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

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

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

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

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

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

### Display items

None

### Impact on communication

None

### Response messages

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

Message	Description
<file name>: No such file.	The file to be transferred (<file name>) was not found. <file name>: File name
Execute only console machine.	This command can be executed on only the console. This command cannot be executed on a remote operation terminal.

Message	Description
Receive skipped : <file name> (already exists)	Reception was interrupted because a file with the same name as the file being received already exists. <file name>: File name
Receive skipped : <file name> (permission denied)	Reception was skipped because the user who executed the command did not have the write permission for the file or directory. <file name>: File name
ttyname error.	The terminal type cannot be recognized.

## Notes

1. This command can be executed only from the console. This command cannot be executed on a remote operation terminal.
2. If a file transfer is interrupted for reasons such as a cable failure during execution of this command and the interruption continues for a long period of time, the file transfer fails as follows:
  - When `zmodem get` is executed, the command prompt is displayed if the interruption lasts for one minute.
  - When `zmodem put` is executed, the command prompt is displayed if the interruption lasts for one minute.
3. Control codes displayed during file transfers do not affect system operation. The codes can be ignored. The displayed characters do not have any special meanings.
4. The `zmodem` command can be used to transfer a file under the following communication conditions:
  - Character length: 8 bits
  - Communication speed: 9600 bit/s, 4800 bit/s, or 2400 bit/s
  - Stop bit length: 1 bit or 2 bits
  - Parity bit: None



## Chapter

---

# 5. Stack

---

remote command  
show switch  
set switch  
dump stack

---

## remote command

---

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

### Syntax

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

### Input mode

Administrator mode

### Parameters

{<switch no.> | all}

<switch no.>

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

all

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

<command>

Specifies an operation command to be executed.

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

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

### Operation when a stack configuration is used

The command can be executed only on the master switch.

### Example

- Execute the `show clock` command for the member switch whose switch number is 2.

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

- Execute the `show clock` command for all member switches.

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

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

- Output the result of executing the `show clock` command for the member switch whose switch number is 2. The result is output to the home directory of the switch whose file name is `nowtime.txt`.  

```
# remote command 2 'show clock > ./nowtime.txt'
Switch 2 (Backup)
-----
#
```
- Output the result of executing the `show clock` command for the member switch whose switch number is 2. The result is output to the current directory of the master switch on which this command is executed with the file name `nowtime.txt`.  

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

## Display items

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

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

## Impact on communication

None

## Response messages

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

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

## Notes

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

disabled on switches other than the master switch.

4. When using this command to execute an operation command, paging is disabled on switches other than the master switch.
5. When using the pipe functionality to pass the result of a command executed by using this command to another command, such as the `more` command or the `less` command, keys might be temporarily unavailable. In this case, press the same key again.
6. When using the pipe functionality to pass the result of a command executed by using this command to another command, such as the `more` command or the `less` command, a response message might be displayed in the execution result. In this case, check the execution result without using the pipe functionality.
7. When using this command to execute an operation command, the operation command is executed in a different session than the operation terminal that executes the command.
8. When executing operation commands including this command in succession, wait until this command finishes and the prompt appears, and then execute the next operation command.

---

## show switch

---

Displays information about member switches that configure a stack.

### Syntax

```
show switch [detail]
```

### Input mode

User mode and administrator mode

### Parameters

detail

Displays detailed information about member switches.

Operation when this parameter is omitted:

Summary information about member switches is displayed.

### Operation when a stack configuration is used

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

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

### Example 1

The following shows examples of displaying summary information about member switches.

*Figure 5-1: Example of displaying summary information about member switches (stack configuration)*

```
> show switch
Date 20XX/10/26 11:38:56 UTC
Stack status : Enable      Switch No : 1
System MAC Address : 0012.e220.5101
No  Switch status      Model      Machine ID      Priority  Ver
 1  Master              3650-24t6xw  0012.e220.5101  31       1
 2  Backup (Initializing) 3650-24t6xw  0012.e220.5102  11       1
```

*Figure 5-2: Example of displaying summary information about member switches (standalone configuration)*

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

### Display items in Example 1

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

Item	Meaning	Displayed detailed information
Stack status	Stack operating status	Enable: Operating in a stack configuration Disable: Operating in a standalone configuration
Switch No	Switch number of the device	1 to 2 The switch number set by the <code>set switch</code> command is displayed.
System MAC Address	Device MAC address	Device MAC address of the stack If the master has not been determined, - is displayed.
No	Switch number	1 to 2

Item	Meaning	Displayed detailed information
Switch status	Switch state	Master: Master Backup: Backup Init: Initial state The processing details are displayed during the change processing after a switch state transition. (Initializing): Initializing (Switchover): Switching
Model	Member switch model	3830-44xw: AX3830S-44XW 3830-44x4qw: AX3830S-44X4QW 3650-24t6xw: AX3650S-24T6XW 3650-48t4xw: AX3650S-48T4XW 3650-20s6xw: AX3650S-20S6XW
Machine ID	Chassis MAC address	--
Priority	Master selection priority of member switches	1 to 31
Ver	Stack functionality version	1

## Example 2

The following shows an example of displaying detailed information about member switches.

*Figure 5-3: Example of displaying detailed information about member switches*

```
> show switch detail
Date 20XX/10/26 11:38:56 UTC
Stack status : Enable          Switch No : 1
System MAC Address : 0012.e220.5101
No  Switch status      Model          Machine ID      Priority  Ver
  1  Master            3650-24t6xw    0012.e220.5101  31       1
  2  Backup (Initializing) 3650-24t6xw    0012.e220.5102  11       1
Port  Status      Neighbor (Port  Model          Machine ID)
1/0/25  Up (Forwarding)  2/0/25  3650-24t6xw    0012.e220.5102
1/0/26  Up (Forwarding)  2/0/26  3650-24t6xw    0012.e220.5102
2/0/25  Up (Forwarding)  1/0/25  3650-24t6xw    0012.e220.5101
2/0/26  Up (Forwarding)  1/0/26  3650-24t6xw    0012.e220.5101
```

## Display items in Example 2

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

Item	Meaning	Displayed detailed information
Stack status	Stack operating status	Enable: Operating in a stack configuration Disable: Operating in a standalone configuration
Switch No	Switch number of the device	1 to 2 The switch number set by the <code>set switch</code> command is displayed.
System MAC Address	Switch MAC address	Device MAC address of the stack If the master has not been determined, - is displayed.
No	Switch number	1 to 2

Item		Meaning	Displayed detailed information
Switch status		Switch state	Master: Master Backup: Backup Init: Initial state The processing details are displayed during the change processing after a switch state transition. (Initializing): Initializing (Switchover): Switching
Model		Member switch model	3830-44xw: AX3830S-44XW 3830-44x4qw: AX3830S-44X4QW 3650-24t6xw: AX3650S-24T6XW 3650-48t4xw: AX3650S-48T4XW 3650-20s6xw: AX3650S-20S6XW
Machine ID		Chassis MAC address	--
Priority		Master selection priority of member switches	1 to 31
Ver		Stack functionality version	1
Port		Stack port number	Switch number/NIF number/port number
Status		Link status of the stack port. The frame transfer status is displayed in parentheses.	Up (Forwarding): Indicates that the port status is Up and frame transfer is available. Down: Indicates that the port status is Down, or the port status is Up and frame transfer is unavailable (the neighboring device is not a member switch).
Neighbor	Port	Stack port number of the neighboring member switch	Switch number/NIF number/port number -: Unknown
	Model	Model of the neighboring member switch	3830-44xw: AX3830S-44XW 3830-44x4qw: AX3830S-44X4QW 3650-24t6xw: AX3650S-24T6XW 3650-48t4xw: AX3650S-48T4XW 3650-20s6xw: AX3650S-20S6XW -: Unknown
	Machine ID	Chassis MAC address of the neighboring member switch	-: Unknown

### Impact on communication

None

### Response messages

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

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

### Notes

None

---

## set switch

---

Changes the number of a switch that configures a stack.

To enable the change, restart the switch.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

<switch no.>

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

### Operation when a stack configuration is used

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

### Example 1

*Figure 5-4: Changing the switch number*

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

### Display items

None

### Impact on communication

None

### Response messages

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

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

### Notes

1. The new switch number takes effect after the device is restarted.
2. If you restart the device without setting the `stack enable` configuration command, the switch number is changed to 1. Note that the switch number before the change is displayed in the log message logged during restart of the device that causes the switch number change.

---

## dump stack

---

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

### Syntax

`dump stack`

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

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

### Example

*Figure 5-5: Obtaining a stack management program dump*

```
> dump stack
>
```

### Display items

None

### Impact on communication

None

### Response messages

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

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

### Notes

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

Storage directory: `/usr/var/stack/`

File name: `stack_dump.gz`

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



## Chapter

---

# 6. Login Security and RADIUS or TACACS+

---

- adduser
- rmuser
- password
- clear password
- show sessions (who)
- show whoami (who am i)
- killuser
- show accounting
- clear accounting
- restart accounting
- dump protocols accounting

---

## adduser

---

Adds an account for a new login user.

### Syntax

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

### Input mode

Administrator mode

### Parameters

<user name>

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

no-flash

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

Operation when this parameter is omitted:

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

### Operation when a stack configuration is used

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

### Example

1. Add a new login user user1.  
# adduser user1

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

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

2. Next, enter a password.  
Changing local password for newuser.  
New password:\*\*\*\*\*

If the password configuration is interrupted (press the **Ctrl + D** keys or press only the **Enter** key) at this time, a new login user with no password is created.

3. Re-type the password for confirmation.  
Retype new password:\*\*\*\*\*  
# quit  
>

### Display items

None

### Impact on communication

None

## Response messages

Table 6-1: List of response messages for the adduser command

Message	Description
<user name> is not a valid login name	This user name cannot be used.
already a '<user name>' user	The specified user has already been registered. <user name>: User name
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
can't lock <file name> : <reason>	The addition of a user was canceled because the password file was locked. Re-execute the command. <file name>: Password file name <reason>: Detailed information
Can't synchronize accounts to backup switch or transit switch.	Synchronization of the account to the backup switch or the transit switch failed. Re-execute the command.
Mismatch; try again.	The new password and the re-entered password are not the same. Re-enter the password.
no changes made	The registration of the specified user was canceled. Re-execute the command.
Now another user is executing user account command, please try again.	Another user is executing a user account related command. Re-execute the command after the related command completes.
Password unchanged. /etc/master.passwd: unchanged	The password change was canceled.
Permission denied	The password change is not allowed.
Please don't use an all-lower case password. Unusual capitalization, control characters or digits are suggested.	We recommend that upper-case alphabetic characters, symbols, or numbers be used in addition to lower-case alphabetic characters.
Please enter a longer password.	Enter at least six characters for a password.
synchronize accounts to backup switch or transit switch.	Synchronization of the account to the backup switch or the transit switch will start.

## Notes

1. To abort password configuration, press the **Ctrl + D** keys. If the **Ctrl + D** keys are pressed while retyping, *Mismatch; try again.* appears, and then the input prompt reappears. If this happens, press the **Ctrl + D** keys again. If password configuration is aborted, a new login user with no password is created.
2. A login user name that has already been registered cannot be added. In addition, names such as **root** or **admin** cannot be used as a login user name because they are used inside the Switch.
3. We recommend that you use at least six characters for a password. If fewer than six characters are entered, an error is displayed. Note, however, that if you re-enter the same password, it will be accepted. Also, the maximum number of characters that can be used for a password is 128. If you enter 129 or more characters, only the first 128 characters are registered for the password. We recommend that you use upper-case alphabetic characters, numbers, and symbols in addition to lower-case alphabetic characters. If a password consists of only lower-case alphabetic characters, an error is displayed. Note, however, that if you re-enter the same password, it will be accepted.
4. If an account is added with the `no-flash` parameter specified, do not create any files under the home directory of the added account.

5. If you create an account with the `adduser` command and specify the `no-flash` parameter then configure settings using the `set exec-timeout`, `set terminal help`, or `set terminal pager` commands, they revert to the default settings, and logs of commands of the history functionality are cleared when the device is restarted.
6. When a stack is configured, synchronization of the account might take a long time.

---

## rmuser

---

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

### Syntax

```
rmuser <user name>
```

### Input mode

Administrator mode

### Parameters

*<user name>*

Specifies a login user name registered in the password file.

### Operation when a stack configuration is used

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

### Example

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

If `y` is entered, the account is deleted.

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

### Display items

None

### Impact on communication

None

### Response messages

Table 6-2: List of response messages for the `rmuser` command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
can't lock <file name> : <reason>	The deletion of a user was canceled because the password file was locked. Re-execute the command. <file name>: Password file name <reason>: Detailed information
Can't synchronize accounts to backup switch or transit switch.	Synchronization of the account to the backup switch or the transit switch failed. Re-execute the command.
Last user.	The last user cannot be deleted.
no changes made	The deletion of the specified user was canceled. Re-execute the command.
No such user '<user name>'.	The specified user has not been registered. <user name>: User name

Message	Description
Now another user is executing user account command, please try again.	Another use is executing a user account related command. Re-execute the command after the related command completes.
Permission denied	The specified user could not be deleted.
Remove myself?	The account of the user executing this command cannot be deleted.
synchronize accounts to backup switch or transit switch.	Synchronization of the account to the backup switch or the transit switch will start.

## Notes

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

---

## password

---

Only the password of the login user can be changed. The operation differs depending on the command input mode as follows:

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

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

*<user name>*

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

Operation when this parameter is omitted:

Changes the password of the current login user.

enable-mode

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

### Operation when a stack configuration is used

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

### Example

- Change the password of the login user name operator.  

```
# password operator
Changing local password for operator
New password:***** ... Enter a new password.
Retype new password:***** ... Re-enter the new password.
#
```
- Change the password of the current login user (with no parameters).  

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

### Display items

None

### Impact on communication

None

## Response messages

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

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't synchronize accounts to backup switch or transit switch.	Synchronization of the account to the backup switch or the transit switch failed. Re-execute the command.
Mismatch; try again.	The new password and the re-entered password are not the same. Re-enter both passwords.
Now another user is executing user account command, please try again.	Another user is executing a user account related command. Re-execute the command after the related command completes.
Password unchanged./etc/master.passwd: unchanged	The password change was canceled.
Permission denied.	The password change is not allowed.
Please don't use an all-lower case password.Unusual capitalization, control characters or digits are suggested.	We recommend that upper-case alphabetic characters, symbols, or numbers be used in addition to lower-case alphabetic characters.
Please enter a longer password.	Enter at least six characters for a password.
synchronize accounts to backup switch or transit switch.	Synchronization of the account to the backup switch or the transit switch will start.
unknown user <user name>	The specified user has not been registered. <user name>: User name

## Notes

1. The password of other login users cannot be changed in modes other than administrator mode. When the password of other login users is changed, the prompt (Old password:) is not displayed. Start the procedure by entering the new password at the prompt (New password:).
2. To abort password configuration, press the **Ctrl + D** keys. If the **Ctrl + D** keys are pressed while retyping, the input prompt (Mismatch; try again.) is displayed. If this happens, press the **Ctrl + D** keys again.
3. We recommend that you use at least six characters for a password. If fewer than six characters are entered, an error is displayed. Note, however, that if you re-enter the same password, it will be accepted. Also, the maximum number of characters that can be used for a password is 128. If you enter 129 or more characters, only the first 128 characters are registered for the password. We recommend that you use upper-case alphabetic characters, numbers, and symbols in addition to lower-case alphabetic characters. If a password consists of only lower-case alphabetic characters, an error is displayed. Note, however, that if you re-enter the same password, it will be accepted.
4. When a stack is configured, synchronization of the account might take a long time.

---

## clear password

---

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

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

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

<user name>

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

Operation when this parameter is omitted:

Clears the password of the current login user.

enable-mode

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

### Operation when a stack configuration is used

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

### Example

Clear the password of the current login user.

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

### Display items

None

### Impact on communication

None

### Response messages

Table 6-4: List of response messages for the clear password command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't synchronize accounts to backup switch or transit switch.	Synchronization of the account to the backup switch or the transit switch failed. Re-execute the command.

Message	Description
Now another user is executing user account command, please try again.	Another use is executing a user account related command. Re-execute the command after the related command completes.
Permission denied	The password of the specified user could not be changed.
synchronize accounts to backup switch or transit switch.	Synchronization of the account to the backup switch or the transit switch will start.
unknown user <user name>	The specified user has not been registered. <user name>: User name

## Notes

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

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

---

## show sessions (who)

---

Displays the users currently logged in to the Switch.

### Syntax

```
show sessions
who
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

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

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

### Example

Display the users currently logged in to the Switch.

```
> show sessions
Date 20XX/06/16 12:00:00 UTC
kikuchi console ----- 0 Jun 15 14:16 <--1
shimizu tty0 admin 2 Jun 15 14:16 (192.168.0.1) <--2
shimizu tty1 ----- 3 Jun 15 14:17 (192.168.0.1) <--3
tanaka tty2 ----- 4 Jun 15 15:52 (192.168.0.1 VRF:2) <--4
>
```

1. Login from CONSOLE
2. Login from a remote operation terminal (administrator mode)
3. Login from a remote operation terminal
4. Login from a remote operation terminal (VRF 2) [OS-L3SA]

### Display items

The following information is displayed:

- Login user name
- tty name
- Command input mode: `admin` (administrator mode) or `-----` (user mode)
- Login number
- Date and time
- Terminal IP address (displayed only when the user has logged in from a remote operation terminal)
- VRF ID (displayed only when the user has logged in from VRF) [OS-L3SA]

### Impact on communication

None

### Response messages

None

## Notes

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

---

## show whoami (who am i)

---

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

### Syntax

```
show whoami
who am i
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

### Example

Displays the login name of the current login user.

```
> show whoami
Date 20XX/01/07 12:00:00 UTC
shimizu tty0 ----- 2 Jan 6 14:17 (192.168.0.1)
>
```

Displays the login name of the current login user when the user logged in from VRF2. [OS-L3SA]

```
> show whoami
Date 20XX/06/16 12:00:00 UTC
tanaka tty2 ----- 4 Jun 15 15:52 (192.168.0.1 VRF:2)
>
```

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

#### ■ When staff1 is authenticated by a TACACS+ server

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

```
> show whoami
Date 20XX/01/07 12:00:00 UTC
staff1 tty0 ----- 2 Jan 6 14:17 (192.168.0.1)

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

#### ■ When staff2 is authenticated by the RADIUS server

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

```
> show whoami
Date 20XX/01/07 12:00:00 UTC
staff2 tty0 ----- 2 Jan 6 14:17 (192.168.0.1)
```

```

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

```

■ When staff3 is authenticated by local password authentication

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

```

> show whoami
Date 20XX/01/07 12:00:00 UTC
staff3 tty0 ----- 2 Jan 6 14:17 (192.168.0.1)

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

```

## Display items

Table 6-5: Information displayed by the show whoami command

Item		Displayed information
User information		Displays information about the user who executed the command. <ul style="list-style-type: none"> <li>• Login user name</li> <li>• tty name</li> <li>• Command input mode: admin (administrator mode) or ----- (user mode)</li> <li>• Login number</li> <li>• Date and time</li> <li>• Terminal IP address (displayed only when the user has logged in from a remote operation terminal)</li> <li>• VRF ID (displayed only when the user has logged in from VRF) [OS-L3SA]</li> </ul>
Home-directory		Displays the home directory.
Authentication		Displays the authentication type (RADIUS, TACACS+, or LOCAL). Displays the address authentication information of the remote authentication server only when the user is authenticated by RADIUS or TACACS+.
Class	Class	Displays a class name. If no class is set, ----- is displayed. If the invalid class name is set, a comment (Invalid Class) is displayed next to the class name. If the invalid class name includes characters that cannot be displayed such as non-ASCII characters, they are replaced by " ." in the display.
	Allow	If a class is set, the contents of the "allow" command list of the class are displayed. If the class is root, commands are not denied, and the message (Command unlimited) is displayed. If an "allow" command list is not specified for the applicable class, ----- is displayed.
	Deny	If a class is set, the contents of the "deny" command list of the class are displayed. If the class is root, a command "deny" list is not possible. The message (Command unlimited) is displayed. If a "deny" command list is not specified for the applicable class, ----- is displayed.

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

### Impact on communication

None

### Response messages

None

### Notes

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

---

## killuser

---

Forcibly logs out a login user.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

<login no.>

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

### Operation when a stack configuration is used

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

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

### Example 1

Use the `show sessions` command to check the login number of a user to be logged out. Execute the `killuser` command with the login number specified.

```
> show sessions
Date 20XX/01/07 12:00:00 UTC
kikuchi console ----- 0#   Jan  6 14:16
shimizu tty0     admin   2#   Jan  6 14:16 (192.168.0.1) <-- (Note 1)
shimizu tty1     ----- 3#   Jan  6 14:17 (192.168.0.1)
kikuchi tty2     ----- 4#   Jan  6 14:20 (localhost)
>
> killuser 2
```

#: Login number

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

### Example 2

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

Execute the `show sessions` command by using `remote command` to check the login number of the user to be logged out. Execute this command using `remote command`.

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

#: Login number

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

### Display items

None

## Impact on communication

None

## Response messages

Table 6-6: List of response messages for the killuser command

Message	Description
different user.	Users other than that of the same account cannot be forcibly logged out. For details, see item 3 in Notes. Alternatively, the previously login user is currently logging out, and cannot be forced to log out. Wait for 10 or more seconds, and then try again.
invalid Login-No: <login no.>	The specified login number is invalid. <login no.>: Specified login number
kill myself?	The user who is executing this command cannot forcibly log themselves out.
no user(UserName)	The user does not exist.

## Notes

1. This command is prepared for forcibly logging out a login user who remains logged in due to a network failure or terminal failure occurring while the user is logged in. Use the `logout` command or `exit` command for normal logout. Do not use this command except in an emergency. Even if a user remains logged in, the user will eventually be logged out by the auto-logout functionality.
2. The user who is executing this command cannot specify himself as the forced logout target. If such a user is specified as described above, an error occurs. However, a user can specify himself as logout target when logged in from the console.
3. Only users who have the same account as the user who is executing this command can be forcibly logged out by using this command and specifying the applicable login number. In the above example 2, shimizu with login number 3 can forcibly log out shimizu with login number 2, but not kikuchi with login number 4. However, when this command is executed from the console, users with different accounts can be forcibly logged out.

Also, if the `remote command` command is used to execute this command for the backup switch, users with different accounts can be forcibly logged out.

4. If a failure occurs, such as a cable disconnection when the command execution results are being displayed, a forced logout might not be able to be performed. In this case, a forced logout is performed after the recovery from the failure. If the failure recovery is not successful, a forced logout is performed after the TCP protocol times out. Although the timeout period of the TCP protocol varies depending on the line speed or line quality, the protocol usually times out after 10 minutes.

---

## show accounting

---

Displays accounting information.

### Syntax

```
show accounting
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

The command can display information only for the master switch.

### Example

*Figure 6-1: Display of accounting information*

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

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

  InQueue:          10
  Discard :          5

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

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

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

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

  InQueue:        512 (Congestion)
  Discard :       55000

[TACACS+]
Host: 192.168.111.112
  Event Counts:        500          (Timeout: 0)
  Request Information
    Success           :          0
    Failure           :          0
    Invalid           :          0
    Timeout           :          0
    Retransmit        :          0
    Response Information
```

Send	:	500	Success	:	400
Communicate Error	:	0	Failure	:	100
Timeout	:	0	Invalid	:	0

## Display items

Table 6-7: Display items for the accounting information

Item	Meaning	Displayed information
Since	Statistics start time	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second
Event	Displays the status of accounting events.	
Login	Number of login events	Displays - when target event accounting is not set in the system configuration.
Logout	Number of logout events	Displays - when target event accounting is not set in the system configuration.
Command	Number of execution events for operation commands	Displays - when target event accounting is not set in the system configuration.
Config	Number of execution events for configuration commands	Displays - when target event accounting is not set in the system configuration.
Total	Total number of accounting events	Indicates the total number of the above events.
InQueue	Number of transmission queue events	<ul style="list-style-type: none"> <li>Displays the number of transmission queue accounting events when a large volume of accounting events to be transmitted occurs.</li> <li>Displays (Congestion) when a device log is output and a congested state occurs.</li> </ul>
Discard	Number of discarded events	When the congesting of an accounting event transmission occurs, the number of discarded events is counted.
[RADIUS]	<ul style="list-style-type: none"> <li>This item is displayed when a RADIUS server is set to be used by the system accounting configuration.</li> <li>The following accounting statistics are displayed for each RADIUS server. (Not configured) is displayed in the following items when the RADIUS server configuration is not set or all RADIUS servers are for logon authentication only, not accounting.</li> </ul>	
Timeout	Reply timeout time	1 to 30 (seconds)
Retransmit	Number of re-transmissions	0 to 15 (times)
Host	Target host name or IP address	It is displayed in order of server priority.
Event Counts	Number of accounting events	Displays the number of events to be reported to the target RADIUS server.
Request Information	Displays accounting request information.	
Send	Number of accounting request transmissions	<ul style="list-style-type: none"> <li>The number of times the Switch sent accounting requests to servers.</li> <li>It is counted as a response timeout (Timeout), but not as a transmission error (Communicate Error).</li> </ul>
Communicate Error	Number of accounting request transmission errors	This item is counted when communication to servers is not successful, such as when the address corresponding to the host name is not found, or a route to the server does not exist.
Timeout	Number of accounting response timeouts	This item is counted when a response from a server times out.

Item	Meaning	Displayed information
Response Information	Displays accounting response information.	
Success	Number of successful accounting responses	This item is counted when an accounting response is received from a server.
Failure	Number of failed accounting responses	This item is counted when a response other than an accounting response is received from a server.
Invalid	Number of invalid message responses	This item is counted when an invalid message is received from a server.
[TACACS+]	<ul style="list-style-type: none"> <li>This item is displayed when a TACACS+ server is set to be used by the system accounting configuration.</li> <li>The following accounting statistics are displayed for each TACACS+ server. A term (Not configured) is displayed in the following items when the TACACS+ server configuration is not set or all TACACS+ servers are for logon authentication only, not accounting.</li> </ul>	
Timeout	Reply timeout time	1 to 30 (seconds)
Host	Target host name or IP address	It is displayed in order of server priority.
Event Counts	Number of accounting events	Displays the number of events to be reported to the target TACACS+ server.
Request Information	Displays accounting request information.	
Send	Number of accounting request transmissions	<ul style="list-style-type: none"> <li>The number of times the Switch sent accounting requests to servers.</li> <li>It is not counted as a response timeout (Timeout) or as a transmission error (Communicate Error).</li> </ul>
Communicate Error	Number of connection errors	This item is counted when communication to servers is not successful, such as when the address corresponding to the host name is not found, or a route to the server does not exist.
Timeout	Number of timeouts of accounting connections and responses	This item is counted when a connection or communication to a server times out.
Response Information	Displays accounting response information.	
Success	Number of successful accounting responses	This item is counted when an accounting success is received from a server.
Failure	Number of failed accounting responses	This item is counted when an accounting failure is received from a server.
Invalid	Number of invalid message responses	This item is counted when an invalid message is received from a server.

## Impact on communication

None

## Response messages

Table 6-8: List of response messages for the show accounting command

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

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to accounting program.	Communication with the accounting program failed. Make sure the accounting settings have been set. If this error occurs frequently, use the <code>restart accounting</code> command to restart the accounting program.

**Notes**

None

---

## clear accounting

---

Clears accounting statistics.

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

### Syntax

```
clear accounting
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

The command can clear information only from the master switch.

### Example

*Figure 6-2: Clearing accounting information*

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

### Display items

None

### Impact on communication

None

### Response messages

*Table 6-9: List of response messages for the clear accounting command*

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to accounting program.	Communication with the accounting program failed. Re-execute the command. If this error occurs frequently, use the <code>restart accounting</code> command to restart the accounting program.

### Notes

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

---

## restart accounting

---

Restarts the accounting program.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

-f

Restarts the accounting program without outputting a restart confirmation message.

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 accounting program after outputting a restart confirmation message.

### Operation when a stack configuration is used

The command can be executed only on the master switch.

### Example

*Figure 6-3: Example of the restart of the accounting program*

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

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

### Display items

None

### Impact on communication

None

### Response messages

*Table 6-10: List of response messages for the restart accounting command*

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

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to accounting program.	Communication with the accounting program failed. Re-execute the command. If this error occurs frequently, use the <code>restart accounting</code> command to restart the accounting program.

## Notes

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

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

Core file name: `acctd.core`

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

---

## dump protocols accounting

---

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

### Syntax

```
dump protocols accounting
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

The command can be executed only on the master switch.

### Example

*Figure 6-4: Example of executing accounting dump*

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

### Display items

None

### Impact on communication

None

### Response messages

*Table 6-11: List of response messages for the dump protocols accounting command*

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to accounting program.	Communication with the accounting program failed. Re-execute the command. If this error occurs frequently, use the <code>restart accounting</code> command to restart the accounting program.
File open error.	An attempt to open or access a dump file failed.

### Notes

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

Storage directory: `/usr/var/accounting/`

File name: `accounting_dump.gz`

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



## Chapter

---

# 7. Time Settings and NTP

---

show clock  
set clock  
show ntp associations  
restart ntp

---

## show clock

---

Displays the current date and time.

### Syntax

`show clock`

### Input mode

User mode and administrator mode

### Parameters

None

Displays the current time.

### Operation when a stack configuration is used

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

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

### Example

Enter the following command to display the current time.

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

### Display items

None

### Impact on communication

None

### Response messages

None

### Notes

None

---

## set clock

---

Displays and sets the date and time.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

yy

Specifies the last two digits of the year. The specifiable values are from 69 to 99 (for the 1900s) and from 00 to 38 (for the 2000s). (For example, 00 means the year 2000.)

mm

Specifies the month in the range 1 to 12.

dd

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

hh

Specifies the hour in the range 0 to 23.

mm

Specifies the minute in the range 0 to 59.

ss

Specifies the second in the range 0 to 59.

Operation when all parameters are omitted:

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

### Operation when a stack configuration is used

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

### Example

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

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

### Impact on communication

Use of Web authentication or MAC authentication might affect communication. For details, see *5.4.1 Notes on changing the Switch configuration and status* in the manual *Configuration Guide Vol. 2 For Version 11.10*.

## Response messages

*Table 7-1:* List of response messages for the set clock command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
illegal time format.	The input format of the time is incorrect.
illegal time.	The date and time values are outside the valid range. Set values within the range.
invalid day of month supplied.	The day value is outside the valid range. Set a value within the range.
invalid hour supplied.	The hour value is outside the valid range. Set a value within the range.
invalid minute supplied.	The minute value is outside the valid range. Set a value within the range.
invalid month supplied.	The month value is outside the valid range. Set a value within the range.
invalid second supplied.	The second value is outside the valid range. Set a value within the range.

## Notes

- Statistics on CPU usage collected by the Switch will be cleared to zero at the following timing:
  - In a standalone configuration, the information is cleared to zero when the time is changed.
  - In a stack configuration, the information in the master switch is cleared to zero when the time is changed. For member switches other than the master switch, if the time difference between before and after the change is five seconds or more, the CPU usage information collected for each second is cleared to zero.
- The specifiable values are from 1969/01/01 00:00:00 to 2038/01/19 03:14:07.

---

## show ntp associations

---

Displays the activity status of the connected NTP server.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

{vrf <vrf id> | global} [OS-L3SA]

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

Operation when this parameter is omitted:

Displays the activity status of the NTP server of all VRFs including the global network.

### Operation when a stack configuration is used

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

### Example 1

Figure 7-1: Display of the activity status of an NTP server

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

### Example 2

Figure 7-2: Display of the activity status of the NTP servers of all VRFs [OS-L3SA]

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

Figure 7-3: Display of the activity status of the NTP server of the specified VRF [OS-L3SA]

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

## Display items

Table 7-2: Information displayed by the show ntp associations command

Item	Meaning
VRF [OS-L3SA]	VRF ID
remote	Indicates the name of the time server host. If a local time server is set, LOCAL (1) is displayed. [Meaning of the code at the beginning of the host name] " ": A host that is treated as invalid because the activity cannot be checked, or the stratum value is high. +: A host remaining as an available choice. #: A selected synchronized host. However, the upper limit of the distance is exceeded. *: A selected synchronized host. Other symbols: Hosts that are found to be invalid by test results.
refid	The destination host to which the time server is synchronized.
st	The stratum value of the host
t	Indicates a server type. [Meaning of displayed server types] u: Unicast server b: Broadcast server l: Local server
when	When the Switch is connected to the host, this item indicates the time elapsed since the last packet was received from the host. If the Switch is disconnected from the host, this item indicates the time elapsed since the host was last synchronized. - is displayed when the elapsed time is 0 seconds or less. [Meaning of the symbol at the end of a displayed number] m: In minutes (for 2049 seconds or more) h: In hours (for 301 minutes or more) d: In days (for 97 hours or more) If only a number is displayed with no symbol, the displayed value is in seconds.
poll	Indicates the host polling interval (in seconds).
reach	Indicates reachability in octal notation.
delay	Indicates the total both-way delay time from the reference source to the synchronized subnet (in milliseconds).
offset	Indicates the offset value (in milliseconds).
disp	Indicates the latency (variation) in the time from the reference source to the synchronized subnet (in milliseconds).

## Impact on communication

None

## Response messages

Table 7-3: List of response messages for the show ntp associations command

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

**Notes**

None

---

## restart ntp

---

Restarts the local NTP server.

### Syntax

```
restart ntp
```

### Input mode

Administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

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

### Example

*Figure 7-4: Restarting the NTP server*

```
# restart ntp
#
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 7-4: List of response messages for the restart ntp command*

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

### Notes

None

## Chapter

---

# 8. Utilities

---

diff  
grep  
more  
less  
tail  
hexdump

---

## diff

---

Compares two specified files and displays their differences.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

*<option>*

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

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

Operation when this parameter is omitted:

Compares specified files, distinguishing between upper-case and lower-case letters.

*<file name1> <file name2>*

Specifies the names of files to be compared.

*<directory1> <directory2>*

Specifies the names of directories to be compared.

### Operation when a stack configuration is used

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

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

### Example and display items

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

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

### Impact on communication

None

### Response messages

None

**Notes**

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

---

## grep

---

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

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

*<option>*

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

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

Operation when this parameter is omitted:

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

*<pattern>*

Specifies the search string.

*<file name>*

Specifies the file name.

Operation when this parameter is omitted:

Searches for specified *<pattern>* from the standard input.

Operation when all parameters are omitted:

Searches for specified *<pattern>* from the standard input.

### Operation when a stack configuration is used

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

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

### Example and display items

None

### Impact on communication

None

### Response messages

None

### Notes

None

---

## more

---

Displays one page of the contents of a specified file.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

*<option>*

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

Operation when this parameter is omitted:

Line numbers are not displayed.

*<file name>*

Specifies the file name.

### Operation when a stack configuration is used

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

### Example and display items

None

### Impact on communication

None

### Response messages

None

### Notes

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

---

## less

---

Displays one page of the contents of a specified file.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

*<option>*

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

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

Operation when this parameter is omitted:

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

*<file name>*

Specifies the file name.

### Operation when a stack configuration is used

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

### Example and display items

None

### Impact on communication

None

### Response messages

None

### Notes

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

---

## tail

---

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

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

*<option>*

-n: Outputs n lines from the end.

Operation when this parameter is omitted:

Outputs 10 lines from the end.

*<file name>*

Specifies the file name.

### Operation when a stack configuration is used

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

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

### Example and display items

None

### Impact on communication

None

### Response messages

None

### Notes

None

---

## hexdump

---

Displays a hexadecimal dump.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

*<option>*

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

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

Operation when this parameter is omitted:

Displays a dump in hexadecimal notation every one byte.

*<file name>*

Specifies the file name.

### Operation when a stack configuration is used

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

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

### Example and display items

None

### Impact on communication

None

### Response messages

None

### Notes

None

## Chapter

---

# 9. Checking Software Versions and Device Statuses

---

show version  
show system  
clear control-counter  
show environment  
reload  
show tech-support  
show tcpdump (tcpdump)  
backup  
restore

---

## show version

---

Displays information about the Switch software and the board installed.

### Syntax

```
show version [software]
```

### Input mode

User mode and administrator mode

### Parameters

software

Only the software information is displayed.

Operation when this parameter is omitted:

Displays information about the Switch software and the boards installed.

### Operation when a stack configuration is used

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

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

### Example

*Figure 9-1:* Example of displaying only the software version

```
> show version software
Date 20XX/12/10 15:11:20 UTC
S/W: OS-L3SA Ver. 11.5
>
```

*Figure 9-2:* Example of displaying information about the Switch software and the boards installed

```
> show version
Date 20XX/12/10 17:52:58 UTC
Model: AX3650S-24T6XW
S/W: OS-L3SA Ver. 11.5
H/W: Main board
      AX-3650-24T6XW-A [TA03FA24T6XWS406006W005:80C50021:503:11B636]
Power slot 1 PS-M(AC)
      AX-F2430-PSA03 [TA0PSA030000C1103041006]
Power slot 2 PS-M(AC)
      AX-F2430-PSA03 [TA0PSA030000C1103041006]
Fan slot      FAN-M
      AX-F2430-FAN03 [TA0FAN030000C140306W011]
>
```

### Display items

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

Item	Display format	Meaning
Model	AX3830S-44XW	AX3830S-44XW (L3 switch) <ul style="list-style-type: none"> <li>Redundant power model</li> <li>Gigabit Ethernet 4 (10/100/1000BASE-T)</li> <li>10 gigabit Ethernet 44 (10GBASE-R (SFP+) or 1000BASE-X (SFP))</li> </ul>

Item	Display format	Meaning
	AX3830S-44X4QW	AX3830S-44X4QW (L3 switch) <ul style="list-style-type: none"> <li>Redundant power model</li> <li>Gigabit Ethernet 4 (10/100/1000BASE-T)</li> <li>10 gigabit Ethernet 44 (10GBASE-R (SFP+) or 1000BASE-X (SFP))</li> <li>40 gigabit Ethernet 4 (40GBASE-R (QSFP+))</li> </ul>
	AX3650S-24T6XW	AX3650S-24T6XW (L3 switch) <ul style="list-style-type: none"> <li>Redundant power model</li> <li>Gigabit Ethernet 24 (10/100/1000BASE-T)</li> <li>10 gigabit Ethernet 6 (10GBASE-R (SFP+) or 1000BASE-X (SFP))</li> </ul>
	AX3650S-20S6XW	AX3650S-20S6XW (L3 switch) <ul style="list-style-type: none"> <li>Redundant power model</li> <li>Gigabit Ethernet 24 (10/100/1000BASE-T 4 + 1000BASE-X (SFP) 20)</li> <li>10 gigabit Ethernet 6 (10GBASE-R (SFP+) or 1000BASE-X (SFP))</li> </ul>
	AX3650S-48T4XW	AX3650S-48T4XW (L3 switch) <ul style="list-style-type: none"> <li>Redundant power model</li> <li>Gigabit Ethernet 48 (10/100/1000BASE-T)</li> <li>10 gigabit Ethernet 4 (10GBASE-R (SFP+) or 1000BASE-X (SFP))</li> </ul>
S/W <sup>#1</sup>	OS-L3S A-A/ OS-L3S A Ver. vv.v <sup>#2</sup>	L3S advanced software with OSPF, BGP, VRF, and policy-based routing
	OS-L3S L-A/ OS-L3S L Ver. vv.v	L3S light software without OSPF, BGP, VRF, or policy-based routing
H/W <sup>#3</sup>		
Main board		
	AX-3830-44XW-A[ssss...ssss]	AX3830S-44XW (L3 switch) <ul style="list-style-type: none"> <li>Redundant power model</li> <li>Gigabit Ethernet 4 (10/100/1000BASE-T)</li> <li>10 gigabit Ethernet 44 (10GBASE-R (SFP+) or 1000BASE-X (SFP))</li> <li>L3S advanced software (with SSH)</li> </ul>
	AX-3830-44XW-L[ssss...ssss]	AX3830S-44XW (L3 switch) <ul style="list-style-type: none"> <li>Redundant power model</li> <li>Gigabit Ethernet 4 (10/100/1000BASE-T)</li> <li>10 gigabit Ethernet 44 (10GBASE-R (SFP+) or 1000BASE-X (SFP))</li> <li>L3S light software (with SSH)</li> </ul>
	AX-3830-44X4QW-A[ssss...ssss]	AX3830S-44X4QW (L3 switch) <ul style="list-style-type: none"> <li>Redundant power model</li> <li>Gigabit Ethernet 4 (10/100/1000BASE-T)</li> <li>10 gigabit Ethernet 44 (10GBASE-R (SFP+) or 1000BASE-X (SFP))</li> <li>40 gigabit Ethernet 4 (40GBASE-R (QSFP+))</li> <li>L3S advanced software (with SSH)</li> </ul>

Item	Display format	Meaning
	AX-3830-44X4 QW-L[ssss....ssss]	AX3830S-44X4QW (L3 switch) <ul style="list-style-type: none"> <li>• Redundant power model</li> <li>• Gigabit Ethernet 4 (10/100/1000BASE-T)</li> <li>• 10 gigabit Ethernet 44 (10GBASE-R (SFP+) or 1000BASE-X (SFP))</li> <li>• 40 gigabit Ethernet 4 (40GBASE-R (QSFP+))</li> <li>• L3S light software (with SSH)</li> </ul>
	AX-3650-24T6XW-A[ssss....ssss]	AX3650S-24T6XW (L3 switch) <ul style="list-style-type: none"> <li>• Redundant power model</li> <li>• Gigabit Ethernet 24 (10/100/1000BASE-T)</li> <li>• 10 gigabit Ethernet 6 (10GBASE-R (SFP+) or 1000BASE-X (SFP))</li> <li>• L3S advanced software (with SSH)</li> </ul>
	AX-3650-20S6XW-A[ssss....ssss]	AX3650S-20S6XW (L3 switch) <ul style="list-style-type: none"> <li>• Redundant power model</li> <li>• Gigabit Ethernet 24 (10/100/1000BASE-T 4 + 1000BASE-X (SFP) 20)</li> <li>• 10 gigabit Ethernet 6 (10GBASE-R (SFP+) or 1000BASE-X (SFP))</li> <li>• L3S advanced software (with SSH)</li> </ul>
	AX-3650-48T4XW-A[ssss....ssss]	AX3650S-48T4XW (L3 switch) <ul style="list-style-type: none"> <li>• Redundant power model</li> <li>• Gigabit Ethernet 48 (10/100/1000BASE-T)</li> <li>• 10 gigabit Ethernet 4 (10GBASE-R (SFP+) or 1000BASE-X (SFP))</li> <li>• L3S advanced software (with SSH)</li> </ul>
	AX-3650-24T6XW-L[ssss....ssss]	AX3650S-24T6XW (L3 switch) <ul style="list-style-type: none"> <li>• Redundant power model</li> <li>• Gigabit Ethernet 24 (10/100/1000BASE-T)</li> <li>• 10 gigabit Ethernet 6 (10GBASE-R (SFP+) or 1000BASE-X (SFP))</li> <li>• L3S light software (with SSH)</li> </ul>
	AX-3650-20S6XW-L[ssss....ssss]	AX3650S-20S6XW (L3 switch) <ul style="list-style-type: none"> <li>• Redundant power model</li> <li>• Gigabit Ethernet 24 (10/100/1000BASE-T 4 + 1000BASE-X (SFP) 20)</li> <li>• 10 gigabit Ethernet 6 (10GBASE-R (SFP+) or 1000BASE-X (SFP))</li> <li>• L3S light software (with SSH)</li> </ul>
	AX-3650-48T4XW-L[ssss....ssss]	AX3650S-48T4XW (L3 switch) <ul style="list-style-type: none"> <li>• Redundant power model</li> <li>• Gigabit Ethernet 48 (10/100/1000BASE-T)</li> <li>• 10 gigabit Ethernet 4 (10GBASE-R (SFP+) or 1000BASE-X (SFP))</li> <li>• L3S light software (with SSH)</li> </ul>
Power slot		
PS-M <sup>#4</sup>	AX-F2430-PSA03[ssss....ssss]	AC power supply common to AX3830S and AX3650S series switches. 100/200V AC. Designated for front-side air intake and rear-side air exhaust.
	AX-F2430-PSD03[ssss....ssss]	DC power supply common to AX3830S and AX3650S series switches. Designated for front-side air intake and rear-side air exhaust.
	AX-F2430-PSA03R[ssss....ssss]	AC power supply for AX3830S series switches. 100/200V AC. Designated for rear-side air intake and front-side air exhaust.

Item	Display format	Meaning
	AX-F24 30-PSD0 3R[ssss.. ..ssss]	DC power supply for AX3830S series switches. Designated for rear-side air intake and front-side air exhaust.
Fan slot		
FAN-M <sup>#4</sup>	AX-F24 30-FAN 03[ssss.. ..ssss]	Fan unit common to AX3650S series switches. Designated for front-side air intake and rear-side air exhaust.
	AX-F24 30-FAN 04[ssss.. ..ssss]	Fan unit for AX3830S series switches. Designated for front-side air intake and rear-side air exhaust.
	AX-F24 30-FAN 04R[ssss.. ....ssss]	Fan unit for AX3830S series switches. Designated for rear-side air intake and front-side air exhaust.

#1: The variable *v* for display item *s/w* indicates the software version. For encryption software that has been provided with the SSH or SSL functionality via an upgrade, (encryption upgrade) is displayed after the software name.

#2: For L3S software that has been upgraded from the light edition to the advanced edition, (upgrade) is displayed after the software name.

#3: The variable *ssss...ssss* for the display item *H/w* is the switch's serial number.

#4: If a power supply unit or a fan unit that is not supported by software is installed, -----  
[ssss...ssss] is displayed.

## Impact on communication

None

## Response messages

Table 9-2: List of response messages for the show version command

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

## Notes

None

---

## show system

---

Displays operating status.

### Syntax

show system

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

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

### Example 1

*Figure 9-3:* Example showing the result of executing the show system command [AX3800S]

```
> show system
Date 20XX /09/14 09:13:21 UTC
System: AX3830S-44XW, OS-L3SA Ver. 11.7
Node : Name=
      Contact=
      Locate=
      Elapsed time : 00:05:16
      LED Brightness mode : normal
      Machine ID : 0012.e238.0900
      Power redundancy-mode : check is not executed
      Power slot 1 : active PS-M(AC)
          Fan : active No = Fan1(1) Speed = normal , Direction = F-to-R
          PS : active
          Lamp : Power LED=green , ALM1 LED=light off , ALM2 LED=light off
      Power slot 2 : active PS-M(AC)
          Fan : active No = Fan2(1) Speed = normal , Direction = F-to-R
          PS : active
          Lamp : Power LED=green , ALM1 LED=light off , ALM2 LED=light off
      Fan slot : active FAN-M
          Fan : active No = Fan3(1) , Fan3(2) , Fan3(3) , Fan3(4)
              Speed = normal , Direction = F-to-R
          Lamp : ALM LED=light off
      Main board : active
          Boot : 20XX /09/1 09:08:26 , power on
          Fatal restart : CPU 0 times , SW 0 times
          Lamp : Power LED=green , Status LED1=green
          Board : CPU=PowerPC 800MHz , Memory=1,048,576kB(1024MB)
          Temperature : normal(24degree)
          Flash :
              user area    config area    dump area    area total
              used    77,863kB         76kB        4,178kB      82,117kB
              free    57,917kB        75,330kB       61,212kB     194,459kB
              total 135,780kB        75,406kB       65,390kB     276,576kB
      MC : notconnect
:
:
:
```

*Figure 9-4:* Example showing the result of executing the show system command [AX3650S]

```
> show system
Date 20XX/12/10 15:26:54 UTC
```

```

System: AX3650S-20S6XW, OS-L3SA Ver. 11.5
Node : Name=System Name
      Contact=Contact Address
      Locate=Location
      Elapsed time : 04:32:13
      LED Brightness mode : normal
      Machine ID : 0012.e222.1dd3
      Power redundancy-mode : check is not executed
      Power slot 1 : active PS-M(AC)
        Fan : active No = Fan1(1) Speed = normal
        PS : active
        Lamp : Power LED=green , ALM1 LED=light off , ALM2 LED=light off
      Power slot 2 : active PS-M(AC)
        Fan : active No = Fan2(1) Speed = normal
        PS : active
        Lamp : Power LED=green , ALM1 LED=light off , ALM2 LED=light off
      Fan slot : active FAN-M
        Fan : active No = Fan3(1) , Fan3(2) , Fan3(3) , Fan3(4) Speed = normal
        Lamp : ALM LED=light off
      Main board : active
        Boot : 20XX/12/10 10:54:49 , operation reboot
        Fatal restart : CPU 0 times , SW 0 times
        Lamp : Power LED=green , Status LED1=green
        Board : CPU=PowerPC 800MHz , Memory=1,048,576kB(1024MB)
        Temperature : normal(28degree)
        Flash :
            user area  config area  dump area  area total
        used  114,175kB      74kB      3,306kB    117,555kB
        free   91,381kB    120,597kB    62,084kB    274,062kB
        total 205,556kB    120,671kB    65,390kB    391,617kB
      MC : notconnect
:
:
:

```

## Display items in Example 1

Table 9-3: Information displayed by the show system command

Item	Displayed information	Displayed detailed information
System	Device model	Device model
	Software information	Software type, version
Node	Node information	--
Name	System name	Identification name set by the user
Contact	Contact information	Contact information set by the user
Locate	Installation location	Installation location set by the user
Elapsed time	Elapsed time	The time elapsed since the switch started
LED Brightness mode	LED brightness status	normal: Normal brightness economy: Power saving brightness off: The LED is off. auto (xxx) :Automatic brightness adjustment xxx: normal, economy, or off
Machine ID	Chassis MAC address	--
Power redundancy-mode	Power mode	check is executed: A check of whether the power is in a redundant configuration is performed. check is not executed: A check of whether the power is in a redundant configuration is not performed.

Item	Displayed information	Displayed detailed information
Power slot	Power supply unit slots	--
	Power supply unit slot status	active: Supplied normally fault: Failed notconnect: Not installed
	Power supply type <sup>#1</sup>	PS-M (AC): AC power supply unit PS-M (DC): DC power supply unit
Fan	Fan operating status <sup>#2</sup>	The numbers of active fans
Speed	The rotational speed of the fan	normal: Normal rotation high: High-speed rotation stop: Stopped rotation
Direction [AX3800S]	Direction of the fan	F-to-R: Front-side air intake and rear-side air exhaust R-to-F: Rear-side air intake and front-side air exhaust
	Fan direction mismatch information <sup>#3</sup>	(mismatch): The direction does not match the direction of the fan unit.
PS <sup>#1</sup>	Status of the input power supply unit	active: Supplied normally fault: No power is being supplied or there is an abnormal voltage.
Lamp <sup>#1</sup>		
Power LED	LED indicating the power status	light off: The LED is off. green: The LED is on and green.
ALM1 LED	LED indicating the internal power status.	light off: The LED is off. red: The LED is on and red.
ALM2 LED	LED indicating the status of the fans in the power supply unit.	light off: The LED is off. red: The LED is on and red.
Fan slot	Fan unit	--
	Status of the fan unit	active: Supplied normally fault: Failed notconnect: Not installed
	Type of the fan unit	FAN-M: Fan unit
Fan	Fan operating status <sup>#2</sup>	The numbers of active fans
Speed	The rotational speed of the fan	normal: Normal rotation high: High-speed rotation stop: Stopped rotation
Direction [AX3800S]	Direction of the fan	F-to-R: Front-side air intake and rear-side air exhaust R-to-F: Rear-side air intake and front-side air exhaust
Lamp <sup>#1</sup>		
ALM LED	LED indicating the fan status.	light off: The LED is off. red: The LED is on and red.
Main board	Information about the main board	--

Item	Displayed information	Displayed detailed information
	Operating status of the main board	active: Running fault: Failed initialize: Initializing
Boot	Startup time of CPU	Startup time of CPU
	Cause of CPU startup	power on: Startup because the power switch turned on operation reboot: Reboot command fatal: Restart (a fault occurs) default restart: Restart due to a default restart hardware reset: Restart due to the reset button wake on rtc: Activated if the timer runs out while the switch is in a sleep mode wake on reset: Activated if the RESET button is held down while the switch is in a sleep mode
Fatal restart	Number of times a restart is performed due to a failure	CPU: Number of times the CPU restarts due to a failure SW: Number of times the switching processor is restarted due to a failure Note: The CPU value is initialized one hour after the switch is restarted. The SW value is initialized one hour after the switch is restarted or after the first failure occurs.
Lamp	LED indication	light off: The LED is off. green blink: The LED is green and blinking. greenblink 2: The LED is green and blinking 2 (at long interval). green: The LED is on and green. red blink: The LED is red and blinking. red: The LED is on and red.
Board	CPU information	The type and clock of the CPU
	Amount of memory installed on the main board	Amount of memory installed on the main board
Temperature	Intake temperature information	When FAB-04 is mounted on AX3830S series switches: normal: Normal level (higher than -10 degrees Celsius, and lower than 50 degrees Celsius) caution: Caution level (-10 degrees Celsius or lower, or 50 degrees Celsius or higher and lower than 60 degrees Celsius) When FAN-04R is mounted on AX3830S series switches: normal: Normal level (higher than -10 degrees Celsius, and lower than 45 degrees Celsius) caution: Caution level (-10 degrees Celsius or lower, or 45 degrees Celsius or higher and lower than 60 degrees Celsius) For AX3650S series switches: normal: Normal level (higher than -10 degrees Celsius, and lower than 50 degrees Celsius) caution: Caution level (-10 degrees Celsius or lower, or 50 degrees Celsius or higher and lower than 60 degrees Celsius) Note: If the sensor detects a temperature of 60 degrees Celsius or higher, the software stops.

Item	Displayed information	Displayed detailed information
Flash	Used capacity <sup>#4, #5</sup>	Capacity in use by the file system in the internal flash memory user area: Used capacity of the user area config area: Used capacity of the configuration area dump area: Used capacity of the dump area area total: Total of each used capacity of the user area, configuration area, and dump area
	Unused capacity <sup>#4, #5</sup>	Capacity not being used by the file system in the internal flash memory user area: Unused capacity of the user area config area: Unused capacity of the configuration area dump area: Unused capacity of the dump area area total: Total of each unused capacity of the user area, configuration area, and dump area
	Total capacity <sup>#4, #5</sup>	Total of capacity being used and capacity not being used for the file system in the internal flash memory user area: Total of used and unused capacity of the user area config area: Total of used and unused capacity of the configuration area dump area: Total of used and unused capacity of the dump area area total: Total capacity being used and not being used by the file system in the internal flash memory
MC	Memory card status	enabled: The memory card can be accessed. notconnect: The memory card is not installed. write protect: Writing to the memory card is not allowed.
	Type <sup>#4, #5</sup>	Manufacture ID: Memory card manufacturer number
	Used capacity <sup>#4, #5</sup>	Capacity in use in the memory card file system
	Unused capacity <sup>#4, #5</sup>	Capacity not in use in the memory card file system
	Total capacity <sup>#4, #5</sup>	Total of capacity in use and capacity not in use for the memory card file system

#1: This item is displayed when the status of the relevant module is either `active` or `fault`.

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

Table 9-4: Correspondence between fan numbers, operation log data, and chassis

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

Unit	Unit correspondence	
	Command and operation log display	Location on the chassis
	FAN3(2)	On the right in the rear of the fan unit 2
	FAN3(3)	On the right in the rear of the fan unit 3
	FAN3(4)	On the right in the rear of the fan unit 4

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

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

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

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

## Example 2

The following is an example of displayed resource information.

*Figure 9-5: Example of displaying resource Information [AX3800S]*

```
> show system
Date 20XX/3/1 06:35:27 JST
System: AX3830S-44XW, OS-L3SA Ver. 11.6
Node : Name=System Name
:
:
:
Device resources
Current selected swrt_table_resource: l3switch-2
Current selected swrt_multicast_table: On
Current selected unicast multipath number: 8
IP routing entry :
    Unicast : current number=6 , max number=8192
    Multicast : current number=0 , max number=256
    ARP : current number=1 , max number=5120
IPv6 routing entry :
    Unicast : current number=1 , max number=2048
    Multicast : current number=0 , max number=128
    NDP : current number=0 , max number=1024
MAC-Address table entry : current number=7 , max number=131072
System Layer2 Table Mode : auto (mode=1)
Flow detection mode : layer3-1
    Used resources for filter inbound(Used/Max)
        MAC      IPv4      IPv6
        0/ 512   30/ 512     n/a
    Used resources for QoS(Used/Max)
        MAC      IPv4      IPv6
        0/ 128   26/ 128     n/a
    Used resources for UPC(Used/Max)
        MAC      IPv4      IPv6
        0/ 128   26/ 128     n/a
    Used resources for TCP/UDP port detection pattern
    Resources(Used/Max): 3/32
    Source Port
    10-20          : filter/ -
    Destination Port
    1-2            : -/QoS
    65534-65535    : filter/QoS
Flow detection out mode : layer3-1-out
    Used resources for filter outbound(Used/Max)
```

```

MAC      IPv4      IPv6
n/a      0/1024    n/a
>

```

*Figure 9-6: Example of displaying resource Information [AX3650S]*

```

> show system
Date 20XX/3/1 06:35:27 JST
System: AX3650S-48T4XW, OS-L3SA Ver. 11.5
Node : Name=System Name
:
:
:
Device resources
Current selected swrt_table_resource: l3switch-2
Current selected swrt_multicast_table: On
Current selected unicast multipath number: 8
IP routing entry :
  Unicast : current number=6 , max number=8192
  Multicast : current number=0 , max number=1024
  ARP : current number=1 , max number=2048
IPv6 routing entry :
  Unicast : current number=1 , max number=4096
  Multicast : current number=0 , max number=256
  NDP : current number=0 , max number=2048
MAC-Address table entry : current number=7 , max number=32768
System Layer2 Table Mode : auto (mode=1)
Flow detection mode : layer3-1
  Used resources for filter inbound(Used/Max)
    MAC      IPv4      IPv6
Port 0/ 1-24 : 0/512   30/512   n/a
Port 0/25-48 : 0/512   24/512   n/a
Port 0/49-52 : 0/512   24/512   n/a
VLAN        : 0/512   2/512    n/a
  Used resources for QoS(Used/Max)
    MAC      IPv4      IPv6
Port 0/ 1-52 : 0/256   26/256   n/a
VLAN        : 0/256   2/256    n/a
  Used resources for UPC(Used/Max)
    MAC      IPv4      IPv6
Port 0/ 1-52 : 0/256   26/256   n/a
VLAN        : 0/256   2/256    n/a
  Used resources for TCP/UDP port detection pattern
Resources(Used/Max): 4/64
Source Port
  10-20      : filter/  -
Destination Port
  1-2        : -/QoS
  65534-65535 : filter/QoS
Flow detection out mode : layer3-3-out
  Used resources for filter outbound(Used/Max)
    MAC      IPv4      IPv6
Port 0/ 1-52 : n/a     n/a     n/a
VLAN        : 256/256 256/256 256/256
>

```

## Display items in Example 2

*Table 9-5: Information displayed by the show system command (resource information)*

Item	Displayed information	Displayed detailed information
Device resources	Hardware entry information	--
Current selected swrt_table_resource	Hardware table entry pattern	Pattern of the number of entries in the hardware table that is set

Item	Displayed information	Displayed detailed information
		<p>l3switch-1: Information for only IPv4 is displayed.</p> <p>l3switch-2: Information for both IPv4 and IPv6 is displayed.</p> <p>l3switch-3: IPv6 unicast priority mode</p>
Current selected swrt_multicast_table	Whether both IP multicast routing and IGMP/MLD snooping can be used at the same time	<p>On: IP multicast routing and IGMP/MLD snooping can be used at the same time.</p> <p>Off: IP multicast routing and IGMP/MLD snooping cannot be used at the same time.</p>
Current selected unicast multipath number	Maximum number of paths that can be handled as a single unicast route by the Switch	<p>Maximum number of paths that can be set in the hardware table for a unicast route (4, 8, or 16 for AX3800S series switches, and 2, 4, 8, or 16 for AX3650S series switches).</p> <p>Note that when the maximum number of paths is changed by using a configuration command, the change is not immediately applied to the value displayed for this item. To apply the change, restart the switch.</p>
IP routing entry Unicast	Number of IPv4 unicast routing entries set on the hardware	<p>current number: Number of IPv4 unicast routing table entries currently set on the hardware.<sup>#1</sup></p> <p>max number: Maximum number of IPv4 unicast routing table entries that can be set on the hardware.</p> <p>Note: A hyphen (-) is displayed if the status of the main board is Fault.</p>
IP routing entry Multicast	Number of IPv4 multicast routing entries set on the hardware	<p>current number: Number of IPv4 multicast routing table entries currently set on the hardware.</p> <p>max number: Maximum number of IPv4 multicast routing table entries that can be set on the hardware.</p> <p>Note: A hyphen (-) is displayed if the status of the main board is Fault.</p>
IP routing entry ARP	Number of ARP entries set on the hardware	<p>current number: Number of ARP entries currently set on the hardware.</p> <p>max number: Maximum number of ARP entries that can be set on the hardware.</p> <p>Note: A hyphen (-) is displayed if the status of the main board is Fault.</p>
IPv6 routing entry Unicast	Number of IPv6 unicast routing entries set on the hardware	<p>Number of IPv6 unicast routing table entries currently set on the hardware.<sup>#2</sup></p> <p>max number: Maximum number of IPv6 unicast routing table entries that can be set on the hardware.</p> <p>Note: A hyphen (-) is displayed if the status of the main board is Fault.</p>
IPv6 routing entry Multicast	Number of IPv6 multicast routing entries set on the hardware	<p>current number: Number of IPv6 multicast routing table entries currently set on the hardware.</p> <p>max number: Maximum number of IPv6 multicast routing table entries that can be set on the hardware.</p>

Item	Displayed information	Displayed detailed information
		Note: A hyphen (-) is displayed if the status of the main board is Fault.
IPv6 routing entry NDP	Number of NDP entries set on the hardware	<p>current number: Number of NDP entries currently set on the hardware.</p> <p>max number: Maximum number of NDP entries that can be set on the hardware.</p> <p>Note: A hyphen (-) is displayed if the status of the main board is Fault.</p>
MAC-Address table entry	Number of MAC address table entries set on the hardware	<p>current number: Number of MAC address table entries currently set on the hardware.</p> <p>max number: Maximum number of MAC address table entries that can be set on the hardware.</p> <p>Note: A hyphen (-) is displayed if the status of the main board is Fault.</p>
System Layer2 Table Mode	Search method for the Layer 2 hardware table	<p>auto (mode=x): Mode selected automatically.</p> <p>mode=x: Value set by the system l2-table mode configuration command</p> <p>If the mode is not set by using the system l2-table mode configuration command, 0 is displayed for x.</p> <p>(For details, see 8. Device Management in the manual Configuration Command Reference Vol. 1 For Version 11.10.)</p>
Flow detection mode	Receiving-side flow detection mode for the filters and QoS functionality	<p>layer3-1</p> <p>layer3-2</p> <p>layer3-5</p> <p>layer3-6</p> <p>layer3-dhcp-1</p> <p>(For details, see 18. Flow Detection Mode in the manual Configuration Command Reference Vol. 1 For Version 11.10.)</p>
Used resources for filter inbound(Used/Max), and Used resources for filter outbound(Used/Max)	<p>Number of entries currently registered as filter conditions on the target interface, and the maximum number of specifiable entries</p> <p>The number of the setting entries is the total of the implicit discard entries and the filtering condition entries set during configuration.</p> <p>(For the ports indicated by Port 0/1-8, 25-26 in Example for AX3650S series switches, ports 1 to 8 and ports 25 and 26 are the target interfaces. The total number of entries that have been set for these ports and the maximum number of entries that can be set for these ports are displayed.)</p>	
	Target interfaces <sup>#3</sup>	<p>For AX3800S series switches:</p> <p>The interfaces are not displayed because there is no limit on the number of entries for each interface.</p> <p>For AX3650S series switches:</p> <p>Port (NIF/Port): Ethernet interfaces</p> <p>VLAN: VLAN interfaces</p> <p>Port (NIF/Port), VLAN: Ethernet and VLAN interfaces are both used.</p>
	Target access list type	MAC: MAC access lists
		IPv4: IPv4 access lists, standard IPv4 access lists, and extended IPv4 access lists
		IPv6: IPv6 access lists

Item	Displayed information	Displayed detailed information
	Number of entries that have been set and the maximum number of entries that can be set	In the receiving-side flow detection mode and the sending-side flow detection mode, access lists marked n/a are not subject to detection.
Used resources for QoS(Used/Max)	The number of entries for QoS flow detection conditions and the operating information that are currently registered on the target interface, and the maximum number of specifiable entries (For the ports indicated by Port 0/1-8, 25-26 in Example for AX3650S series switches, ports 1 to 8 and ports 25 and 26 are the target interfaces. The total number of entries that have been set for these ports and the maximum number of entries that can be set for these ports are displayed.)	
	Target interfaces <sup>#3</sup>	For AX3800S series switches: The interfaces are not displayed because there is no limit on the number of entries for each interface. For AX3650S series switches: Port (NIF/Port): Ethernet interfaces VLAN: VLAN interfaces
	Target QoS flow list type	MAC: MAC QoS flow lists
		IPv4: IPv4 QoS flow lists
		IPv6: IPv6 QoS flow lists
	Number of entries that have been set and the maximum number of entries that can be set	In the receiving-side flow detection mode, QoS flow lists marked n/a are not subject to detection.
Used resources for UPC(Used/Max)	The number of entries with the UPC setting for QoS flow detection conditions and the operating information that are currently registered on the target interface, and the maximum number of specifiable entries. (For the ports indicated by Port 0/1-8, 25-26 in Example for AX3650S series switches, ports 1 to 8 and ports 25 and 26 are the target interfaces. The total number of entries that have been set for these ports and the maximum number of entries that can be set for these ports are displayed.)	
	Target interfaces <sup>#3</sup>	For AX3800S series switches: The interfaces are not displayed because there is no limit on the number of entries for each interface. For AX3650S series switches: Port (NIF/Port): Ethernet interfaces VLAN: VLAN interfaces
	Target QoS flow list type	MAC: MAC QoS flow lists
		IPv4: IPv4 QoS flow lists
		IPv6: IPv6 QoS flow lists
	Number of entries that have been set and the maximum number of entries that can be set	In the receiving-side flow detection mode, QoS flow lists marked n/a are not subject to detection.
Used resources for TCP/UDP port detection pattern	Of the receiving-side interface filter conditions and QoS flow detection conditions that have been registered on the switch, the following items are displayed: the number of TCP/UDP port number detection patterns that use hardware resources, the maximum number of detection patterns that can be set, and the details of TCP/UDP port number detection patterns.	

Item	Displayed information	Displayed detailed information
	Number of detection patterns that have been set / Maximum number of detection patterns that can be set	Resources (Used/Max) : Number of TCP/UDP port number detection patterns that use hardware resources, and the maximum number of detection patterns that can be set on the switch
	Source and destination TCP/UDP port numbers	Source Port: Source TCP/UDP port number Destination Port: Destination TCP/UDP port number
	Details of TCP/UDP port number detection patterns	Details of the TCP/UDP port number detection patterns that use hardware resources. filter: The patterns are set with filter conditions. QoS: The patterns are set with QoS flow detection conditions. -: Not set
Flow detection out mode	Sending-side flow detection mode for filtering	For AX3800S series switches: layer3-1-out layer3-2-out For AX3650S series switches: layer3-1-out layer3-2-out layer3-3-out (For details, see 18. <i>Flow Detection Mode</i> in the manual <i>Configuration Command Reference Vol. 1 For Version 11.10.</i> )

#1: During startup of the switch, the initial routing entries for the switch are set. The value displayed during this period might be different from the number of routing entries displayed by the `show ip route` command.

#2: During startup of the switch, the initial routing entries for the switch are set. The value displayed during this period might be different from the number of routing entries displayed by the `show ipv6 route` command.

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

#3: For all the switch models of AX3800S series, there is no limit on capacities of each target port. The following table shows the range of target port numbers for each switch model.

*Table 9-6: Target port numbers for the switch models, receiving-side flow detection modes, and sending-side flow detection modes [AX3650S]*

Device model	Flow detection mode	Target port number		
		filter	QoS	UPC
AX3650S-24T6XW	layer3-1	Port 0/ 1- 12 Port 0/13-24 Port 0/25-30	Port 0/ 1-30	Port 0/ 1-30

Device model	Flow detection mode	Target port number		
		filter	QoS	UPC
	layer3-2	Port 0/ 1- 4 Port 0/ 5- 8 Port 0/ 9- 12 Port 0/13-16 Port 0/17-20 Port 0/21-24 Port 0/25-27 Port 0/28-30	Port 0/ 1- 8 Port 0/ 9-16 Port 0/17-24 Port 0/25-30	Port 0/ 1- 8 Port 0/ 9-16 Port 0/17-24 Port 0/25-30
	layer3-5	Port 0/ 1- 8 Port 0/ 9-16 Port 0/17-24 Port 0/25-30	Port 0/ 1-24 Port 0/25-30	Port 0/ 1-24 Port 0/25-30
	layer3-6	Port 0/ 1-30	Port 0/ 1-30	Port 0/ 1-30
	layer3-dhcp-1	Port 0/ 1-24 Port 0/25-30	Port 0/ 1-24 Port 0/25-30	Port 0/ 1-24 Port 0/25-30
	layer3-1-out	Port 0/ 1- 8 Port 0/ 9-16 Port 0/17-24 Port 0/25-30	None	None
	layer3-2-out	Port 0/ 1-30	None	None
	layer3-3-out	None	None	None
AX3650S-20S6XW	layer3-1	Port 0/ 1-10 Port 0/11-20 Port 0/21-30	Port 0/ 1-30	Port 0/ 1-30
	layer3-2	Port 0/ 1- 4 Port 0/ 5- 8 Port 0/ 9- 12 Port 0/13-16 Port 0/17-20 Port 0/21-24 Port 0/25-27 Port 0/28-30	Port 0/ 1-10 Port 0/11-20 Port 0/21-24 Port 0/25-30	Port 0/ 1-10 Port 0/11-20 Port 0/21-24 Port 0/25-30
	layer3-5	Port 0/ 1-10 Port 0/11-20 Port 0/21-24 Port 0/25-30	Port 0/ 1-20 Port 0/21-30	Port 0/ 1-20 Port 0/21-30
	layer3-6	Port 0/ 1-30	Port 0/ 1-30	Port 0/ 1-30
	layer3-dhcp-1	Port 0/ 1-20 Port 0/21-30	Port 0/ 1-20 Port 0/21-30	Port 0/ 1-20 Port 0/21-30
	layer3-1-out	Port 0/ 1-10 Port 0/11-20 Port 0/21-24 Port 0/25-30	None	None
	layer3-2-out	Port 0/ 1-30	None	None
	layer3-3-out	None	None	None

Device model	Flow detection mode	Target port number		
		filter	QoS	UPC
AX3650S-48T4XW	layer3-1	Port 0/ 1-24 Port 0/25-48 Port 0/49-52	Port 0/ 1-52	Port 0/ 1-52
	layer3-2	Port 0/ 1- 8 Port 0/ 9-16 Port 0/17-24 Port 0/25-32 Port 0/33-40 Port 0/41-48 Port 0/49-50 Port 0/51-52	Port 0/ 1-16 Port 0/17-32 Port 0/33-48 Port 0/49-52	Port 0/ 1-16 Port 0/17-32 Port 0/33-48 Port 0/49-52
	layer3-5	Port 0/ 1-16 Port 0/17-32 Port 0/33-48 Port 0/49-52	Port 0/ 1-48 Port 0/49-52	Port 0/ 1-48 Port 0/49-52
	layer3-6	Port 0/ 1-52	Port 0/ 1-52	Port 0/ 1-52
	layer3-dhcp-1	Port 0/ 1-48 Port 0/49-52	Port 0/ 1-48 Port 0/49-52	Port 0/ 1-48 Port 0/49-52
	layer3-1-out	Port 0/ 1-16 Port 0/17-32 Port 0/33-48 Port 0/49-52	None	None
	layer3-2-out	Port 0/ 1-52	None	None
	layer3-3-out	None	None	None

### Impact on communication

None

### Response messages

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

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

### Notes

None

---

## clear control-counter

---

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

### Syntax

```
clear control-counter
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

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

### Example

Resets to zero the number of restarts due to a failure.

```
> clear control-counter
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 9-8:* List of response messages for the clear control-counter command

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

### Notes

None

---

## show environment

---

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

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

temperature-logging

Displays the temperature history of the target switch.

Operation when this parameter is omitted:

The environmental status of the switch is displayed.

### Operation when a stack configuration is used

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

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

### Example 1

The following shows an example of displaying the operating status.

*Figure 9-7:* Example showing the result of executing the `show environment` command [AX3800S]

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

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

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

Temperature environment
  Main : 30 degrees C
  Warning level : normal

Accumulated running time
  Main : total      : 36 days and 6 hours.
        critical    : 0 days and 0 hours.
  Power slot 1 : total      : 36 days and 6 hours.
        critical    : 0 days and 0 hours.
```

```

Power slot 2 : total      : 36 days and 6 hours.
               critical   : 0 days and 0 hours.
Fan slot      : total      : 36 days and 6 hours.
               critical   : 0 days and 0 hours.
>

```

**Figure 9-8:** Example showing the result of executing the show environment command [AX3650S]

```

> show environment
Date 20XX/12/10 17:53:04 UTC
Power slot 1 : PS-M(AC)
Power slot 2 : PS-M(AC)
Fan slot      : FAN-M

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

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

Temperature environment
  Main : 30 degrees C
  Warning level : normal

Accumulated running time
  Main : total      : 365 days and 18 hours.
        critical   : 10 days and 8 hours.
  Power slot 1 : total      : 365 days and 18 hours.
        critical   : 10 days and 8 hours.
  Power slot 2 : total      : 365 days and 18 hours.
        critical   : 10 days and 8 hours.
  Fan slot      : total      : 365 days and 18 hours.
        critical   : 10 days and 8 hours.
>

```

## Display items in Example 1

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

Item	Displayed information	Displayed detailed information
Power slot 1	Power supply unit type	PS-M(AC): AC power supply unit PS-M(DC): DC power supply unit notconnect: Not installed
	Direction: Direction of the fan#1 [AX3800S]	F-to-R: Front-side air intake and rear-side air exhaust R-to-F: Rear-side air intake and front-side air exhaust
Power slot 2	Power supply unit type	PS-M(AC): AC power supply unit PS-M(DC): DC power supply unit notconnect: Not installed

## 9. Checking Software Versions and Device Statuses

Item	Displayed information	Displayed detailed information
	Direction: Direction of the fan <sup>#1</sup> [AX3800S]	F-to-R: Front-side air intake and rear-side air exhaust R-to-F: Rear-side air intake and front-side air exhaust
Fan slot	Fan unit type	FAN-M: Fan unit notconnect: Not installed
	Direction: Direction of the fan <sup>#1</sup> [AX3800S]	F-to-R: Front-side air intake and rear-side air exhaust R-to-F: Rear-side air intake and front-side air exhaust
Fan environment		
Power slot	Slot number	--
Fan <sup>#2</sup>	Fan operating status	active: Running fault: A fault has occurred. notconnect: Not installed
Speed	The rotational speed of the fan	normal: Normal rotation high: High-speed rotation stop: Stopped rotation
Fan slot		
Fan <sup>#2</sup>	Fan operating status	active: Running fault: A fault has occurred. notconnect: Not installed
Speed	The rotational speed of the fan	normal: Normal rotation high: High-speed rotation stop: Stopped rotation
Fan mode	Fan operating mode	1 (silent): Reducing switch noise takes priority. 2 (cool): Keeping the switch cool takes priority.
Power environment		
Power slot	Status of the input power supply unit	active: Supplied normally fault: No power is being supplied or there is an abnormal voltage. notconnect: Not installed
Temperature environment	Temperature information	--
Main	Intake temperature information	Displays temperature information for a device.
Warning level <sup>#3</sup>	Operating condition level	normal: Normal caution: Caution (High or low temperature)
Accumulated running time l <sup>#4</sup>		
Main	total: Cumulative operating time of the switch critical: Cumulative operating time of the switch at 50 degrees Celsius or higher	During normal operation, total is displayed. fault: The operating time could not be loaded. ***: The operating time is being loaded.

Item	Displayed information	Displayed detailed information
Power slot	total: Cumulative operating time of the power supply unit critical: Cumulative operating time of the power supply unit at 50 degrees Celsius or higher	During normal operation, total is displayed. notconnect: Not installed fault: The operating time could not be loaded. ****: The operating time is being loaded.
Fan slot	total: Cumulative operating time of the fan critical: Cumulative operating time of the fan at 50 degrees Celsius or higher	During normal operation, total is displayed. notconnect: Not installed fault: The operating time could not be loaded. ****: The operating time is being loaded.

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

#2

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

Table 9-10: Correspondence between fan numbers, operation log data, and chassis

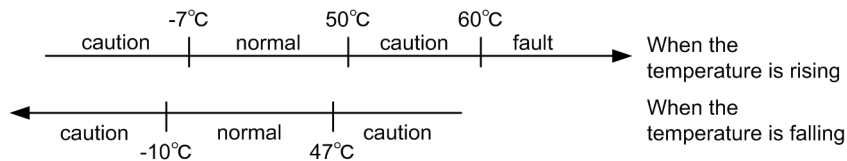
Unit	Unit correspondence	
	Command and operation log display	Location on the chassis
PS-M	FAN1(1)	Power supply unit on the right in the rear
	FAN2(1)	Power supply unit on the left in the rear
FAN-M	FAN3(1)	On the right in the rear of the fan unit 1
	FAN3(2)	On the right in the rear of the fan unit 2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

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

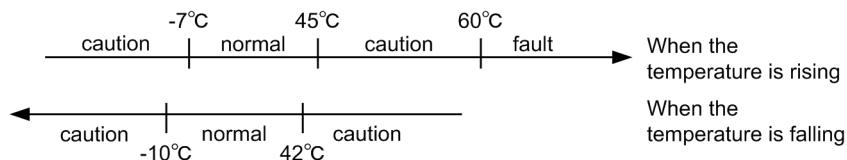
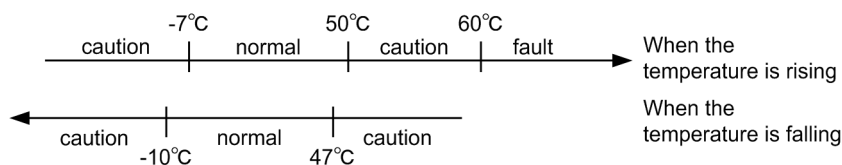
If the sensor detects a temperature of 60 degrees Celsius or higher, the software stops.

*Figure 9-9: Operating condition level and temperature [AX3800S]*

## ●FAN-04 mounted



## ●FAN-04R mounted

*Figure 9-10: Operating condition level and temperature [AX3650S]*

#4

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

At power-up (cumulative operating time = 0)

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

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

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

**Example 2**

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

*Figure 9-11: Example of displaying average temperature information*

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

**Display items in Example 2***Table 9-11: Information displayed by the show environment temperature-logging command*

Item	Displayed information	Displayed detailed information
Date	Date	--

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

### Impact on communication

None

### Response messages

*Table 9-12:* List of response messages for the show environment command

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

### Notes

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

---

## reload

---

Restarts the device, and then collect logs. During normal operation, memory dump information is collected.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

stop

Stops without restarting.

{no-dump-image | dump-image }

no-dump-image

Disables the collection of memory dump information.

dump-image

Enables the collection of memory dump information.

Operation when this parameter is omitted:

Operation is the same as the operation when `dump-image` is selected.

-f

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

Operation when this parameter is omitted:

A confirmation message is displayed.

### Operation when a stack configuration is used

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

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

### Example

1. Restarts the switch.  

```
>reload
```
2. Displays a confirmation message for memory dump collection when the `reload` command is started.  

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

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

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

```
old dump file(rmdump 01/01 00:00) delete OK? (y/n) : _
```

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

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

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

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

If `y` is entered here, the system displays a message indicating that the request to restart the switch was accepted, and restarts the switch without writing memory dump information to the internal flash memory. If `n` is entered, the system displays the command prompt without restarting the switch.

## Display items

None

## Impact on communication

Communication is interrupted while the device is being restarted

## Response messages

Table 9-13: List of response messages for the reload command

Message	Description
another user is executing update command.	This command cannot be executed because the <code>restore</code> or <code>ppupdate</code> command executed by another user is still in progress.
Can't execute.	The command could not be executed. Re-execute the command.

## Notes

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

---

## show tech-support

---

Collects hardware and software status information required for technical support.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

page

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

<password>

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

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

no-config

The configuration is not collected.

Operation when this parameter is omitted:

The configuration is collected.

ftp

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

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

{unicast|multicast|layer-2}

unicast

Collects information required for communication failure analysis of unicast routing.

multicast

Collects information required for communication failure analysis of multicast routing.

layer-2

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

Operation when this parameter is omitted:

Collects basic information about the hardware and software.

## Operation when a stack configuration is used

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

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

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

## Example

### ■ Example of executing the `show tech-support` command:

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

*Figure 9-12: Example of displaying the collected information on the screen*

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

:                               :
:      (omitted)              :
:                               :

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

### ■ Example of executing the `show tech-support ftp` command:

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

*Figure 9-13: Example of saving the collected information to the FTP server*

```
> show tech-support ftp
Specify Host Name of FTP Server.      :
Specify Host Name of FTP Server.      : ftpserver.example.com
Specify User ID for FTP connections.   : user1
Specify Password for FTP connections.  : <user1's password>
Specify Path Name on FTP Server.       : /usr/home/user1
Specify File Name of log and Dump files: support
Mon Dec 18 20:42:58 UTC 20XX
Transferred support.txt .
Executing.
.....
....
.....
Operation normal end.
##### Dump files' Information #####
**** ls -l /dump0 ****
total 2344
-rwxrwxrwx 1 root wheel 2400114 Dec  8 16:46 rmdump
**** ls -l /usr/var/hardware ****
total 1368
-rwxrwxrwx 1 root wheel 738699 Dec 27 11:56:16 20XX ni00.000
##### End of Dump files' Information #####
##### Core files' Information #####
**** ls -l /usr/var/core ****
No Core files
##### End of Core files' Information #####
Transferred support.tgz .
```

```

Executing.
.....
....
.....
.....
Operation normal end.
>

```

## Display items

Table 9-14: Information displayed by the show tech-support command

Item	Displayed information
##### <Information Type> #####	<p>A separator indicating the beginning of each type of collected information. &lt;Information Type&gt; indicates the type of information.</p> <p>The following describes the contents of &lt;Information Type&gt;:</p> <p>Dump files' Information: List of existing dump files</p> <p>Core files' Information: List of existing core files</p> <p>Tech-Support Log: Basic information that shows the hardware and software status.</p> <p>Tech-Support Unicast Log: Detailed information about unicast routing</p> <p>Tech-Support Multicast Log: Detailed information about multicast routing</p> <p>Tech-Support Layer-2 Log: Detailed information about Layer 2 protocols</p>
##### End of <Information Type> #####	<p>A separator indicating the end of each type of collected information. &lt;Information Type&gt; indicates the type of information.</p>
##### <Command Name> #####	<p>&lt;Command Name&gt; indicates the name of the command executed to collect the information. The execution result of the indicated command is displayed after this separator.</p>
##### End of <Command Name> #####	<p>A separator that indicates the end of the execution result of the indicated command. &lt;Command Name&gt; indicates the name of the command executed to collect the information.</p>

## Impact on communication

None

## Response messages

Table 9-15: List of response messages for the show tech-support command

Message	Description
<File Name>:Permission denied.	A file that has the same name as <File Name> in the response message already exists in the destination directory. You do not have permission to modify the file. Change the permission for the file in the destination directory, or change the name of the file to be saved.
<Host Name>: Unknown host	The host name (<Host-name>) is invalid.
<Path>: No such file or directory.	The directory specified for <Path> does not exist.
<Path>: Not a directory.	<Path> is not a directory.
<Path>: Permission denied.	You do not have permission to access the directory specified for <Path>.

Message	Description
connection Time out.	An attempt to connect to the FTP server failed. Check communication with the FTP server.
Exec failed.	The command execution failed.
Is the Password retyped?(y/n)	When <i>y</i> is selected in response to the message <i>Is the Password retyped?</i> , the password can be re-entered. When <i>n</i> is selected, the command execution is continued assuming that an incorrect password was entered.
Login incorrect.Login failed.	You are not permitted to log in to the specified host. A login attempt has failed.
Operation normal end.	The file transfer ended normally.
Password for Administrator Mode Invalid.	The password for administrator mode entered in the <i>&lt;password&gt;</i> parameter is incorrect.
Sorry, already execute show tech-support	Another user is executing <i>show tech-support</i> command.
Specify File Name of log and Dump files:	Specify the name of a log file and dump file. If not specified, a 14-digit number is specified as the file name by using the command execution date and time. Note that the file name entered in response to this message is reflected in <i>&lt;File Name&gt;</i> in subsequent response messages.
Specify Host Name of FTP Server. :	Specify a host name. Note that the host name entered in response to this message is reflected in <i>&lt;Host Name&gt;</i> in subsequent response messages.
Specify Password for Administrator Mode.:	Enter the password for administrator mode.
Specify Password for FTP connections. :	Enter the password of the User ID entered for the response message <i>Specify User ID for FTP connections.</i> :.
Specify Path Name on FTP Server. :	Specify a destination directory name. Note that the destination directory name entered in response to this message is reflected in <i>&lt;Path&gt;</i> in subsequent response messages.
Specify User ID for FTP connections. :	Specify a login user name. Note that the login user name entered in response to this message is reflected in <i>&lt;User ID&gt;</i> in subsequent response messages.
Write failed.	An attempt to transfer the file failed. Check the free capacity of the destination and the state of the communication line.

## Notes

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

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

Example

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

2. When the collected information is displayed on the screen (without the *ftp* parameter), the display interval is as follows:
  - When the information is displayed on the console terminal screen connected to RS232C,

the display interval with no parameters specified is five minutes, and the display time with the `unicast`, `multicast`, or `layer-2` parameters depends on the network configuration.

- When the information is displayed on the remote operation terminal screen, the display interval with no parameter is 30 seconds, and the display interval with the `unicast`, `multicast`, or `layer-2` parameters depends on the network configuration.
3. When a dump file, core file, and collected information are saved to an FTP server (with the `ftp` option), the time for transferring the files to the FTP server is as follows:
    - When only the dump file and core file for the active system are transferred, the transfer time is one to three minutes.
  4. If an IP address is set for the device itself by the `ip address (loopback)` configuration command, the IP address is used as the source IP address during communication with the FTP server.
  5. Only dump files and core files in the following directories can be saved to an FTP server when the `ftp` parameter is specified:
    - Storage directory for dump files  
`/dump0` or `/usr/var/hardware`
    - Storage directory for core files  
`/usr/var/core`

## show tcpdump (tcpdump)

Monitors incoming and outgoing packets.

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

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

Table 9-16: List of packets that can be monitored and analyzed

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

## Syntax

*<Monitoring interface packets>*

```
show tcpdump interface <interface type> <interface number> [{no-resolv |
no-domain}] [abs-seq] [no-time] [{brief | detail | extensive | debug}] [{hex
| hex-ascii}] [count <count>] [snaplen <snaplen>] [writefile <file name>]
[<expression>]
```

*<Displaying the packet monitoring file>*

```
show tcpdump readfile <file name> [{ no-resolv | no-domain }] [abs-seq]
[no-time] [{ brief | detail | extensive | debug }] [{ hex | hex-ascii }]
[count <count>] [writefile <file name>] [<expression>]
```

#: show tcpdump can be abbreviated as tcpdump. To use tcpdump, enter the following parameters:

```
tcpdump -i <interface type> <interface number> [{-n | -N}] [-S] [-t] [-q] [-v[v[v]]]
[{-x | -X}] [-c <count>] [-s <snaplen>] [-w <file name>] [<expression>]
tcpdump -r <file name> [{-n | -N}] [-S] [-t] [-q] [-v[v[v]]] [{-x | -X}] [-c
<count>] [-w <file name>] [<expression>]
```

## Input mode

User mode and administrator mode

## Parameters

interface <interface type> <interface number> (-i <interface type> <interface number>)

Specify the type (*<interface type>*) and number (*<interface number>*) of the interface that you want to monitor.

For *<interface type>* and *<interface number>*, you can specify the following:

- `vlan <vlan id>`

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

- `loopback 0`
- `loopback <loopback id> [OS-L3SA]`

For *<loopback id>*, specify a loopback interface ID set by the `interface loopback` configuration command.

`readfile <file name> (-r <file name>)`

Reads a packet from *<file name>* (created by the `writelfile` option).

{no-resolv | no-domain}

`no-resolv (-n)`

Addresses (host addresses, port numbers, or others) are not converted into names.

`no-domain (-N)`

The domain name of the host is not displayed. For example, `server` is displayed rather than `server.example.com`.

Operation when this parameter is omitted:

Addresses (host addresses, port numbers, or others) are converted into names. A host address is displayed including the domain name.

`abs-seq (-S)`

Displays the TCP sequence number as an absolute value rather than a relative value.

Operation when this parameter is omitted:

Displays the TCP sequence number as a relative value.

`no-time (-t)`

Does not display time information on each line of a dump.

Operation when this parameter is omitted:

Displays time information on each line of a dump.

{brief | detail | extensive | debug}

`brief (-q)`

Partially omits the display of protocol information such as TCP or UDP to simplify the displayed information more than usual. The Layer 2 section (address family) is also not displayed.

`detail (-v)`

Displays the information in a little more detail than usual.

For example, the information about the time to live, identification, total length, or options of IP packets is displayed. Furthermore, a check of the integrity of packets is also added. For example, the checksum of the IP or ICMP header is checked.

`extensive (-vv)`

Displays the information in more detail than the `detail` parameter.

For example, the extended fields of NFS response packets are displayed.

debug (-vvv)

Displays the most detailed information.

For example, the sub option of the `telnet` protocol is also displayed.

Operation when this parameter is omitted:

Displays normal information rather than displaying the information briefly or in detail.

{hex | hex-ascii}

hex (-x)

Displays each packet in hexadecimal except for the link layer.

hex-ascii (-X)

In hexadecimal notation, ASCII characters are also displayed.

Operation when this parameter is omitted:

Only the result of analyzing each line of a dump is displayed, without hexadecimal or ASCII.

count <count> (-c <count>)

Exits after receiving <count> packets. The specifiable values are from 1 to 2147483647.

Operation when this parameter is omitted:

Can be exited by pressing the **Ctrl + C** key.

snaplen <snaplen> (-s <snaplen>)

Retrieves <snaplen> bytes from each packet and dumps them. The permissible values are 0, and from 4 to 65535. This value should be set at a minimum required to obtain protocol information. In the Switch, set 4 or more for <snaplen> because the Layer 2 section of a packet is treated as a 4-byte Null/Loopback header including the address family.

Packets truncated by the restriction set by <snaplen> are output in the format [*<proto>*] (<proto> is the protocol name corresponding to the level where the truncation occurs).

When <snaplen> is specified as 0, length (65535) is used (to ensure capturing the whole packet).

Operation when this parameter is omitted:

Retrieves 96 bytes from each packet and dumps them.

writefile <file name> (-w <file name>)

Writes monitored information to <file name> instead of analyzing or displaying packets.

The <file name> can be displayed later by using the `readfile <file name>` option.

Operation when this parameter is omitted:

Displays the result of analyzing each dump.

<expression>

Selects the type of packets to be dumped. When <expression> is specified, only the packets that match <expression> are monitored.

When the Switch receives or transmits a large number of packets, specify this parameter to monitor only required packets.

The following is an example of the <expression> specification.

Specify one basic element or a combination of multiple basic elements for *<expression>*.

The basic element consists of four qualifiers *<protocol>* *<direction>* *<type>* *<identification>*.

The basic element is specified by placing *<type>* in front of *<identification>* and placing *<direction>*, *<protocol>*, or *<protocol>* *<direction>* qualifiers without conflict in front of *<type>* and *<identification>*.

The pattern of the basic elements is as follows:

Pattern of the basic elements:

```
<type> <identification>
<direction> <type> <identification>
<protocol> <type> <identification>
<protocol> <direction> <type> <identification>
```

*<identification>*

Indicates the name or number of addresses or port numbers.

Ex: 10.10.10.10, serverA, 23, telnet

*<type>*

Indicates the type of target for which *<identification>* is specified. The usable *<type>* is host, net, and port.

Ex: host serverA, net 192.168, port 22

When the *<type>* qualifier is omitted depending on combination with other qualifiers, it is assumed that host is specified.

Ex: src serverA represents src host serverA.

*<direction>*

Indicates the communication direction, such as from *<identification>*, to *<identification>*, or both ways.

Usable values for *<direction>* are src, dst, src or dst, and src and dst.

Ex: src serverA, dst net fe80::/64, src or dst port telnet

When the *<direction>* qualifier is not specified, it is assumed that src or dst is specified.

Ex: port telnet represents src or dst port telnet.

*<protocol>*

This qualifier is specified to limit the use of protocols to specific protocols.

Usable values for *<protocol>* are ip, ip6, tcp, and udp.

Ex: ip6 src fec0::1, ip net 192.168, tcp port 23

When the *<protocol>* qualifier is not specified, it is assumed that all the protocols that are consistent with the *<type>* specification are specified.

Ex: port 53 represents tcp port 53 or udp port 53.

Example of the basic elements:

dst host *<host>*

This is true when the IPv4/IPv6 destination of packets is *<host>*.

src host *<host>*

This is true when the IPv4/IPv6 source of packets is *<host>*.

host *<host>*

This is true when the IPv4/IPv6 destination or source of packets is *<host>*.

IPv4 or IPv6 can be limited by adding **ip** or **ip6** to the front of the above conditional expression indicating each host.

Ex: **ip** host *<host>*

Ex: **ip6** src host *<host>*

dst net *<network>/<length>*

This is true when the IPv4/IPv6 destination address of packets is included in the specified *<length>*-bit netmask *<network>*.

src net *<network>/<length>*

This is true when the IPv4/IPv6 source address of packets is included in the specified *<length>*-bit netmask *<network>*.

net *<network>/<length>*

This is true when the IPv4/IPv6 destination address of packets is included in the specified *<length>*-bit netmask *<network>*.

dst port *<port>*

This is true when a packet is ip/tcp, ip/udp, ipv6/tcp, or ipv6/udp, if the destination port number is *<port>*.

src port *<port>*

This is true when a packet is ip/tcp, ip/udp, ipv6/tcp, or ipv6/udp, if the source port number is *<port>*.

port *<port>*

This is true when a packet is ip/tcp, ip/udp, ipv6/tcp, or ipv6/udp, if the destination or source port number is *<port>*.

tcp or udp can be limited by adding **tcp** or **udp** to the front of the above conditional expression indicating each port.

Ex: **tcp** src port *<port>*

Furthermore, basic elements for which *<identification>* or other qualifiers are not specified are as follows:

ip proto *<protocol number>*

This is true when a packet is the IPv4 packet of the *<protocol number>* protocol.

Note that, when the protocol header is chained, it is not traced.

ip6 proto *<protocol number>*

This is true when a packet is the IPv6 packet of the *<protocol number>* protocol.

Note that, when the protocol header is chained, it is not traced.

ip multicast

This is true when a packet is an IPv4 multicast packet.

ip6 multicast

This is true when a packet is an IPv6 multicast packet.

ip, ip6, arp (Specify any of them)

This is true when a packet is ip, ip6, or arp.

tcp, udp, icmp, icmp6 (Specify any of them)

This is true when a packet is tcp, udp, icmp, or icmp6.

Note that, when the protocol header is chained, it is not traced.

ip protochain *<protocol number>*

The conditional expression is the same as that of `ip proto <protocol number>`, but the chain of the protocol header is traced.

ip6 protochain *<protocol number>*

The conditional expression is the same as that of `ip6 proto <protocol number>`, but the chain of the protocol header is traced.

Combinations of basic elements

A complicated filter conditional expression is represented by combining basic elements by using **and**, **or**, **not**.

To combine conditional expressions, enclose them in parentheses ( ).

Ex: `host server1 and not ( port ssh or port http )`

The above expression filters packets for which host server1 is true, and port ssh or port http is false.

Explicit qualifiers can be omitted.

Ex: `tcp dst port ftp or ssh or domain is`

the same meaning as that of `tcp dst port ftp or tcp dst port ssh or tcp dst port domain`.

Example of *<expression>* specification

host serverA

Monitors packets communication with serverA.

tcp port telnet

Monitors Telnet communication packets.

not tcp port ssh

Monitors packets other than SSH communication.

host serverA and tcp port bgp

Monitors BGP4/BGP4+ communication (IPv4 and IPv6) packets with serverA.

ip6 and host serverA and tcp port bgp

Monitors BGP4+ communication (IPv6) packets with serverA.

ip and not net 192.168.1/24

Monitors IPv4 packets whose destination and source is not the network 192.168.1/24.

udp port 520 or 521

Monitors RIP/RIPng communication (IPv4/IPv6) packets.

ip6 proto 89

Monitors OSPFv3 communication (IPv6) packets.

Operation when this parameter is omitted:

Dumps all packets without filtering received packets.

### Operation when a stack configuration is used

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

#### Example 1

When IPv4/IPv6 packets are monitored

*Figure 9-14: When IPv4/IPv6 packets are monitored*

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

#### Display items in Example 1

*Table 9-17: Information displayed for monitoring IPv4/IPv6 packets*

Displayed information	Description
1. Time stamp	Displays a time stamp when a packet is captured (not displayed when <code>no-time</code> is specified).
2. Protocol	Displays the protocol name and packet length except four bytes of the null/loopback header section (not displayed when <code>brief</code> is specified).
3. IP address pair	Displays a pair of the source address and destination address. For encapsulated packets such as tunneled packets, multiple address pairs are displayed.
4. Upper-layer protocol	Displays upper-level protocols for packet types such as ICMP or TCP.
5. Monitor statistics	Displays the number of received packets.
6. Monitor statistics	Displays the number of dropped packets.

#### Example 2

When ARP packets are monitored

*Figure 9-15: When ARP packets are monitored*

```
# show tcpdump interface vlan 10
Date 20XX/01/20 16:07:00 UTC
tcpdump: listening on VLAN0010
16:07:29.683632 arp 46: arp who-has 100.100.100.1 tell 100.100.100.2
16:07:29.683758 arp 46: arp reply 100.100.100.1 is-at 0:12:e2:98:dc:1
      1              2              3
^C
4 packets received by filter      <--4
0 packets dropped by kernel      <--5
```

## Display items in Example 2

Table 9-18: Information displayed for monitoring ARP packets

Displayed information	Description
1. Time stamp	Displays a time stamp when a packet is captured (not displayed when <code>no-time</code> is specified).
2. Protocol	Displays ARP and the packet length except four bytes of the null/loopback header section (not displayed when <code>brief</code> is specified).
3. Upper-layer protocol	Displays the information of the ARP protocol.
4. Monitor statistics	Displays the number of received packets.
5. Monitor statistics	Displays the number of dropped packets.

## Example 3

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

Figure 9-16: Result of executing the command with an interface name specified

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

Figure 9-17: Result of executing the command with `no-resolv` specified not to perform reverse lookup

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

Figure 9-18: Result of executing the command with `no-domain` specified not to display the host name and subsequent part (domain name)

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

*Figure 9-19: Result of executing the command with ip6 specified as <expression>*

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

*Figure 9-20: Result of executing the command with count <count> specified*

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

*Figure 9-21: Result of executing the command with no-time specified not to display a time stamp at each line*

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

*Figure 9-22: Result of executing the command with writefile specified to specify the file name and save a dump to the file*

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

*Figure 9-23: Result of executing the command with readfile specified to specify the file name and read a dump from the file and display it*

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

*Figure 9-24: Result of executing the command with readfile specified to read a dump from the file, and with icmp specified as <expression> to display only icmp*

```
# show tcpdump readfile mydump icmp
Date 20XX/01/20 20:23:00 UTC
reading from file mydump, link-type NULL (BSD loopback)
```

```

20:23:10.113591 ip 84: hostA.example.com > myhost.example.com: icmp 64: echo
request seq 20
20:23:10.113692 ip 84: myhost.example.com > hostA.example.com: icmp 64: echo
reply seq 20

```

### Display items in Example 3

None

### Impact on communication

None

### Response messages

Table 9-19: List of response messages for the show tcpdump command

Message	Description
tcpdump: <file name>: Is a directory	<file name> is a directory (Specify the name of a file).
tcpdump: <file name>: No such file or directory	<file name> could not be found.
tcpdump: <file name>: Permission denied	Access to <file name> has not been permitted.
tcpdump: archaic file format	The file format is old.
tcpdump: bad dump file format	The file format is invalid.
tcpdump: BIOCSETIF: Device not configured	An invalid interface has been specified. The command execution ends now.
tcpdump: BIOCSETIF: Network is down	An invalid interface has been specified. The command execution ends now.
tcpdump: bogus savefile header	The file header is invalid.
tcpdump: ethernet addresses supported only on ethernet, FDDI or token ring	Layer 2 monitoring is not supported.
tcpdump: expression rejects all packets	The specified filter condition <expression> filters all packets. So, change the condition.
tcpdump: fread: Operation not permitted	The file could not be read (an invalid file might be specified).
tcpdump: fread: Undefined error: 0	The file is abnormal (an unusually short file might be specified).
tcpdump: fwrite: No space left on device	The file could not be written (the disk space might be insufficient).
tcpdump: illegal char: <character>	An invalid <character> has been specified.
tcpdump: illegal Interface name -- <interface name>.	The specified interface has not been set. <interface name>: Name assigned to the specified interface
tcpdump: illegal qualifier of 'port'	An invalid port condition has been specified.
tcpdump: illegal token: <token>	An invalid <token> has been specified.
tcpdump: inbound/outbound not supported on linktype 0	inbound/outbound specification is not supported.
tcpdump: invalid ip6 address <address>	The IPv6 address <address> is invalid.
tcpdump: invalid packet count <count>	The <count> value is invalid.
tcpdump: invalid qualifier against IPv6 address	An invalid qualifier has been specified for the IPv6 address.
tcpdump: invalid snaplen <snaplen>	The <snaplen> value is invalid.
tcpdump: link layer applied in wrong context	Layer 2 monitoring is not supported.

Message	Description
tcpdump: listening on <i>&lt;interface name&gt;</i>	The interface <i>&lt;interface name&gt;</i> is being monitored. <i>&lt;interface name&gt;</i> : Name assigned to the specified interface
tcpdump: mask length must be $\leq$ <i>&lt;length&gt;</i>	The mask length should be <i>&lt;length&gt;</i> or less.
tcpdump: Mask syntax for networks only	Masks can be specified only by the net qualifier.
tcpdump: No match.	The specified file does not exist.
tcpdump: no VLAN support for data link type 0	VLAN specification is not supported.
tcpdump: non-network bits set in " <i>&lt;address&gt;</i> "	<i>&lt;address&gt;</i> whose host bit is not 0 has been specified.
tcpdump: only IP multicast filters supported on ethernet/FDDI	To specify multicast, place <code>ip</code> or <code>ip6</code> in front of it.
tcpdump: parse error	The syntax of the specified filter condition <i>&lt;expression&gt;</i> is invalid.
tcpdump: pcap_loop: link-layer type <i>&lt;type&gt;</i> isn't supported in savefiles	The link layer type <i>&lt;type&gt;</i> of the read file is not supported.
tcpdump: pcap_loop: truncated dump file; tried to read <i>&lt;bytes1&gt;</i> captured bytes, only got <i>&lt;bytes2&gt;</i> .	The read file has been dropped on the way. <i>&lt;byte1&gt;</i> bytes were captured, but there are only <i>&lt;bytes2&gt;</i> bytes.
tcpdump: pcap_loop: truncated dump file; tried to read <i>&lt;bytes1&gt;</i> header bytes, only got <i>&lt;bytes2&gt;</i> .	The read file has been dropped on the way. The header is <i>&lt;byte1&gt;</i> -bytes, but there are only <i>&lt;bytes2&gt;</i> bytes.
tcpdump: port ' <i>&lt;port&gt;</i> ' is <i>&lt;protocol&gt;</i>	The port specification <i>&lt;port&gt;</i> is <i>&lt;protocol&gt;</i> protocol.
tcpdump: syntax error	The syntax of the specified filter condition <i>&lt;expression&gt;</i> is invalid.
tcpdump: unknown host ' <i>&lt;host&gt;</i> '	An unknown host name <i>&lt;host&gt;</i> was specified. Write the network with the address.
tcpdump: unknown host ' <i>&lt;host&gt;</i> ' for specified address family	The address of the host <i>&lt;host&gt;</i> could not be resolved by the specified address family.
tcpdump: unknown ip proto ' <i>&lt;protocol&gt;</i> '	The protocol name <i>&lt;protocol&gt;</i> of the specified filter condition <i>&lt;expression&gt;</i> could not be specified. Specify the protocol with the protocol number.
tcpdump: unknown network ' <i>&lt;network&gt;</i> '	An unknown network name <i>&lt;network&gt;</i> was specified. Write the network with the address.
tcpdump: unknown osi proto ' <i>&lt;protocol&gt;</i> '	An unknown osi protocol <i>&lt;protocol&gt;</i> was specified.
tcpdump: unknown port ' <i>&lt;port&gt;</i> '	The port name <i>&lt;port&gt;</i> of the specified filter condition <i>&lt;expression&gt;</i> could not be specified. Specify the port with the port number.
tcpdump: unknown protocol: <i>&lt;protocol&gt;</i>	An unknown protocol <i>&lt;protocol&gt;</i> was specified.
tcpdump: WARNING: no IPv4 address assigned	This is displayed if an IPv4 address is not assigned.
tcpdump: WARNING: SIOCGIFADDR: Operation not permitted	An invalid interface has been specified. Exit by pressing the <b>Ctrl + C</b> key.
tcpdump: <i>&lt;filter&gt;</i> host filtering not implemented	The host filter of <i>&lt;filter&gt;</i> is not supported.
tcpdump: ' <i>&lt;string&gt;</i> ' modifier applied to host	The <i>&lt;string&gt;</i> qualifier has been added to the host (invalid).
tcpdump: ' <i>&lt;string&gt;</i> ' modifier applied to <i>&lt;host&gt;</i> host	The <i>&lt;string&gt;</i> qualifier has been added to the host <i>&lt;host&gt;</i> (invalid).
tcpdump: ' <i>&lt;protocol&gt;</i> proto' is bogus	The protocol specification <i>&lt;protocol&gt;</i> is invalid.
tcpdump: <i>&lt;host&gt;</i> resolved to multiple address	<i>&lt;host&gt;</i> has resolved multiple addresses.

## Notes

1. This command can monitor incoming and outgoing software processing packets such as routing protocols.
2. This command cannot monitor packets other than incoming and outgoing packets, such as an IPv4/IPv6 transfer packets, MPLS transfer packets, multicast transfer packets, or tunnel processing packets. Note that filtered packets or packets that are not processed by software (various Layer 2 packets such as PPP), which are one type of incoming and outgoing packet, cannot be monitored.
3. This command can monitor the Layer 3 packet traffic and the lower layers. The Layer 2 traffic such as Ethernet headers cannot be monitored. The Layer 2 traffic is replaced with the null/loopback header (data link type) regardless of the type of the specified VLAN *<vlan id>*.
4. The address family (ip/ip6/arp) is displayed in the information of the null/loopback header section.
5. The length of the null/loopback header is four bytes. This is displayed as [|null] when the *<snaplen>* setting is set to less than four bytes.
6. When the *no-resolve* parameter is not specified, if the dns-resolver configuration is wrong, displaying the monitoring status takes some time.
7. When there is a large amount of traffic, there might be too many packets to be monitored and packets might be dropped (Count of packets dropped by kernel is displayed after the command execution ends). In such a case, specify *<expression>* to monitor only required packets.

---

## backup

---

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

### Syntax

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

### Input mode

Administrator mode

### Parameters

mc

Specifies the memory card as the backup destination.

ftp <ftp-server>

Specifies the remote FTP server as the backup destination. Specify the IP address or host name of a server (IPv4 address or IPv6 address) for <ftp-server>.

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

<filename>

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

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

no-software

No software is backed up.

Operation when this parameter is omitted:

Backup, including software information, is performed.

### Operation when a stack configuration is used

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

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

### Example 1

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

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

### Example 2

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

```
> enable
# backup ftp ftpserver MCBackup.dat
Backup information to MCBackup.dat in FTP(ftpserver) .
Input username: guest
Input password:
```

```
ftp transfer start.

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

### Example 3

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

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

### Display items

None

### Impact on communication

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

### Response messages

Table 9-20: List of response messages for the backup command

Message	Description
<code>/usr/var/update/k.img</code> is not exist. please put <code>k.img</code> to <code>/usr/var/update</code> and retry.	The file <code>k.img</code> does not exist in <code>/usr/var/update</code> . Copy <code>k.img</code> to <code>/usr/var/update</code> and then re-execute the command.
Filename is invalid	A file with the specified name could not be created on a memory card. Specify another file name.
ftp transfer failed.	An attempt to transfer the device information by using the <code>backup ftp</code> command failed.
MC file write error.	Writing to the memory card failed. There might not be enough free space on the memory card. Delete unnecessary files and then re-execute the command.
MC is busy.	Another process is accessing the memory card. Wait a while, and then re-execute the command.
MC is write protected.	Make sure the memory card's protect switch is not set to ▼ Lock. If the switch is set to ▼ Lock, slide the switch, and then insert the memory card again. Make sure there is no dust in the memory card slot. If there is dust, remove it with a dry cloth and then insert the memory card again.
MC not found.	A memory card was not inserted into the slot. Make sure that a memory card is inserted into the device properly. Make sure there is no dust in the memory card slot. If there is dust, remove it with a dry cloth and then insert the memory card again.
Saving file( <code>&lt;file name&gt;</code> ) to MC failed.	Writing to the memory card failed.
This command is executable only the start-up from flash memory	The command could not be executed because the switch booted from a memory card. Start up the switch from flash memory and then re-execute the command.

## Notes

- Before using the `backup ftp` command, make sure that the target FTP server has about 50 MB of free space.
- The files under `/usr/home/` are not backed up.
- The device information saved by this command can be restored to the Switch by using the `restore` command.
- Perform backup and restoration between the same models.
- When the file `k.img` does not exist in the directory `/usr/var/update`, this command cannot be executed. Before executing the command, copy the file `k.img` to `/usr/var/update`.
- Do not allow other users to log in while this command is being executed.
- Do not remove or insert the memory card while the `backup mc` command is backing up data to the memory card.
- Accessing a memory card increases load on the device. Before specifying the `mc` parameter, if the monitoring time and sending interval of the Layer 2 or Layer 3 protocol, which are settings for maintaining connection with neighboring devices, are set shorter than the initial value, reset the monitoring time and sending interval to longer values.

---

## restore

---

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

### Syntax

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

### Input mode

Administrator mode

### Parameters

mc

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

ftp <ftp-server>

Specifies the remote FTP server as the location where the image is stored. Specify the IP address or host name of a server (IPv4 address or IPv6 address) for <ftp-server>.

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

<filename>

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

no-software

No software is restored.

Operation when this parameter is omitted:

Restores all the backup data.

### Operation when a stack configuration is used

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

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

### Example 1

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

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

### Example 2

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

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

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

## Display items

None

## Impact on communication

When the device information has been restored, the device restarts automatically. During the restart, communication is temporarily suspended. When the `mc` parameter is specified, if monitoring time or sending interval of the Layer 2 or Layer 3 protocol is set shorter than the initial value on neighboring devices, communication might be disconnected when the Layer 2 or Layer 3 protocol is disconnected.

## Response messages

Table 9-21: List of response messages for the restore command

Message	Description
another user is executing now.	This command cannot be executed because the <code>restore</code> or <code>ppupdate</code> command executed by another user is still in progress.
Can't execute.	The command could not be executed. Re-execute the command.
File is not found.	The specified file could not be found.
MC is busy.	Another process is accessing the memory card. Wait a while, and then re-execute the command.
MC not found.	A memory card was not inserted into the slot. Make sure that a memory card is inserted into the device properly. Make sure there is no dust in the memory card slot. If there is dust, remove it with a dry cloth and then insert the memory card again.
Restore operation failed.	An attempt to restore the device information failed. There might not be enough free space on the disk of the Switch. Delete unnecessary files and then re-execute the command.

## Notes

- When the device information has been restored, the device restarts automatically. During the restart, communication is temporarily suspended.
- Do not allow other users to log in while this command is being executed.
- Do not remove or insert the memory card while the `restore mc` command is restoring data from the memory card.
- Perform backup and restoration between the same models.
- Accessing a memory card increases load on the device. Before specifying the `mc` parameter, if the monitoring time and sending interval of the Layer 2 or Layer 3 protocol, which are settings for maintaining connection with neighboring devices, are set shorter than the initial value, reset the monitoring time and sending interval to longer values.
- During execution of this command, the sleep mode functionality is disabled. If the scheduled time period is entered during execution of this command, the Switch enters the sleep mode after command execution is complete.
- You cannot execute this command while the `ppupdate` or `restore` command executed by another user is still in progress. If you attempt to do so, the command terminates abnormally, and the following message is displayed: `another user is executing now`. In such a case, wait a while, and then re-execute the command. If the command still terminates abnormally, execute `rm /tmp/ppupdate.exec` to delete files, and then re-execute the command.
- When restoring the switches that make up a stack, first restore the switches, and then configure the stack.

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

## Chapter

---

# 10. Power Saving Functionality

---

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

---

## show power-control schedule

---

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

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

<yymmdd>

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

yy

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

For example, 00 means the year 2000.

mm

Specify the month in the range from 01 to 12.

dd

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

Operation when this parameter is omitted:

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

count <count>

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

Operation when this parameter is omitted:

The scheduled dates and times for 10 schedules are displayed.

Operation when all parameters are omitted:

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

### Operation when a stack configuration is used

This command is not supported.

### Example

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

*Figure 10-1: Result of executing show power-control schedule*

```
> show power-control schedule XX0401 count 5
Date 20XX/04/01(Thu) 18:36:57 UTC
Current Schedule Status : Disable
Schedule Power Control Date:
  20XX/04/01(Thu) 20:00 UTC - 20XX/04/02(Fri) 06:00 UTC
  20XX/04/02(Fri) 20:00 UTC - 20XX/04/05(Mon) 06:00 UTC
  20XX/04/05(Mon) 20:00 UTC - 20XX/04/06(Tue) 06:00 UTC
  20XX/04/06(Tue) 20:00 UTC - 20XX/04/07(Wed) 06:00 UTC
```

20XX/04/07 (Wed) 20:00 UTC - 20XX/04/08 (Thu) 06:00 UTC  
>

## Display items

Table 10-1: Information displayed by the show power-control schedule command

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

## Impact on communication

None

## Response messages

Table 10-2: List of response messages for the show power-control schedule command

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

## Notes

None

---

## show power

---

Displays information about power consumption and estimated power consumption amount of the Switch.

### Syntax

```
show power
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

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

### Example

*Figure 10-2: Result of executing the show power command*

```
>show power
Date 20XX/09/21 12:00:00 UTC
Elapsed time 2Days 01:30
H/W      Wattage  Accumulated Wattage
Chassis  60.59 W   3.50 kWh
>
```

### Display items

*Table 10-3: Information displayed by the show power command*

Item	Displayed information	Displayed detailed information
Elapsed time	Elapsed time	If the <code>clear power</code> command was not executed, the time elapsed since the switch started is displayed. If the <code>clear power</code> command was executed, the time elapsed since the <code>clear power</code> command was executed is displayed. The time is displayed in days and then hours: minutes. <sup>#1</sup>
H/W	Parts information	Displays the Switch.
Wattage	Power consumption	Displays the estimated power consumption. This is displayed in W. <sup>#2</sup>
Accumulated Wattage	Amount of power consumption	Displays the cumulative power consumption. This is displayed in kWh. <sup>#1#3</sup>

#1: The elapsed time and the amount of power consumption are also accumulated while the Switch is in the sleep state.

#2: This estimated value is different from the actual power consumption. To obtain an accurate value, measure it with a measuring instrument.

#3: Because this information is rounded off to two decimal places, there are some errors between this information and the power consumption value obtained by an MIB (axisPconPowerConPowerConsumption).

**Impact on communication**

None

**Response messages***Table 10-4:* List of response messages for the show power command

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

**Notes**

- The value of cumulative power consumption is cleared when the device is restarted.
- The power consumption information displayed by this command is equal to the result value of the command execution.

---

## clear power

---

Clears the information about the power consumption of the Switch.

### Syntax

`clear power`

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

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

### Example

*Figure 10-3: Result of executing the clear power command*

```
> clear power
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 10-5: List of response messages for the clear power command*

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

### Notes

Even if you use this command to clear the information about the power consumption, the value of the MIB information obtained by using SNMP is not cleared to zero.

---

## set power-control schedule

---

Sets whether power saving scheduling is enabled or disabled while the scheduled time range of power saving scheduling is in effect. The setting of this command is valid until the time range moves from scheduled to normal. Note that if this command is executed when the normal time range is in effect, the setting will be enabled in the next scheduled time range.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

{enable | disable}

enable

Enables power saving scheduling.

disable

Disables power saving scheduling. If the normal time range is set, schedule-disabled mode takes effect in the next scheduled time range.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following shows an example of disabling the power saving schedules.

*Figure 10-4:* Result of executing the set power-control schedule command

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

### Display items

None

### Impact on communication

None

### Response messages

*Table 10-6:* List of response messages for the set power-control schedule command

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

### Notes

None

---

**show power-control port**

---

Displays the operating status of the port power saving functionality.

**Syntax**

show power-control port

**Input mode**

User mode and administrator mode

**Parameters**

None

**Operation when a stack configuration is used**

This command is not supported.

**Example**

The following shows an example of displaying the status of port power saving control.

*Figure 10-5: Result of executing show power-control port*

```
> show power-control port
Date 20XX/09/21 20:03:12 UTC
Port  Status  Cool-standby
0/1   up       -
0/2   down     applied
0/3   down     applied
0/4   up       -
0/5   up       -
:
:
0/48  down     applied
0/49  up       -
0/50  down     -
0/51  down     -
0/52  up       -
>
```

**Display items**

*Table 10-7: Information displayed by the show power-control port command*

Item	Displayed information	Displayed detailed information
Port	Port	NIF number/port number

Item	Displayed information	Displayed detailed information
Status	Port state	<p>up: Active (normal operating state)</p> <p>down: Active (A line failure occurred.)</p> <p>init: Currently initializing or waiting for establishment of negotiation (auto-negotiation is operating).</p> <p>test: A line test is in progress.</p> <p>fault: Failed</p> <p>inact:</p> <ul style="list-style-type: none"> <li>- Operation was stopped by the <code>inactivate</code> command.</li> <li>- Inactive due to the standby link functionality of link aggregation</li> <li>- Inactive due to the BPDU guard functionality of the Spanning Tree Protocol</li> <li>- Inactive due to the port resetting functionality of GSRP</li> <li>- The port has been deactivated by the unidirectional link failure detection functionality.</li> <li>- The port has been deactivated by the L2 loop detection functionality.</li> <li>- The port has been deactivated by storm control.</li> </ul> <p>dis: Operation was stopped by the <code>shutdown</code> or <code>schedule-power-control shutdown</code> configuration command.</p>
Cool-standby	Port power saving functionality operating status	<p>applied: The port power saving functionality is operating.</p> <p>A hyphen (-) is displayed when the port power saving functionality is stopped or the port is in the link-up status.</p>

### Impact on communication

None

### Response messages

*Table 10-8:* List of response messages for the show power-control port command

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

### Notes

None



## Chapter

---

# 11. Checking Internal Memory and Memory Cards

---

```
show mc  
format mc  
show flash
```

---

## show mc

---

Displays the memory card format and card usage.

### Syntax

show mc

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

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

### Example

```
>show mc
Date 20XX/09/13 06:35:27 UTC
MC : enabled
    Manufacture ID : 00000003
        7,717kB used
        50,128kB free
        57,845kB total
>
```

### Display items

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

Item		Displayed information	Displayed detailed information
MC	--	Memory card status	enabled: The memory card can be accessed. notconnect: The memory card is not installed. write protect: Writing to the memory card is not allowed. -----: Another process is accessing the memory card. <sup>#1</sup>
	Manufacture ID	Production ID number <sup>#2</sup>	Memory card production ID number
	used	Used capacity <sup>#2</sup>	Used capacity of the memory card file system
	free	Unused capacity <sup>#2</sup>	Unused capacity of the memory card file system
	total	Total capacity <sup>#2</sup>	Total of capacity in use and capacity not in use for the memory card file system

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

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

### Impact on communication

None

## Response messages

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

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

## Notes

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

---

## format mc

---

Initializes formats the memory card for use by the Switch.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

-f

Executes the command without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

### Operation when a stack configuration is used

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

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

### Example

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

```
>format mc
```
2. A message asking for confirmation is displayed after executing the `format` command.  

```
MC initialize OK? (y/n):_
```

If `y` is entered, the memory card will be initialized.

If an error occurs, an error message is displayed.

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

### Display items

None

### Impact on communication

None

### Response messages

Table 11-3: List of response messages for the `format mc` command

Message	Description
Can't access to MC by write protection.	The write protection switch of the memory card is set for the write-protected status. Reset the write protection switch to the write-permitted status, and then re-execute the command.
Can't execute.	The command could not be executed. Re-execute the command.
Can't gain access to MC.	The memory card is not installed, or an attempt to access the memory card failed.

**Notes**

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

## show flash

Shows internal flash memory usage.

### Syntax

```
show flash
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

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

### Example

```
> show flash
Date 20XX/06/21 17:53:11 UTC
Flash :
      user area  config area  dump area  area total
used  114,175kB      74kB      3,306kB    117,555kB
free   91,381kB    120,597kB    62,084kB    274,062kB
total 205,556kB    120,671kB    65,390kB    391,617kB
>
```

### Display items

Table 11-4: Information displayed by the show flash command

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

<sup>#</sup>: If used capacity exceeds 95 percent of the total capacity, unused capacity might be displayed as

a negative value. If unused capacity is displayed as a negative value, delete user files so as to free up enough unused capacity.

### Impact on communication

None

### Response messages

*Table 11-5:* List of response messages for the show flash command

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

### Notes

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



## Chapter

---

# 12. Log

---

show logging  
clear logging  
show logging console  
set logging console

---

## show logging

---

Shows the log entries recorded by the Switch.

This command handles two types of logs, operation logs and reference logs, which are displayed or controlled independently. The operation logs consist of entered command strings, command response messages, and various event messages. The reference logs contain statistics obtained by compiling events that occurred for each code.

For details about the information to be displayed as the command execution result, see *1.2 Checking a log* in the manual *Message and Log Reference For Version 11.10*.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

<kind>

reference

Specifies the reference log.

Operation when this parameter is omitted:

Specifies the operation log.

<command classification>

-h

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

Operation when this parameter is omitted:

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

Operation when all parameters are omitted:

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

### Operation when a stack configuration is used

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

```
remote command {<switch no.> | all} show logging [<kind>] [<command classification>]
```

### Example

- Display the operation log entries for the switch.
- ```
> show logging
```

*Figure 12-1: Operation log display*

```
> show logging
Date 20XX/12/25 14:14:18 UTC
System Information
  AX3650S-20S6XW, OS-L3SA Ver. 11.5 (Build:45)
Logging Information
KEY 12/24 12:37:30 user1:ping 192.111.214.10
.
.
```

```
> .
```

- Display the reference log entries for the switch.  
> show logging reference

*Figure 12-2: Reference log display*

```
> show logging reference
Date 20XX/12/25 14:14:18 UTC
System Information
  AX3650S-20S6XW, OS-L3SA Ver. 11.5 (Build:45)
Logging Information
E4 PORT GigabitEthernet 0/20 25011001 1350:000000000000
  10/25 14:12:10      10/25 14:12:10      1
.
.
.
```

## Display items

None

## Impact on communication

None

## Response messages

*Table 12-1: List of response messages for the show logging command*

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

## Notes

- Log information is obtained at the UTC time immediately after the device is started.
- The operation log entries are displayed in reverse chronological order from the latest message or operation (the latest information is displayed at the top). Note that the reboot reason log entry of the switch appears after the startup log entry, but its timestamp is earlier than that of the startup log entry. If several log entries are generated at the same time, those log entries might not be displayed in reverse chronological order.
- The reference log entries are collected for each event in chronological order. However, the order in which command execution results are displayed is not always in chronological order because the information about events that have occurred is grouped by event type.

---

## clear logging

---

Erases the log entries recorded by the Switch.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

<kind>

reference

Specifies the reference log.

Operation when this parameter is omitted:

Specifies the operation log.

### Operation when a stack configuration is used

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

```
remote command {<switch no.> | all} clear logging [<kind>]
```

### Example

- Erase the operation log entries.  
    > clear logging
  
- Erase the reference log.  
    > clear logging reference

### Display items

None

### Impact on communication

None

### Response messages

Table 12-2: List of response messages for the clear logging command

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

### Notes

None

---

## show logging console

---

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

### Syntax

```
show logging console
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

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

### Example

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

```
> show logging console
System message mode : Display all
```
- Indicate that system messages whose event level is E6 or less are prevented from being displayed.  

```
> show logging console
System message mode : E6
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 12-3: List of response messages for the show logging console command*

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

### Notes

None

---

## set logging console

---

Controls the display of system messages by event level. Low priority system messages that might be displayed frequently due to system configuration changes can be suppressed.

### Syntax

```
set logging console { disable <event level> | enable }
```

### Input mode

User mode and administrator mode

### Parameters

```
{ disable <event level> | enable }
```

```
disable <event level>
```

Specifies an event level (E3 to E9); messages related to events at this specified level and lower levels will not be displayed.

```
enable
```

Specifies that all system messages will be displayed.

### Operation when a stack configuration is used

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

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

```
set logging console { disable <event level> | enable }
```

### Example

- Specify that all system messages be displayed.  

```
> set logging console enable
```
- Specify that system messages whose event level is E5 or less not be displayed.  

```
> set logging console disable E5
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 12-4:* List of response messages for the set logging console command

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

### Notes

None

## Chapter

---

# 13. Software Management

---

ppupdate  
set license  
show license  
erase license

---

## ppupdate

---

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

### Syntax

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

### Input mode

Administrator mode

### Parameters

test

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

no-display

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

-f

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

Operation when this parameter is omitted:

A confirmation message is displayed.

no-reload

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

<file-name>

Specifies the update file name.

### Operation when a stack configuration is used

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

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

### Example

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

```
# ppupdate k.img
```

```
Software update start
```

```
Broadcast Message from operator@
(??) at 15:32 UTC...
```

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

```
Current version is 11.5
```

```
New version is 11.6
```

```
Automatic reboot process will be run after installation process.
```

```
Do you wish to continue? (y/n) y
```

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

## Display items

None

## Impact on communication

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

## Response messages

Table 13-1: List of response messages for the `ppupdate` command

| Message                                             | Description                                                                                                                                      |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| another user is executing now.                      | This command cannot be executed because the <code>restore</code> or <code>ppupdate</code> command executed by another user is still in progress. |
| Can't execute.                                      | The command could not be executed. Re-execute the command.                                                                                       |
| Can't open <code>&lt;file-name&gt;</code> .         | The specified file could not be opened. Specify the correct file name.                                                                           |
| extract failed.                                     | Updating has failed. Re-execute the command.                                                                                                     |
| Invalid file <code>&lt;file-name&gt;</code> .       | The contents of the specified file are invalid. Specify a valid file.                                                                            |
| OS Type mismatch.<br>Can not apply this package.    | The specified file cannot be used because it is intended for a different device.                                                                 |
| OS version mismatch.<br>Can not apply this package. | The specified file cannot be used for this Switch.                                                                                               |

## Notes

- When updating is performed, the configuration in effect before the update is inherited. Note that, when the inherited configuration includes a configuration that is not supported by the updated software version, the unsupported configuration command is not inherited. At this time, the startup configuration and running configuration do not match. Therefore, a prompt indicating that the configuration has not been saved is displayed until a save operation is performed. In addition, unsupported configuration commands that are not inherited are output as operation log entries. For details, see *3.1 Configuration* in the manual *Message and Log Reference For Version 11.10*.
- If many configurations are set and software is updated, device startup might take some time because the configurations are inherited to the new version.
- Where a memory card that contains the software image file `k.img` is mounted in a Switch, the switch boots from the memory card when it is restarted. If you do this, the account and configuration information reverts to the factory defaults and you cannot save your own settings. Avoid using this method under normal circumstances.
- During execution of this command, the sleep mode functionality is disabled. If the scheduled time period is entered during execution of this command, the Switch enters the sleep mode after the command execution is complete.
- You cannot execute this command while the `ppupdate` or `restore` command executed by another user is still in progress. If you attempt to do so, the command terminates abnormally, and the following message is displayed: `another user is executing now`. Wait a while, and

then re-execute the command. If the command still terminates abnormally, execute `rm /tmp/ppupdate.exec` to delete files, and then re-execute the command.

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

---

## set license

---

Registers a purchased optional license onto the Switch.

### Syntax

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

### Input mode

Administrator mode

### Parameters

key-file <file name>

Sets an optional license with the specified file name.

key-code <license key>

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

### Operation when a stack configuration is used

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

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

### Example

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

```
# set license key-file addopt.dat
#
```
- Example of specifying a license key (In this example, `0123-4567-89ab-cdef-0123-4567-89ab-cdef` is specified as a license key)
 

Example of specifying a license key that uses hyphens as delimiters:

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

Example of specifying a license key that does not use hyphens as delimiters:

```
#set license key-code 0123456789abcdef0123456789abcdef
```

### Display items

None

### Impact on communication

None

### Response messages

Table 13-2: List of response messages for the set license command

| Message                                 | Description                                                           |
|-----------------------------------------|-----------------------------------------------------------------------|
| <license key> is not for this system.   | The license key is not for this system.<br><license key>: License key |
| A license key cannot be added any more. | The number of optional licenses exceeds the maximum allowed number.   |

| Message                                            | Description                                                                                                                                            |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Can't execute.                                     | The command could not be executed. Re-execute the command.                                                                                             |
| Invalid contents of <i>&lt;file name&gt;</i> .     | The contents of the specified license key file are invalid. Specify a valid license key file.<br><i>&lt;file name&gt;</i> : Specified license key file |
| Invalid license key <i>&lt;license key&gt;</i> .   | The entered license key is invalid.                                                                                                                    |
| Invalid serial number <i>&lt;license key&gt;</i> . | The license key is invalid.<br><i>&lt;license key&gt;</i> : License key                                                                                |
| No such file <i>&lt;file name&gt;</i>              | The specified license key file does not exist.<br><i>&lt;file name&gt;</i> : Specified license key file                                                |
| This license is already registered.                | This optional license has already been set.                                                                                                            |

## Notes

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

---

## show license

---

Displays authorized optional licenses.

### Syntax

```
show license
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

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

### Example

An example of displaying authorized optional licenses is described below:

```
# show license
Date 20XX/01/23 12:00:00 UTC
  Available: OP-VAA
    Serial Number      Licensed software
    0500-0001-0200-0000 OP-VAA (AX-P3630-F6)
#
```

### Display items

Table 13-3: Information displayed by the show license command

| Item              | Displayed information                                                                                                                                                   | Displayed detailed information                                  |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| Available:        | Name of an option that takes effect                                                                                                                                     | ----- is displayed when no option exists.                       |
| Serial Number     | Specified optional license serial number                                                                                                                                | --                                                              |
| Licensed software | Abbreviated name of purchased software.<br>(The model name is enclosed in parentheses.)<br>If multiple options are purchased for one license, each option is displayed. | unknown (-----) is displayed when the software name is unknown. |

### Impact on communication

None

### Response messages

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

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

### Notes

None

---

## erase license

---

Erases the specified optional license.

### Syntax

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

### Input mode

Administrator mode

### Parameters

<serial no.>

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

### Operation when a stack configuration is used

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

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

### Example

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

```
# erase license 0100-0001-0200-0000
```

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

If you enter y here, the optional license is deleted.

If you enter n here, the optional license is not deleted, and the command prompt is displayed.

### Display items

None

### Impact on communication

None

### Response messages

Table 13-5: List of response messages for the erase license command

| Message                            | Description                                                                                        |
|------------------------------------|----------------------------------------------------------------------------------------------------|
| Can't execute.                     | The command could not be executed. Re-execute the command.                                         |
| Invalid serial number <serial no.> | The optional license of the specified serial number does not exist.<br><serial no.>: Serial number |

### Notes

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

## Chapter

---

# 14. Resource Information

---

show cpu  
show processes  
show memory  
df  
du

---

## show cpu

---

Shows CPU usage.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

days

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

hours

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

minutes

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

seconds

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

Operation when each parameter is omitted:

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

Operation when all parameters are omitted:

You cannot omit all of the parameters.

### Operation when a stack configuration is used

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

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

### Example and display items

*Figure 14-1: Example of specifying days*

```
> show cpu days
Date 20XX/09/13 14:15:37 UTC
*** day ***
date      time                cpu average
Dec 13    16:00:00-23:59:59    5
Dec 14    00:00:00-23:59:59    4
Dec 15    00:00:00-23:59:59    25
:
Dec 29    00:00:00-23:59:59    5
>
```

Table 14-1: Information displayed by specifying days

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

Figure 14-2: Example of specifying hours

```

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

```

Table 14-2: Information displayed by specifying hours

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

Figure 14-3: Example of specifying minutes

```

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

```

Table 14-3: Information displayed by specifying minutes

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

Figure 14-4: Example of specifying seconds

```

> show cpu seconds
Date 20XX/12/13 14:15:37 UTC
*** second ***
date      time                cpu average
Dec 13    14:43:14-14:43:23    20 10  5  4  70  9  80  30  7  50
Dec 13    14:43:24-14:43:33    10  9  40  40  7  4  6  10  7  4
Dec 13    14:43:34-14:43:43    20 10  5  4  52  9  80  30  7  50
Dec 13    14:43:44-14:43:53    10  9  40  40  7  4  6  10  7  4
Dec 13    14:43:54-14:44:03    20 10  5  4  63  9  80  30  7  50
Dec 13    14:44:04-14:44:13    10  9  40  40  7  4  6  10  7  4
>

```

*Table 14-4:* Information displayed by specifying seconds

| Item        | Displayed information                                                                    |
|-------------|------------------------------------------------------------------------------------------|
| cpu average | The CPU utilization per second within the time range indicated under <code>time</code> . |

**Impact on communication**

None

**Response messages***Table 14-5:* List of response messages for the show cpu commands

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

**Notes**

None

---

## show processes

---

Shows information about processes being executed by the Switch.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

memory

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

cpu

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

### Operation when a stack configuration is used

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

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

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

### Example

- Show the memory usage of processes with a higher priority.

*Figure 14-5: Example of displaying the memory usage of processes*

```
> show processes memory
Date 20XX/01/23 12:00:00 UTC
PID  From      Text  Static Alloc Stack  Real  Process
 0  ??          0      0    0    0 24396  swapper
 1  ??          16      8   36    4   208   init
 2  ??          0      0    0    0 24396  tef_ev
 3  ??          0      0    0    0 24396  tef_io
 4  ??          0      0    0    0 24396  tef_led
 5  ??          0      0    0    0 24396  tffs_io
14  ??          0      0    0    0 24396  pagedaemon
15  ??          0      0    0    0 24396  ioflush
16  ??          0      0    0    0 24396  aiodoned
108 console      24     40    8    4   316  configEvent
110 console      20      4    8    4   140  configTimer
112 console      44     16   68   16   356  configResource
160 console     232     44   12   12   500  Node Control
162 console     120    168    8    8     0  Interface Control
163 console      20     24   16   12     0  Duplex Control
168 console      40     16   12   12   236  commandCpustat
180 ??          28     12  104   16     0  syslogd
212 console    3620    552  2272   16   556  configManager
215 ??          60     16   24    8   256  inetd
230 ??         408    976  5324    8   864  stpd
237 console     312   3052   24   12   624  gsrpd
241 console     252    716   28   40   612  L2MacManager
285 ??          72     16    8    4     0  sdwatchd
295 ??         2532   3120  4748   16  3352  rtm
312 ??          12      8    0    4     0  krfclogd
315 ??           8      8   16    4   100  snooper
```

```

350 console          72      28    132    16    556 RFC Log Control
362 console          16       12     24    24     0  getty
380 console          60     176    224    16    748 System Log Control
411 ??              52     284     72     4     0  ifidxd
431 192.168.111.50 3056    156    148    56 2228 cli
445 console        1480    308   3108    88 1372 snmpd
470 ??            1040   4820  4452    96 2832 nimd
502 console         144    172     52    16   484 configControl
505 console         212    268    300    20   260 rmon
563 console          44    104     16    12   248 Node Command Control
575 ??             200    112    428    16 1604 ntpd
607 console          84     24     16    36   244 configAPI
794 192.168.111.50   12      4     60     4   628 process
796 192.168.111.50  120     12     16     4   676 sh
1202 ??            68      16     96    12   948 telnetd
>

```

- Show the CPU usage of processes with a higher priority.

*Figure 14-6: Example of displaying the CPU usage of processes*

```

> show processes cpu
Date 20XX/01/23 12:00:00 UTC
PID From          5Sec    1Min    5Min  Runtime(ms) Process
 0 ??              0%      0%      0%        240 swapper
 1 ??              0%      0%      0%         25 init
 2 ??              0%      0%      0%          0 tef_ev
 3 ??              0%      0%      0%          0 tef_io
 4 ??              0%      0%      0%       1569 tef_led
 5 ??             9.48%   2.20%   0.78%      6075 tffs_io
14 ??              0%      0%      0%          6 pagedaemon
15 ??              0%      0%      0%     295260 ioflush
16 ??              0%      0%      0%         34 aiodoned
108 console        0%      0%      0%         319 configEvent
110 console        0%      0%      0%     115504 configTimer
112 console        0%      0%      0%        1868 configResource
160 console        0%      0%      0%     910476 Node Control
162 console        0%      0%      0%         26 Interface Control
163 console        0%      0%      0%         11 Duplex Control
168 console        0%      0%      0%     158688 commandCpustat
180 ??             0%      0%      0%         49 syslogd
212 console        0%      0%      0%         333 configManager
215 ??             0%      0%      0%         13 inetd
230 ??             0%      0%      0%     93299 stpd
237 console        0%      0%      0%        1011 gsrpd
241 console        0%      0%      0%        1564 L2MacManager
285 ??             0%      0%      0%          4 sdwatchd
295 ??             0%      0%      0%     324249 rtm
312 ??             0%      0%      0%          9 krfclogd
315 ??             0%      0%      0%         47 snooper
350 console        0%      0%      0%        3464 RFC Log Control
362 console        0%      0%      0%         13 getty
380 console        0.63%   0.24%   0.08%      1376 System Log Control
411 ??             0%      0%      0%       4047 ifidxd
431 192.168.111.50  5.06%   3.75%   0.28%        197 cli
445 console        0%      0%      0%     41847 snmpd
470 ??            0.63%   0.05%   0.02%    3717524 nimd
502 console        0%      0%      0%         558 configControl
505 console        0%      0%      0%     129625 rmon
563 console        0%      0%      0%     10313 Node Command Control
575 ??             0%      0%      0%       77018 ntpd
607 console        0%      0%      0%     43297 configAPI
873 192.168.111.50  0%      0%      0%          9 sh
921 192.168.111.50  0%      0%      0%          9 process
1202 ??            0%    0.22%   0.02%         32 telnetd
>

```

## Display items

*Table 14-6:* Explanation of the display items when the show processes command is executed

| Item    | Displayed information               | Displayed detailed information                                                                                                                                                           |
|---------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PID     | Process number                      | Displays the process management number for each process.                                                                                                                                 |
| From    | Input terminal                      | console<br>Management terminal connected to the serial port on the Switch<br>IP address<br>IP address of a remotely connected terminal<br>??<br>No terminal associated with this process |
| Text    | Text size                           | Shows the text size of each running process in kB.                                                                                                                                       |
| Static  | Static data size                    | Shows the size of static data area for each running process in kB.                                                                                                                       |
| Alloc   | Dynamic data size                   | Shows the size of dynamic data area for each running process in kB.                                                                                                                      |
| Stack   | Stack size                          | Shows the amount of stack usage for each running process in kB.                                                                                                                          |
| Real    | Real memory usage                   | Shows the size of real memory usage for each running process in kB.                                                                                                                      |
| Process | Function name                       | Shows the function name of each running process.                                                                                                                                         |
| 5Sec    | CPU usage for the past five seconds | Shows the CPU usage of each running process for the past five seconds in percentages.                                                                                                    |
| 1Min    | CPU usage for the past minute       | Shows the CPU usage of each running process for the past minute in percentages.                                                                                                          |
| 5Min    | CPU usage for the past five minutes | Shows the CPU usage of each running process for the past five minutes in percentages.                                                                                                    |
| Runtime | Actual run time of CPU              | Shows actual CPU run time for each running process in milliseconds.                                                                                                                      |

## Impact on communication

None

## Response messages

*Table 14-7:* List of response messages for the show processes command

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

## Notes

None

---

## show memory

---

Shows information about memory being used by the Switch.

### Syntax

```
show memory [summary]
```

### Input mode

User mode and administrator mode

### Parameters

summary

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

Operation when this parameter is omitted:

Shows information about pages related to processes with a higher priority in memory being used by the Switch.

### Operation when a stack configuration is used

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

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

### Example

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

*Figure 14-7: Example of displaying information about the physical memory being used*

```
> show memory summary
Date 20XX/01/23 12:00:00 UTC
physical memory = 262144KB(256.00MB)
used      memory = 158856KB(155.13MB)
free      memory = 103288KB(100.87MB)
```

- Display information about virtual memory related to processes with a higher priority in memory being used.

*Figure 14-8: Example of displaying information about the memory related to processes being used*

```
> show memory
Date 20XX/01/23 12:00:00 UTC
process init (pid: 1):
  start   size flag                                name
-----
01800000   20K read/exec                          / -?-
01814000    4K read/write/exec                    [ heap ]
01815000   32K read/write                        [ anon ]
41814000    4K read/exec                          [ uvm_aobj ]
41815000   36K read/write                        [ anon ]
41820000   52K read/write/exec                      /usr/libexec/ld.elf_so
4182D000    4K read/write/exec                    [ anon ]
41830000  760K read/exec                          /lib/libc.so.12.114.1
418EE000   60K                                /lib/libc.so.12.114.1
418FD000   36K read/write/exec                      /lib/libc.so.12.114.1
41906000   60K read/write/exec                        [ anon ]
41920000   40K read/exec                          /lib/libutil.so.7.3
4192A000   60K                                /lib/libutil.so.7.3
```

```

41939000      4K read/write/exec  /lib/libutil.so.7.3
4193A000      8K read/write/exec  [ anon ]
41940000     20K read/exec        /lib/libcrypt.so.0.1
41945000     60K                 /lib/libcrypt.so.0.1
41954000      4K read/write/exec  /lib/libcrypt.so.0.1
41955000     16K read/write/exec  [ anon ]
EE000000    30720K                [ stack ]
EFE00000    1984K read/write      [ stack ]
EFFF0000     64K read/write      [ stack ]

```

## Display items

The following table describes the items displayed when the `summary` parameter is specified.

*Table 14-8:* Information displayed when the `summary` parameter is specified

| Item            | Displayed information                               |
|-----------------|-----------------------------------------------------|
| physical memory | Displays the installed capacity of physical memory. |
| used memory     | Displays the used capacity of physical memory.      |
| free memory     | Displays the free capacity of physical memory.      |

The following table describes the items displayed when the `summary` parameter is omitted.

*Table 14-9:* Information displayed when the `summary` parameter is omitted

| Item    | Displayed information                                                                                                                                   |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| process | Displays the name of processes running in the device.                                                                                                   |
| pid     | Displays the number of processes running in the device.                                                                                                 |
| Start   | Displays the start address of virtual memory.                                                                                                           |
| size    | Displays the size of virtual memory.                                                                                                                    |
| Flag    | Displays the attribute of virtual memory.<br>[read] The memory can be read.<br>[write] The memory can be written.<br>[exec] The memory can be executed. |
| name    | Displays a summary of information in memory.                                                                                                            |

## Impact on communication

None

## Response messages

*Table 14-10:* List of response messages for the `show memory` command

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

## Notes

None

---

## df

---

Shows the available disk space.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

*<option>*

-t: Specifies the type of file system.

*<file name>*

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

### Operation when a stack configuration is used

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

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

### Example and display items

None

### Impact on communication

None

### Response messages

None

### Notes

None

---

## du

---

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

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

*<option>*

-s: Displays only the total number of blocks.

*<file name>*

Displays information about this file or directory.

### Operation when a stack configuration is used

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

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

### Example and display items

None

### Impact on communication

None

### Response messages

None

### Notes

None



## Chapter

---

# 15. Dump Information

---

erase dumpfile  
show dumpfile

---

## erase dumpfile

---

Deletes dump files stored in the dump file storage directory.

The dump file storage directory is /dump0 and /usr/var/hardware.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

all

Specifies all dump files.

<file name>

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

- rmdump: Memory dump file
- ni##.###: NIF failure dump file

### Operation when a stack configuration is used

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

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

### Example

- Delete all the dump files stored in the dump file storage directory.  
> erase dumpfile all
- Delete the rmdump dump file stored in the dump file storage directory.  
> erase dumpfile rmdump

### Impact on communication

None

### Response messages

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

| Message                                 | Description                                                                   |
|-----------------------------------------|-------------------------------------------------------------------------------|
| <file name>: No such file or directory. | The specified file does not exist. Or, the specified file is not a dump file. |
| Can't execute.                          | The command could not be executed. Re-execute the command.                    |

### Notes

None

---

## show dumpfile

---

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

### Syntax

```
show dumpfile
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

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

### Example

Display dump files stored in the dump file storage directory.

```
>show dumpfile
Date 20XX/05/02 06:29:25 UTC
[/dump0]:
  No dump file
[/usr/var/hardware]
  File name      ni00.000
  Date           20XX/03/03 12:08:32
  Version        OS-L3SA Ver. 11.5
  Serial No      TA03FA24T6XWS406006W003
  Factor         2101 25040201
```

### Display items

Table 15-2: Information displayed by the show dumpfile command

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

If there is no dump information in the dump file storage directory, `No dump file.` is displayed.

Similarly, if there is no dump file storage directory, `No such directory.` is displayed.

If the dump file fails to load, nothing is displayed.

### Impact on communication

None

## Response messages

*Table 15-3:* List of response messages for the show dumpfile command

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

## Notes

When the displayed content is for `rmddump`, the dump collection date (Date) is displayed in UTC time. Additionally, software type is not displayed in the version information. Instead, internal management information, which indicates software type is displayed in the version information.

## Chapter

---

# 16. Ethernet

---

```
show interfaces (10BASE-T/100BASE-TX/1000BASE-T)
show interfaces (100BASE-FX) [AX3650S]
show interfaces (1000BASE-X)
show interfaces (10GBASE-R)
show interfaces (40GBASE-R) [AX3800S]
clear counters
show port
activate
inactivate
test interfaces
no test interfaces
```

---

## show interfaces (10BASE-T/100BASE-TX/1000BASE-T)

---

Displays Ethernet information.

### Syntax

```
show interfaces gigabitethernet <switch no.>/<nif no.>/<port no.> [detail]
show interfaces tengigabitethernet <switch no.>/<nif no.>/<port no.> [detail]
```

### Input mode

User mode and administrator mode

### Parameters

gigabitethernet

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

tengigabitethernet [AX3800S]

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

<switch no.>/<nif no.>/<port no.>

Specifies the switch number, NIF number, and port number. For the specifiable range of values, see *Specifiable values for parameters*.

detail

Specifies that detailed statistics be displayed.

Operation when this parameter is omitted:

Detailed information is not displayed.

### Operation when a stack configuration is used

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

```
remote command <switch no.> show interfaces gigabitethernet <switch no.>/<nif no.>/<port no.> [detail]
```

### Example 1

The following shows an example of displaying the NIF information and detailed port information about the specified 10BASE-T/100BASE-TX/1000BASE-T interface.

*Figure 16-1:* Execution results when a 10BASE-T/100BASE-TX/1000BASE-T interface is specified

```
> show interfaces gigabitethernet 1/0/1
Date 20XX/03/04 12:34:36 UTC
NIF0:
Port1: active up 1000BASE-T full(auto) 0012.e245.0405 <-1
      Time-since-last-status-change:0:08:24 <-2
      Bandwidth:1000000kbps Average out:0Mbps Average in:0Mbps
      Peak out:1Mbps at 10:59:06 Peak in:1Mbps at 10:59:19
      Output rate: 0bps 0pps
      Input rate: 0bps 0pps
      Flow control send :off
      Flow control receive:off
      TPID:8100
      Frame size:1518 Octets retry:0 Interface name:gehl1/0/1
      description:test lab area network
      <Out octets/packets counter> <In octets/packets counter>
      Octets : 27706 Octets : 28994
      All packets : 272 All packets : 286
```

```

Unicast packets      :      271  Unicast packets      :      272
Multicast packets    :          0  Multicast packets    :       11
Broadcast packets    :          1  Broadcast packets    :          3
Pause packets        :          0  Pause packets        :          0
<Out line error counter>
Late collision        :          0  Defer indication      :          0
Single collision      :          0  Excessive deferral    :          0
Multiple collisions   :          0  Excessive collisions   :          0
Error frames          :          0
<In line error counter>
CRC errors            :          0  Symbol errors         :          0
Alignment             :          0  Fragments             :          0
Short frames          :          0  Jabber                 :          0
Long frames           :          0  Error frames           :          0
<Line fault counter>
Polarity changed      :          0  MDI cross over changed :          0
Link down             :          0
Link down in operational state :          0
In limit over         :          0
>

```

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

## Example 2

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

*Figure 16-2:* Execution results for the specification of 10BASE-T/100BASE-TX/1000BASE-T detailed statistics

```

>
> show interfaces gigabitethernet 1/0/1 detail
Date 20XX/03/04 12:35:06 UTC
NIF0:
Port1: active up 1000BASE-T full(auto) 0012.e245.0405
Time-since-last-status-change:0:08:54
Bandwidth:1000000kbps Average out:0Mbps Average in:0Mbps
Peak out:1Mbps at 10:59:06 Peak in:1Mbps at 10:59:19
Output rate:          0bps          0pps
Input rate:           0bps          0pps
Flow control send     :off
Flow control receive:off
TPID:8100
Frame size:1518 Octets retry:0 Interface name:geth1/0/1
description:test lab area network
<Out octets/packets counter>
Octets      :      27706  Octets      :      28994
All packets :          272  All packets :          286
Unicast packets :          271  Unicast packets :          272
Multicast packets :          0  Multicast packets :          11
Broadcast packets :          1  Broadcast packets :          3
Pause packets :          0  Pause packets :          0
64 packets :          1  64 packets :          13
65-127 packets :          271  65-127 packets :          271
128-255 packets :          0  128-255 packets :          1
256-511 packets :          0  256-511 packets :          1
>

```

```

512-1023 packets      :      0  512-1023 packets      :      0 |
1024-1518 packets    :      0  1024-1518 packets    :      0_|
:
:

```

&gt;

1. NIF information
2. Summary port information
3. Detailed port information
4. Send and receive statistics

## Display items in Example 1 and 2

The following tables describe the items displayed as the NIF information, detailed port information, and statistics about 10BASE-T/100BASE-TX/1000BASE-T interfaces.

*Table 16-1:* NIF information about 10BASE-T/100BASE-TX/1000BASE-T interfaces

| Item                  | Displayed information |         |
|-----------------------|-----------------------|---------|
|                       | Detailed information  | Meaning |
| NIF< <i>nif no.</i> > | NIF number            |         |

*Table 16-2:* Summary information about 10BASE-T/100BASE-TX/1000BASE-T interfaces

| Item                    | Displayed information   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         | Detailed information    | Meaning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Port< <i>port no.</i> > | Port number             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| < <i>port status</i> >  | active up               | Active (normal operating state)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                         | active down             | Active (A line failure occurred.)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                         | initialize              | Currently initializing or waiting for establishment of negotiation (auto-negotiation is operating)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                         | test                    | A line test is in progress.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                         | fault                   | Failed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                         | inactive                | <ul style="list-style-type: none"> <li>Operation was stopped by the <code>inactivate</code> command.</li> <li>The port has been deactivated by the standby link functionality of link aggregation.</li> <li>The port has been deactivated by the BPDU guard functionality of the Spanning Tree Protocol.</li> <li>The port has been deactivated by the port resetting functionality of GSRP.</li> <li>The port has been deactivated by the unidirectional link failure detection functionality.</li> <li>The port has been deactivated by the L2 loop detection functionality.</li> <li>The port has been deactivated by storm control.</li> </ul> |
|                         | disable                 | Operation was stopped by using the <code>shutdown</code> or <code>schedule-power-control shutdown</code> configuration command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| < <i>line type</i> >    | 10BASE-T half [AX3650S] | 10BASE-T half duplex                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Item                  | Displayed information           |                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | Detailed information            | Meaning                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                       | 10BASE-T half(auto) [AX3650S]   | 10BASE-T half duplex<br>(Line type determined by auto-negotiation.)                                                                                                                                                                                                                                                                                                                                                       |
|                       | 10BASE-T full                   | 10BASE-T full duplex                                                                                                                                                                                                                                                                                                                                                                                                      |
|                       | 10BASE-T full(auto)             | 10BASE-T full duplex<br>(Line type determined by auto-negotiation.)                                                                                                                                                                                                                                                                                                                                                       |
|                       | 100BASE-TX half [AX3650S]       | 100BASE-TX half duplex                                                                                                                                                                                                                                                                                                                                                                                                    |
|                       | 100BASE-TX half(auto) [AX3650S] | 100BASE-TX half duplex<br>(Line type determined by auto-negotiation.)                                                                                                                                                                                                                                                                                                                                                     |
|                       | 100BASE-TX full                 | 100BASE-TX full duplex                                                                                                                                                                                                                                                                                                                                                                                                    |
|                       | 100BASE-TX full(auto)           | 100BASE-TX full duplex<br>(Line type determined by auto-negotiation.)                                                                                                                                                                                                                                                                                                                                                     |
|                       | 1000BASE-T full(auto)           | 1000BASE-T full duplex<br>(Line type determined by auto-negotiation.)                                                                                                                                                                                                                                                                                                                                                     |
|                       | -                               | The line type is unknown.<br>A hyphen is displayed in the following cases: <ul style="list-style-type: none"> <li>• Auto-negotiation is enabled but the port status is neither <code>active up</code> nor <code>test</code>.</li> <li>• A port is in the <code>initialize</code> status.</li> <li>• A port is in the <code>fault</code> status.</li> <li>• The transceiver status is not <code>connect</code>.</li> </ul> |
| <MAC address>         | MAC address of the port         |                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <type of transceiver> | SFP                             | SFP                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <transceiver status>  | connect                         | Installed                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                       | notconnect                      | Not installed                                                                                                                                                                                                                                                                                                                                                                                                             |
|                       | not support                     | An unsupported transceiver is installed.                                                                                                                                                                                                                                                                                                                                                                                  |
|                       | -                               | The transceiver status is unknown.<br>A hyphen is displayed in the following cases: <ul style="list-style-type: none"> <li>• A port is in the <code>initialize</code> status.</li> <li>• A port is in the <code>fault</code> status.</li> </ul>                                                                                                                                                                           |

Table 16-3: Detailed information and statistics about 10BASE-T/100BASE-TX/1000BASE-T interfaces

| Item                          | Displayed information                                                                                                                                                                                                                                                                                                                                                                                                                                                    |         |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                               | Detailed information                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Meaning |
| Time-since-last-status-change | Displays the elapsed time since the last change in status.<br><code>hh:mm:ss</code> (when the elapsed time is 24 hours or less: <code>hh</code> = hours, <code>mm</code> = minutes, <code>ss</code> = seconds)<br><code>dd.hh:mm:ss</code> (when the elapsed time is more than 24 hours: <code>dd</code> = number of days, <code>hh</code> = hours, <code>mm</code> = minutes, <code>ss</code> = seconds)<br>Over 100 days (when the elapsed time is more than 100 days) |         |

| Item                                                      | Displayed information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                 |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
|                                                           | Detailed information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Meaning                         |
| Bandwidth:<bandwidth of line>kbps                         | <p>Displays the bandwidth of the line in kbps.</p> <p>If the <code>bandwidth</code> configuration command has not been executed, the line speed of the port is displayed. If the <code>bandwidth</code> configuration command has been executed, the setting value is displayed. Note that this setting does not control the bandwidth of the port.</p>                                                                                                                                                                                                               |                                 |
| Average out:<average bandwidth used on sending side>Mbps  | <p>Displays the average bandwidth (in Mbps) used on the sending side of the line for the one minute interval before the command was executed.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>             |                                 |
| Average in:<average bandwidth used on receiving side>Mbps | <p>Displays the average bandwidth (in Mbps) used on the receiving side of the line for the one minute interval before the command was executed.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>           |                                 |
| Peak out                                                  | <p>Displays the maximum bandwidth used on the sending side of the line for the 24-hour interval before the command was executed, and the relevant time.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>   |                                 |
| Peak in                                                   | <p>Displays the maximum bandwidth used on the receiving side of the line for the 24-hour interval before the command was executed, and the relevant time.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p> |                                 |
| Output rate <sup>#1</sup>                                 | <p>Displays the send throughput of the line (in bps and pps) for the one second interval before the command was executed, rounded to two decimal places.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>                                                                                                                                                                                                                                                                                              |                                 |
| Input rate <sup>#1</sup>                                  | <p>Displays the receive throughput of the line (in bps and pps) for the one second interval before the command was executed, rounded to two decimal places.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>                                                                                                                                                                                                                                                                                           |                                 |
| Flow control send <sup>#2</sup>                           | on [AX3650S]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | A pause packet is sent.         |
|                                                           | off                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | A pause packet is not sent.     |
| Flow control receive <sup>#2</sup>                        | on [AX3650S]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | A pause packet is received.     |
|                                                           | off                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | A pause packet is not received. |
| TPID                                                      | <p>Displays a <code>TagProtocolIdentifier</code> value that is used on the port to identify the VLAN.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                 |

| Item                                    |                                                      | Displayed information                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                              |
|-----------------------------------------|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
|                                         |                                                      | Detailed information                                                                                                                                                                                                                                                                                                                                                   | Meaning                                                                                                                                      |
| Frame size <sup>#3</sup>                |                                                      | Displays the maximum frame length of a port in octets.<br>The maximum frame length is calculated starting from the MAC header and ending with the DATA and PAD fields. For details about frame formats, see the description of frame formats in <i>16.1.3 Control on the MAC and LLC sublayers</i> in the manual <i>Configuration Guide Vol. 1 For Version 11.10</i> . |                                                                                                                                              |
| retry:<Counts>                          |                                                      | Displays the number of times the port was reactivated due to a fault.                                                                                                                                                                                                                                                                                                  |                                                                                                                                              |
| Interface name                          |                                                      | Displays the name assigned to a port.                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                              |
| description:<supplementary explanation> |                                                      | Displays the contents of the <code>description</code> configuration.<br>The <code>description</code> configuration can be used to set comments, such as a comment about the purpose of the port. This item is not displayed if the description configuration has not been set.                                                                                         |                                                                                                                                              |
| Statistics                              | Category                                             | <Out octets/packets counter>                                                                                                                                                                                                                                                                                                                                           | Send statistics                                                                                                                              |
|                                         |                                                      | <In octets/packets counter>                                                                                                                                                                                                                                                                                                                                            | Receive statistics                                                                                                                           |
|                                         |                                                      | <Out line error counter>                                                                                                                                                                                                                                                                                                                                               | Send error statistics                                                                                                                        |
|                                         |                                                      | <In line error counter>                                                                                                                                                                                                                                                                                                                                                | Receive error statistics                                                                                                                     |
|                                         |                                                      | <Line fault counter>                                                                                                                                                                                                                                                                                                                                                   | Failure statistics                                                                                                                           |
|                                         | Detailed statistical items for sending and receiving | Octets                                                                                                                                                                                                                                                                                                                                                                 | The number of octets<br>Calculation of octet values is based on the range from the MAC header to the FCS field over the length of the frame. |
|                                         |                                                      | All packets                                                                                                                                                                                                                                                                                                                                                            | Number of packets (including error packets)                                                                                                  |
|                                         |                                                      | Unicast packets                                                                                                                                                                                                                                                                                                                                                        | Number of unicast packets                                                                                                                    |
|                                         |                                                      | Multicast packets                                                                                                                                                                                                                                                                                                                                                      | Number of multicast packets                                                                                                                  |
|                                         |                                                      | Broadcast packets                                                                                                                                                                                                                                                                                                                                                      | Number of broadcast packets                                                                                                                  |
|                                         |                                                      | Pause packets                                                                                                                                                                                                                                                                                                                                                          | Number of pause packets                                                                                                                      |
|                                         |                                                      | 64 packets                                                                                                                                                                                                                                                                                                                                                             | The number of packets whose frame length is 64 octets.                                                                                       |
|                                         |                                                      | 65-127 packets                                                                                                                                                                                                                                                                                                                                                         | The number of packets whose frame length is from 65 to 127 octets.                                                                           |
|                                         |                                                      | 128-255 packets                                                                                                                                                                                                                                                                                                                                                        | The number of packets whose frame length is from 128 to 255 octets.                                                                          |
|                                         |                                                      | 256-511 packets                                                                                                                                                                                                                                                                                                                                                        | The number of packets whose frame length is from 256 to 511 octets.                                                                          |
|                                         |                                                      | 512-1023 packets                                                                                                                                                                                                                                                                                                                                                       | The number of packets whose frame length is from 512 to 1023 octets.                                                                         |
|                                         |                                                      | 1024-1518 packets                                                                                                                                                                                                                                                                                                                                                      | The number of packets whose frame length is from 1024 to 1518 octets. <sup>#4</sup>                                                          |
|                                         | Detailed statistical items for send errors           | Late collision                                                                                                                                                                                                                                                                                                                                                         | The number of collisions detected after the 512-bit time has elapsed                                                                         |

| Item |                                               | Displayed information  |                                                                                                                                                                  |
|------|-----------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                               | Detailed information   | Meaning                                                                                                                                                          |
|      |                                               | Single collision       | The number of transmissions that were successful after one collision                                                                                             |
|      |                                               | Multiple collisions    | The number of transmissions that were successful after two or more collisions                                                                                    |
|      |                                               | Defer indication       | The number of times the initial transmission was delayed because the transmit line was busy                                                                      |
|      |                                               | Excessive deferral     | The number of times an excessive delay occurred                                                                                                                  |
|      |                                               | Excessive collisions   | The number of transfer failures due to excessive collisions (16 collisions)                                                                                      |
|      |                                               | Error frames           | The total number of frames discarded due to errors (total value of the following items: Late collision, Excessive deferral, Excessive collisions)                |
|      | Detailed statistical items for receive errors | CRC errors             | The number of times the frame length was valid but an error was detected by the FCS check <sup>#5</sup>                                                          |
|      |                                               | Alignment              | The number of times the frame length was invalid and an error was detected by the FCS check <sup>#5</sup>                                                        |
|      |                                               | Fragments              | The number of times a short frame (whose length is shorter than 64 octets) is received and an FCS error or an alignment error occurred <sup>#5</sup>             |
|      |                                               | Jabber                 | The number of times a long frame (whose length exceeds the max frame length) was received and an FCS error or an alignment error occurred <sup>#5</sup>          |
|      |                                               | Symbol errors          | The number of symbol errors that occurred                                                                                                                        |
|      |                                               | Short frames           | The number of received packets that are shorter than the frame length <sup>#5</sup>                                                                              |
|      |                                               | Long frames            | The number of received packets that exceed the frame length <sup>#5</sup>                                                                                        |
|      |                                               | Error frames           | The total number of frames discarded due to errors (total value of the following items: Short frames, Fragments, Jabber, CRC errors, Long frames, Symbol errors) |
|      | Detailed statistical items for errors         | Polarity changed       | The number of times the polarity of the send or receive pin of a twisted pair cable was changed                                                                  |
|      |                                               | MDI cross over changed | The number of times the send or receive pin of a twisted pair cable was changed                                                                                  |

| Item |  | Displayed information          |                                                                                             |
|------|--|--------------------------------|---------------------------------------------------------------------------------------------|
|      |  | Detailed information           | Meaning                                                                                     |
|      |  | Link down                      | The number of times a link was not established                                              |
|      |  | Link down in operational state | The number of link failures that occurred during communication (a link was not established) |
|      |  | In limit over                  | The number of frames discarded due to exceeded receiving capacity                           |

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

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

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

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

#4: The number of received long frames without VLAN Tag is included.

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

For details about frame formats, see *16.1.3 Control on the MAC and LLC sublayers* in the manual *Configuration Guide Vol. 1 For Version 11.10*.

### Example 3 [AX3800S]

The following shows an example of displaying the NIF information and detailed port information about the 1000BASE-T interface on SFP+/SFP ports.

*Figure 16-3: Execution result when 1000BASE-T is specified on SFP/SFP+ ports*

```
> show interfaces tengigabitethernet 1/0/1
Date 20XX/03/04 13:19:35 UTC
NIF0:
Port1: active up 1000BASE-T full(auto) 0012.e222.1d55
      SFP connect
      Time-since-last-status-change:0:01:03
      Bandwidth:1000000kbps Average out:1Mbps Average in:3Mbps
      Peak out:6Mbps at 13:13:53 Peak in:3Mbps at 13:13:53
      Output rate: 6144.0kbps 12.0kpps
      Input rate: 3072.0kbps 6000pps
      Flow control send :off
      Flow control receive:off
      TPID:8100
      Frame size:1518 Octets retry:0 Interface name:tengeth1/0/1
      description:test lab area network
      <Out octets/packets counter>
      Octets : 2334720
      All packets : 36480
      Unicast packets : 6080
      Multicast packets : 18240
      Broadcast packets : 12160
      Pause packets : 0
      <In octets/packets counter>
      Octets : 1167360
      All packets : 18240
      Unicast packets : 3040
      Multicast packets : 9120
      Broadcast packets : 6080
      Pause packets : 0
```

```
<In line error counter>
CRC errors          : 0
Fragments          : 0
Jabber             : 0
Symbol errors      : 0
Short frames       : 0
Long frames        : 0
Error frames       : 0
<Line fault counter>
Link down          : 0
TX fault           : 0
Signal detect errors : 0
Transceiver notconnect : 0
Link down in operational state : 0
Signal detect errors in operational state : 0
Transceiver notconnect in operational state : 0
In limit over      : 0
```

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

Example 4 [AX3800S]

The following shows an example of displaying the NIF information, detailed port information, and detailed statistics about the 1000BASE-X interface on SFP+/SFP ports.

Figure 16-4: Execution result of displaying detailed statistics when 1000BASE-T is specified on SFP/SFP+ ports

```
> show interfaces tengigabitethernet 1/0/1 detail
Date 20XX/01/21 12:20:28 JST
NIF0:
Port1: active up 1000BASE-T full(auto) 0012.e222.1d55
SFP connect
Time-since-last-status-change:0:01:11
Bandwidth:1000000kbps Average out:2Mbps Average in:3Mbps
Peak out:6Mbps at 13:13:53 Peak in:3Mbps at 13:13:53
Output rate: 6144.0kbps 12.0kpps
Input rate: 3072.0kbps 6000pps
Flow control send :off
Flow control receive:off
TPID:8100
Frame size:1518 Octets retry:0 Interface name:tengeth1/0/1
description:test lab area network
<Out octets/packets counter>
Octets          : 8532608
All packets     : 133322
Unicast packets : 22220
Multicast packets : 66662
Broadcast packets : 44440
Pause packets   : 0
64 packets      : 133322
65-127 packets  : 0
128-255 packets : 0
256-511 packets : 0
512-1023 packets : 0
1024-1518 packets : 0
```

```

<In octets/packets counter>
Octets : 4266304 -
All packets : 66661
Unicast packets : 11110
Multicast packets : 33331
Broadcast packets : 22220
Pause packets : 0 5
64 packets : 66661
65-127 packets : 0
128-255 packets : 0
256-511 packets : 0
512-1023 packets : 0
1024-1518 packets : 0
:
:
>

```

1. NIF information
2. Summary port information
3. Detailed port information
4. Send statistics
5. Receive statistics

### Display items in Example 3 and 4 [AX3800S]

The following tables describe the items displayed as the NIF information, detailed port information, and statistics about the 1000BASE-T interface on SFP+/SFP ports.

*Table 16-4:* NIF information about 1000BASE-T interface on SFP+/SFP ports

Item	Displayed information	
	Detailed information	Meaning
NIF<nif no.>	NIF number	

*Table 16-5:* Summary information about 1000BASE-T interface on SFP+/SFP ports

Item	Displayed information	
	Detailed information	Meaning
Port<port no.>	Port number	
<port status>	active up	Active (normal operating state)
	active down	Active (A line failure occurred.)
	initialize	Currently initializing or waiting for establishment of negotiation (auto-negotiation is operating)
	test	A line test is in progress.
	fault	Failed

Item	Displayed information	
	Detailed information	Meaning
	inactive	<ul style="list-style-type: none"> <li>Operation was stopped by the <code>inactivate</code> command.</li> <li>The port has been deactivated by the standby link functionality of link aggregation.</li> <li>The port has been deactivated by the BPDU guard functionality of the Spanning Tree Protocol.</li> <li>The port has been deactivated by the port resetting functionality of GSRP.</li> <li>The port has been deactivated by the unidirectional link failure detection functionality.</li> <li>The port has been deactivated by the L2 loop detection functionality.</li> <li>The port has been deactivated by storm control.</li> </ul>
	disable	Operation was stopped by using the <code>shutdown</code> or <code>schedule-power-control shutdown</code> configuration command.
<line type>	1000BASE-T full(auto)	100BASE-T full duplex (Line type determined by auto-negotiation.)
	-	The line type is unknown. A hyphen is displayed in the following cases: <ul style="list-style-type: none"> <li>Auto-negotiation is enabled but the port status is neither <code>active up</code> nor <code>test</code>.</li> <li>A port is in the <code>initialize</code> status.</li> <li>A port is in the <code>fault</code> status.</li> <li>The transceiver status is not <code>connect</code>.</li> </ul>
<MAC address>	MAC address of the port	
<type of transceiver>	SFP	SFP
	-	The transceiver type is unknown.
<transceiver status>	connect	Installed
	notconnect	Not installed
	not support	An unsupported transceiver is installed.
	-	The transceiver status is unknown. A hyphen is displayed in the following cases: <ul style="list-style-type: none"> <li>A port is in the <code>initialize</code> status.</li> <li>A port is in the <code>fault</code> status.</li> </ul>

Table 16-6: Detailed information and statistics about 1000BASE-T interface on SFP+/SFP ports

Item	Displayed information	
	Detailed information	Meaning
Time-since-last-status-change	Displays the elapsed time since the last change in status. <code>hh:mm:ss</code> (when the elapsed time is 24 hours or less: <code>hh</code> = hours, <code>mm</code> = minutes, <code>ss</code> = seconds) <code>dd.hh:mm:ss</code> (when the elapsed time is more than 24 hours: <code>dd</code> = number of days, <code>hh</code> = hours, <code>mm</code> = minutes, <code>ss</code> = seconds) Over 100 days (when the elapsed time is more than 100 days)	

Item	Displayed information	
	Detailed information	Meaning
Bandwidth:< <i>bandwidth of line</i> >kbps	<p>Displays the bandwidth of the line in kbps.</p> <p>If the <code>bandwidth</code> configuration command has not been executed, the line speed of the port is displayed. If the <code>bandwidth</code> configuration command has been executed, the setting value is displayed. Note that this setting does not control the bandwidth of the port.</p>	
Average out:< <i>average bandwidth used on sending side</i> >Mbps	<p>Displays the average bandwidth (in Mbps) used on the sending side of the line for the one minute interval before the command was executed.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Average in:< <i>average bandwidth used on receiving side</i> >Mbps	<p>Displays the average bandwidth (in Mbps) used on the receiving side of the line for the one minute interval before the command was executed.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Peak out	<p>Displays the maximum bandwidth used on the sending side of the line for the 24-hour interval before the command was executed, and the relevant time.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Peak in	<p>Displays the maximum bandwidth used on the receiving side of the line for the 24-hour interval before the command was executed, and the relevant time.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Output rate <sup>#1</sup>	<p>Displays the send throughput of the line (in bps and pps) for the one second interval before the command was executed, rounded to two decimal places.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Input rate <sup>#1</sup>	<p>Displays the receive throughput of the line (in bps and pps) for the one second interval before the command was executed, rounded to two decimal places.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Flow control send <sup>#2</sup>	off	A pause packet is not sent.
Flow control receive <sup>#2</sup>	off	A pause packet is not received.
TPID	<p>Displays a <code>TagProtocolIdentifier</code> value that is used on the port to identify the VLAN.</p>	

Item		Displayed information	
		Detailed information	Meaning
Frame size <sup>#3</sup>		Displays the maximum frame length of a port in octets. The maximum frame length is calculated starting from the MAC header and ending with the DATA and PAD fields. For details about frame formats, see the description of frame formats in <i>16.1.3 Control on the MAC and LLC sublayers</i> in the manual <i>Configuration Guide Vol. 1 For Version 11.10</i> .	
retry:<Counts>		Displays the number of times the port was reactivated due to a fault.	
Interface name		Displays the name assigned to a port.	
description: <supplementary explanation>		Displays the contents of the <code>description</code> configuration. The <code>description</code> configuration can be used to set comments, such as a comment about the purpose of the port. This item is not displayed if the description configuration has not been set.	
Statistics	Category	<Out octets/packets counter>	Send statistics
		<In octets/packets counter>	Receive statistics
		<In line error counter>	Receive error statistics
		<Line fault counter>	Failure statistics
	Detailed statistical items for sending and receiving	Octets	The number of octets Calculation of octet values is based on the range from the MAC header to the FCS field over the length of the frame.
		All packets	Number of packets (including error packets)
		Unicast packets	Number of unicast packets
		Multicast packets	Number of multicast packets
		Broadcast packets	Number of broadcast packets
		Pause packets	Number of pause packets
		64 packets	The number of packets whose frame length is 64 octets.
		65-127 packets	The number of packets whose frame length is from 65 to 127 octets.
		128-255 packets	The number of packets whose frame length is from 128 to 255 octets.
		256-511 packets	The number of packets whose frame length is from 256 to 511 octets.
		512-1023 packets	The number of packets whose frame length is from 512 to 1023 octets.
		1024-1518 packets	The number of packets whose frame length is from 1024 to 1518 octets. <sup>#4</sup>
	Detailed statistical items for receive errors	CRC errors	The number of times the frame length was valid but an error was detected by the FCS check <sup>#5</sup>

Item		Displayed information	
		Detailed information	Meaning
		Fragments	The number of times a short frame (whose length is shorter than 64 octets) was received and an FCS error or an alignment error occurred <sup>#5</sup>
		Jabber	The number of times a long frame (whose length exceeds the max frame length) was received and an FCS error or an alignment error occurred <sup>#5</sup>
		Symbol errors	The number of symbol errors that occurred
		Short frames	The number of received packets that are shorter than the frame length <sup>#5</sup>
		Long frames	The number of received packets that exceed the frame length <sup>#5</sup>
		Error frames	The total number of frames discarded due to errors (total value of the following items: Short frames, Fragments, Jabber, CRC errors, Long frames, Symbol errors)
	Detailed statistical items for errors	Link down	The number of times a link was not established
		TX fault	The number of times a send line failure occurred
		Signal detect errors	The number of times a signal line could not be detected
		Transceiver notconnect	The number of times a transceiver was disconnected
		Link down in operational state	The number of link failures that occurred during communication (a link was not established)
		Signal detect errors in operational state	The number of failures that occurred during communication (signal line was not detected)
		Transceiver notconnect in operational state	The number of failures that occurred during communication (transceiver was removed)
		In limit over	The number of frames discarded due to exceeded receiving capacity

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

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

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

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

#4: The number of received long frames without VLAN Tag is included.

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

For details about frame formats, see *16.1.3 Control on the MAC and LLC sublayers* in the manual *Configuration Guide Vol. 1 For Version 11.10*.

## Impact on communication

None

## Response messages

*Table 16-7:* List of response messages for the show interfaces (10BASE-T/100BASE-TX/1000BASE-T) (Ethernet) command

Message	Description
<switch no.>/<nif no.>/<port no.> is not gigabitethernet.	The interface of the specified port is not gigabitethernet. Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<switch no.>/<nif no.>/<port no.> is not tengigabitethernet.	The interface of the specified port is not tengigabitethernet. Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The port number is outside the valid range. Make sure the specified parameter is correct. <port no.>: Indicates the port number.

## Notes

All display items are cleared in the following cases:

- When the Switch starts up
- The `restart vlan` command is executed.
- When a device hardware failure occurs
- An error occurs in the network interface management program (nimd).

# show interfaces (100BASE-FX) [AX3650S]

Displays Ethernet information.

## Syntax

show interfaces gigabitethernet <switch no.>/<nif no.>/<port no.> [detail]

## Input mode

User mode and administrator mode

## Parameters

gigabitethernet

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

<switch no.>/<nif no.>/<port no.>

Specifies the switch number, NIF number, and port number. For the specifiable range of values, see *Specifiable values for parameters*.

detail

Specifies that detailed statistics be displayed.

Operation when this parameter is omitted:

Detailed information is not displayed.

## Operation when a stack configuration is used

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

remote command <switch no.> show interfaces gigabitethernet <switch no.>/<nif no.>/<port no.> [detail]

## Example 1

The following shows an example of displaying the NIF information and detailed port information about the 100BASE-FX interface.

Figure 16-5: Execution result when 100BASE-FX is specified

```
> show interfaces gigabitethernet 1/0/1
Date 20XX/04/08 19:21:08 JST
NIF0:
Port1: active up 100BASE-FX full 0012.e222.1e31
      SFP connect
      Time-since-last-status-change:0:00:59
      Bandwidth:100000kbps Average out:47Mbps Average in:47Mbps
      Peak out:87Mbps at 19:20:42 Peak in:87Mbps at 19:20:42
      Output rate:      86.1Mbps      86.8kpps
      Input rate:      86.1Mbps      86.8kpps
      Flow control send :on
      Flow control receive:off
      TPID:8100
      Frame size:1518 Octets retry:0 Interface name:geth1/0/1
      description:test lab area network
      <Out octets/packets counter>      <In octets/packets counter>
      Octets      :      357504400      Octets      :      357504152
      All packets :      2883099      All packets :      2883098
      Unicast packets :      2882963      Unicast packets :      2882997
      Multicast packets :      73      Multicast packets :      49
      Broadcast packets :      64      Broadcast packets :      40
      Pause packets :      0      Pause packets :      0
      <Out line error counter>
```

```

Late collision      :      0  Defer indication      :      0 |
Single collision   :      0  Excessive deferral   :      0 | 5
Multiple collisions :      0  Excessive collisions :      0 |
Error frames       :      0  -                - |
<In line error counter>
CRC errors         :      0  Symbol errors       :      0 |
Fragments         :      0  Short frames        :      0 | 6
Jabber            :      0  Long frames         :      0 |
Error frames       :      0  -                - |
<Line fault counter>
Link down         :      0  Signal detect errors :      0 |
TX fault          :      0  Transceiver notconnect :      0 |
Link down in operational state :      0 | 7
Signal detect errors in operational state :      0 |
Transceiver notconnect in operational state :      0 |
In limit over     :      0  -                - |
>

```

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

## Example 2

The following shows an example of displaying the NIF information, detailed port information, and detailed statistics about the 100BASE-FX interface.

*Figure 16-6: Execution results for the specification of 100BASE-FX detailed statistics*

```

> show interfaces gigabitethernet 1/0/1 detail
Date 20XX/04/08 19:21:52 JST
NIF0:
Port1: active up 100BASE-FX full 0012.e222.1e31
SFP connect
Time-since-last-status-change:0:01:43
Bandwidth:100000kbps Average out:86Mbps Average in:86Mbps
Peak out:87Mbps at 19:20:42 Peak in:87Mbps at 19:20:42
Output rate:      86.1Mbps      86.8kpps
Input rate:       86.1Mbps      86.8kpps
Flow control send :on
Flow control receive:off
TPID:8100
Frame size:1518 Octets retry:0 Interface name:ge1/0/1
description:test lab area network
<Out octets/packets counter>      <In octets/packets counter>
Octets      :      825085584  Octets      :      825085336
All packets :      6653915    All packets :      6653914
Unicast packets :      6653779  Unicast packets :      6653813
Multicast packets :      73    Multicast packets :      49
Broadcast packets :      64    Broadcast packets :      40
Pause packets :      0        Pause packets :      0
64 packets :      0          64 packets :      0
65-127 packets :      6653915  65-127 packets :      6653914
128-255 packets :      0        128-255 packets :      0
256-511 packets :      0        256-511 packets :      0
512-1023 packets :      0        512-1023 packets :      0
1024-1518 packets :      0      1024-1518 packets :      0
:
:
>

```

1. NIF information
2. Summary port information
3. Detailed port information
4. Send and receive statistics

## Display items in Example 1 and 2

The following tables describe the items displayed as the NIF information, detailed port information, and statistics about the 100BASE-FX interface.

Table 16-8: NIF information about 100BASE-FX interfaces

Item	Displayed information	
	Detailed information	Meaning
NIF<nif no.>	NIF number	

Table 16-9: Summary information about 100BASE-FX interfaces

Item	Displayed information	
	Detailed information	Meaning
Port<port no.>	Port number	
<port status>	active up	Active (normal operating state)
	active down	Active (A line failure occurred.)
	initialize	Currently initializing
	test	A line test is in progress.
	fault	Failed
	inactive	<ul style="list-style-type: none"> <li>Operation was stopped by the <code>inactivate</code> command.</li> <li>The port has been deactivated by the standby link functionality of link aggregation.</li> <li>The port has been deactivated by the BPDU guard functionality of the Spanning Tree Protocol.</li> <li>The port has been deactivated by the port resetting functionality of GSRP.</li> <li>The port has been deactivated by the unidirectional link failure detection functionality.</li> <li>The port has been deactivated by the L2 loop detection functionality.</li> <li>The port has been deactivated by storm control.</li> </ul>
	disable	Operation was stopped by using the <code>shutdown</code> or <code>schedule-power-control shutdown</code> configuration command.
<line type>	100BASE-FX full	100BASE-FX full duplex
	100BASE-FX half	100BASE-FX half duplex

Item	Displayed information	
	Detailed information	Meaning
	-	<p>The line type is unknown.</p> <p>A hyphen is displayed in the following cases:</p> <ul style="list-style-type: none"> <li>• A port is in the <code>initialize</code> status.</li> <li>• A port is in the <code>fault</code> status.</li> <li>• The transceiver status is not <code>connect</code>.</li> </ul>
<MAC address>	MAC address of the port	
<type of transceiver>	SFP	SFP
<transceiver status>	connect	Installed
	notconnect	Not installed
	not support	An unsupported transceiver is installed.
	-	<p>The transceiver status is unknown.</p> <p>A hyphen is displayed in the following cases:</p> <ul style="list-style-type: none"> <li>• A port is in the <code>initialize</code> status.</li> <li>• A port is in the <code>fault</code> status.</li> </ul>

Table 16-10: Detailed information and statistics about 100BASE-FX interfaces

Item	Displayed information	
	Detailed information	Meaning
Time-since-last-status-change	<p>Displays the elapsed time since the last change in status.</p> <p><i>hh:mm:ss</i> (when the elapsed time is 24 hours or less: <i>hh</i> = hours, <i>mm</i> = minutes, <i>ss</i> = seconds)</p> <p><i>dd.hh:mm:ss</i> (when the elapsed time is more than 24 hours: <i>dd</i> = number of days, <i>hh</i> = hours, <i>mm</i> = minutes, <i>ss</i> = seconds)</p> <p>Over 100 days (when the elapsed time is more than 100 days)</p>	
Bandwidth:<bandwidth of line>kbps	<p>Displays the bandwidth of the line in kbps.</p> <p>If the <code>bandwidth</code> configuration command has not been executed, the line speed of the port is displayed. If the <code>bandwidth</code> configuration command has been executed, the setting value is displayed. Note that this setting does not control the bandwidth of the port.</p>	
Average out:<average bandwidth used on sending side>Mbps	<p>Displays the average bandwidth (in Mbps) used on the sending side of the line for the one minute interval before the command was executed.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Average in:<average bandwidth used on receiving side>Mbps	<p>Displays the average bandwidth (in Mbps) used on the receiving side of the line for the one minute interval before the command was executed.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	

Item		Displayed information	
		Detailed information	Meaning
Peak out		Displays the maximum bandwidth used on the sending side of the line for the 24-hour interval before the command was executed, and the relevant time. 0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place. The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.	
Peak in		Displays the maximum bandwidth used on the receiving side of the line for the 24-hour interval before the command was executed, and the relevant time. 0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place. The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.	
Output rate <sup>#1</sup>		Displays the send throughput of the line (in bps and pps) for the one second interval before the command was executed, rounded to two decimal places. The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.	
Input rate <sup>#1</sup>		Displays the receive throughput of the line (in bps and pps) for the one second interval before the command was executed, rounded to two decimal places. The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.	
Flow control send <sup>#2</sup>		on	A pause packet is sent.
		off	A pause packet is not sent.
Flow control receive <sup>#2</sup>		on	A pause packet is received.
		off	A pause packet is not received.
TPID		Displays a TagProtocolIdentifier value that is used on the port to identify the VLAN.	
Frame size <sup>#3</sup>		Displays the maximum frame length of a port in octets. The maximum frame length is calculated starting from the MAC header and ending with the DATA and PAD fields. For details about frame formats, see the description of frame formats in 16.1.3 Control on the MAC and LLC sublayers in the manual Configuration Guide Vol. 1 For Version 11.10.	
retry:<Counts>		Displays the number of times the port was reactivated due to a fault.	
Interface name		Displays the name assigned to a port.	
description:<supplementary explanation>		Displays the contents of the description configuration. The description configuration can be used to set comments, such as a comment about the purpose of the port. This item is not displayed if the description configuration has not been set.	
Statistics	Category	<Out octets/packets counter>	Send statistics
		<In octets/packets counter>	Receive statistics
		<Out line error counter>	Send error statistics
		<In line error counter>	Receive error statistics
		<Line fault counter>	Failure statistics

Item		Displayed information	
		Detailed information	Meaning
	Detailed statistical items for sending and receiving	Octets	The number of octets Calculation of octet values is based on the range from the MAC header to the FCS field over the length of the frame.
		All packets	Number of packets (including error packets)
		Unicast packets	Number of unicast packets
		Multicast packets	Number of multicast packets
		Broadcast packets	Number of broadcast packets
		Pause packets	Number of pause packets
		64 packets	The number of packets whose frame length is 64 octets.
		65-127 packets	The number of packets whose frame length is from 65 to 127 octets.
		128-255 packets	The number of packets whose frame length is from 128 to 255 octets.
		256-511 packets	The number of packets whose frame length is from 256 to 511 octets.
		512-1023 packets	The number of packets whose frame length is from 512 to 1023 octets.
		1024-1518 packets	The number of packets whose frame length is from 1024 to 1518 octets. <sup>#4</sup>
	Detailed statistical items for send error <sup>#5</sup>	Late collision	The number of collisions detected after the 512-bit time has elapsed
		Defer indication	The number of times the initial transmission was delayed because the transmit line was busy
		Single collision	The number of transmissions that were successful after one collision
		Excessive deferral	The number of times an excessive delay occurred
		Multiple collisions	The number of transmissions that were successful after two or more collisions
		Excessive collisions	The number of transfer failures due to excessive collisions (16 collisions)
		Error frames	The total number of frames discarded due to errors (total value of the following items: Late collision, Excessive deferral, Excessive collisions)

Item		Displayed information	
		Detailed information	Meaning
	Detailed statistical items for receive errors	CRC errors	The number of times the frame length was valid but an error was detected by the FCS check <sup>#6</sup>
		Symbol errors	The number of symbol errors that occurred
		Fragments	The number of times a short frame (whose length is shorter than 64 octets) is received and an FCS error or an alignment error occurred <sup>#6</sup>
		Jabber	The number of times a long frame (whose length exceeds the max frame length) was received and an FCS error or an alignment error occurred <sup>#6</sup>
		Short frames	The number of received packets that are shorter than the frame length <sup>#6</sup>
		Long frames	The number of received packets that exceed the frame length <sup>#6</sup>
		Error frames	The total number of frames discarded due to errors (total value of the following items: Short frames, Fragments, Jabber, CRC errors, Long frames, Symbol errors)
	Detailed statistical items for errors	Link down	The number of times a link was not established
		TX fault	The number of times a send line failure occurred
		Signal detect errors	The number of times a signal line could not be detected
		Transceiver notconnect	The number of times a transceiver was removed
		Link down in operational state	The number of link failures that occurred during communication (a link was not established)
		Signal detect errors in operational state	The number of failures that occurred during communication (signal line was not detected)
		Transceiver notconnect in operational state	The number of failures that occurred during communication (transceiver was removed)
		In limit over	The number of frames discarded due to exceeded receiving capacity

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

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

displayed below the decimal point.

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

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

#4: The number of received long frames without VLAN Tag is included.

#5: This value is counted only when 100BASE-FX is used in half-duplex mode.

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

For details about frame formats, see *16.1.3 Control on the MAC and LLC sublayers* in the manual *Configuration Guide Vol. 1 For Version 11.10*.

## Impact on communication

None

## Response messages

*Table 16-11:* List of response messages for the `show interfaces (100BASE-FX) (Ethernet)` command

Message	Description
<switch no.>/<nif no.>/<port no.> is not gigabitethernet.	The interface of the specified port is not gigabitethernet. Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The port number is outside the valid range. Make sure the specified parameter is correct. <port no.>: Indicates the port number.

## Notes

All display items are cleared in the following cases:

- When the Switch starts up
- The `restart vlan` command is executed.
- When a device hardware failure occurs
- An error occurs in the network interface management program (nimd).

---

## show interfaces (1000BASE-X)

---

Displays Ethernet information.

### Syntax

```
show interfaces gigabitethernet <switch no.>/<nif no.>/<port no.> [detail]
show interfaces tengigabitethernet <switch no.>/<nif no.>/<port no.> [detail]
```

### Input mode

User mode and administrator mode

### Parameters

gigabitethernet [AX3650S]

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

tengigabitethernet

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

<switch no.>/<nif no.>/<port no.>

Specifies the switch number, NIF number, and port number. For the specifiable range of values, see *Specifiable values for parameters*.

detail

Specifies that detailed statistics be displayed.

Operation when this parameter is omitted:

Detailed information is not displayed.

### Operation when a stack configuration is used

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

```
remote command <switch no.> show interfaces {gigabitethernet | tengigabitethernet}
<switch no.>/<nif no.>/<port no.> [detail]
```

### Example 1 [AX3650S]

The following shows an example of displaying the NIF information and detailed port information about the 1000BASE-X interface on an SFP dedicated port.

*Figure 16-7:* Execution results when 1000BASE-X is specified on an SFP dedicated port

```
> show interfaces gigabitethernet 1/0/1
Date 20XX/09/21 20:04:01 UTC
NIF0:
Port1: active up 1000BASE-SX full(auto) 0012.e222.1e31
      SFP connect
      Time-since-last-status-change:0:03:23
      Bandwidth:1000000kbps Average out:865Mbps Average in:865Mbps
      Peak out:873Mbps at 05:58:45 Peak in:873Mbps at 05:58:45
      Output rate: 864.9Mbps 844.6kpps
      Input rate: 864.9Mbps 844.6kpps
      Flow control send :off
      Flow control receive:off
      TPID:8100
      Frame size:1518 Octets retry:0 Interface name:ge1/0/1
      description:test lab area network
      <Out octets/packets counter> <In octets/packets counter>
      Octets : 8634720576 Octets : 8634715520
```

```

All packets      : 67458767 All packets      : 67458715
Unicast packets  : 67458736 Unicast packets  : 67458599 | 4
Multicast packets : 39      Multicast packets  : 0
Broadcast packets : 0      Broadcast packets  : 0
Pause packets    : 0      Pause packets    : 0
<Out line error counter>
Late collision    : 0      Defer indication    : 0
Single collision  : 0      Excessive deferral : 0 | 5
Multiple collisions : 0    Excessive collisions : 0
Error frames      : 0
<In line error counter>
CRC errors        : 0      Symbol errors      : 0
Fragments         : 0      Short frames       : 0 | 6
Jabber            : 0      Long frames        : 0
Error frames      : 0
<Line fault counter>
Link down         : 0      Signal detect errors : 0
TX fault          : 0      Transceiver notconnect : 0
Link down in operational state : 0 | 7
Signal detect errors in operational state : 0
Transceiver notconnect in operational state : 0
In limit over     : 0

```

&gt;

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

## Example 2 [AX3650S]

The following shows an example of displaying the NIF information, detailed port information, and detailed statistics about the 1000BASE-X interface on an SFP dedicated port.

*Figure 16-8:* Execution results for the specification of 1000BASE-X detailed statistics on an SFP dedicated port

```

> show interfaces gigabitethernet 1/0/1 detail
Date 20XX/09/21 20:04:01 UTC
NIF0:
Port1: active up 1000BASE-SX full(auto) 0012.e222.1e31
SFP connect
Time-since-last-status-change:0:03:35
Bandwidth:1000000kbps Average out:865Mbps Average in:865Mbps
Peak out:873Mbps at 05:58:45 Peak in:873Mbps at 05:58:45
Output rate: 864.9Mbps 844.6kpps
Input rate: 864.9Mbps 844.6kpps
Flow control send :off
Flow control receive:off
TPID:8100
Frame size:1518 Octets retry:0 Interface name:geth1/0/1
description:test lab area network
<Out octets/packets counter> <In octets/packets counter>
Octets : 9834716224 Octets : 9834711168
All packets : 76833733 All packets : 76833680
Unicast packets : 76833701 Unicast packets : 76833565
Multicast packets : 39 Multicast packets : 0
Broadcast packets : 0 Broadcast packets : 0
Pause packets : 0 Pause packets : 0
64 packets : 39 64 packets : 0

```

```

65-127 packets      :      0  65-127 packets      :      0
128-255 packets     : 76833690 128-255 packets     : 76833677
256-511 packets     :      2  256-511 packets     :      0
512-1023 packets    :      0  512-1023 packets    :      0
1024-1518 packets   :      0  1024-1518 packets   :      0
                    :          :
                    :          :

```

&gt;

1. NIF information
2. Summary port information
3. Detailed port information
4. Send and receive statistics

### Display items in Example 1 and 2 [AX3650S]

The following tables describe the items displayed as the NIF information, detailed port information, and statistics about the 1000BASE-X interface on an SFP dedicated port.

Table 16-12: NIF information about 1000BASE-X interface on an SFP dedicated port

Item	Displayed information	
	Detailed information	Meaning
NIF<nif no.>	NIF number	

Table 16-13: Summary information about 1000BASE-X interface on an SFP dedicated port

Item	Displayed information	
	Detailed information	Meaning
Port<port no.>	Port number	
<port status>	active up	Active (normal operating state)
	active down	Active (A line failure occurred.)
	initialize	Currently initializing or waiting for establishment of negotiation (auto-negotiation is operating)
	test	A line test is in progress.
	fault	Failed
	inactive	<ul style="list-style-type: none"> <li>Operation was stopped by the <code>inactivate</code> command.</li> <li>The port has been deactivated by the standby link functionality of link aggregation.</li> <li>The port has been deactivated by the BPDU guard functionality of the Spanning Tree Protocol.</li> <li>The port has been deactivated by the port resetting functionality of GSRP.</li> <li>The port has been deactivated by the unidirectional link failure detection functionality.</li> <li>The port has been deactivated by the L2 loop detection functionality.</li> <li>The port has been deactivated by storm control.</li> </ul>

Item	Displayed information	
	Detailed information	Meaning
	disable	Operation was stopped by using the <code>shutdown</code> or <code>schedule-power-control shutdown</code> configuration command.
<line type>	1000BASE-LX full	1000BASE-LX full duplex
	1000BASE-SX full	1000BASE-SX full duplex
	1000BASE-SX2 full	1000BASE-SX2 full duplex
	1000BASE-LH full	1000BASE-LH full duplex
	1000BASE-BX10-D full	1000BASE-BX-D (10km) full duplex
	1000BASE-BX10-U full	1000BASE-BX-U (10km) full duplex
	1000BASE-BX40-D full	1000BASE-BX-D (40km) full duplex
	1000BASE-BX40-U full	1000BASE-BX-U (40km) full duplex
	1000BASE-LHB full	1000BASE-LHB full duplex
	1000BASE-LX full(auto)	1000BASE-LX full duplex (Line type determined by auto-negotiation.)
	1000BASE-SX full(auto)	1000BASE-SX full duplex (Line type determined by auto-negotiation.)
	1000BASE-SX2 full(auto)	1000BASE-SX2 full duplex (Line type determined by auto-negotiation.)
	1000BASE-LH full(auto)	1000BASE-LH full duplex (Line type determined by auto-negotiation.)
	1000BASE-BX10-D full(auto)	1000BASE-BX-D (10km) full duplex (Line type determined by auto-negotiation.)
	1000BASE-BX10-U full(auto)	1000BASE-BX-U (10km) full duplex (Line type determined by auto-negotiation.)
	1000BASE-BX40-D full(auto)	1000BASE-BX-D (40km) full duplex (Line type determined by auto-negotiation.)
	1000BASE-BX40-U full(auto)	1000BASE-BX-U (40 km) full duplex (Line type determined by auto-negotiation.)
	1000BASE-LHB full(auto)	1000BASE-LHB full duplex (Line type determined by auto-negotiation.)
	-	The line type is unknown. A hyphen is displayed in the following cases: <ul style="list-style-type: none"> <li>• A port is in the <code>initialize</code> status.</li> <li>• A port is in the <code>fault</code> status.</li> <li>• The transceiver status is not <code>connect</code>.</li> </ul>
<MAC address>	MAC address of the port	
<type of transceiver>	SFP	SFP
<transceiver status>	connect	Installed
	notconnect	Not installed

Item	Displayed information	
	Detailed information	Meaning
	not support	An unsupported transceiver is installed.
	-	The transceiver status is unknown. A hyphen is displayed in the following cases: <ul style="list-style-type: none"> <li>• A port is in the <code>initialize</code> status.</li> <li>• A port is in the <code>fault</code> status.</li> </ul>

Table 16-14: Detailed information and statistics about 1000BASE-X interface on an SFP dedicated port

Item	Displayed information	
	Detailed information	Meaning
Time-since-last-status-change	<p>Displays the elapsed time since the last change in status.</p> <p><i>hh:mm:ss</i> (when the elapsed time is 24 hours or less: <i>hh</i> = hours, <i>mm</i> = minutes, <i>ss</i> = seconds)</p> <p><i>dd.hh:mm:ss</i> (when the elapsed time is more than 24 hours: <i>dd</i> = number of days, <i>hh</i> = hours, <i>mm</i> = minutes, <i>ss</i> = seconds)</p> <p>Over 100 days (when the elapsed time is more than 100 days)</p>	
Bandwidth:<bandwidth of line>kbps	<p>Displays the bandwidth of the line in kbps.</p> <p>If the <code>bandwidth</code> configuration command has not been executed, the line speed of the port is displayed. If the <code>bandwidth</code> configuration command has been executed, the setting value is displayed. Note that this setting does not control the bandwidth of the port.</p>	
Average out:<average bandwidth used on sending side>Mbps	<p>Displays the average bandwidth (in Mbps) used on the sending side of the line for the one minute interval before the command was executed.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Average in:<average bandwidth used on receiving side>Mbps	<p>Displays the average bandwidth (in Mbps) used on the receiving side of the line for the one minute interval before the command was executed.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Peak out	<p>Displays the maximum bandwidth used on the sending side of the line for the 24-hour interval before the command was executed, and the relevant time.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	

Item		Displayed information	
		Detailed information	Meaning
Peak in		<p>Displays the maximum bandwidth used on the receiving side of the line for the 24-hour interval before the command was executed, and the relevant time.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Output rate <sup>#1</sup>		<p>Displays the send throughput of the line (in bps and pps) for the one second interval before the command was executed, rounded to two decimal places.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Input rate <sup>#1</sup>		<p>Displays the receive throughput of the line (in bps and pps) for the one second interval before the command was executed, rounded to two decimal places.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Flow control send <sup>#2</sup>		on	A pause packet is sent.
		off	A pause packet is not sent.
Flow control receive <sup>#2</sup>		on	A pause packet is received.
		off	A pause packet is not received.
TPID		Displays a TagProtocolIdentifier value that is used on the port to identify the VLAN.	
Frame size <sup>#3</sup>		<p>Displays the maximum frame length of a port in octets.</p> <p>The maximum frame length is calculated starting from the MAC header and ending with the DATA and PAD fields. For details about frame formats, see the description of frame formats in <i>16.1.3 Control on the MAC and LLC sublayers</i> in the manual <i>Configuration Guide Vol. 1 For Version 11.10</i>.</p>	
retry:<Counts>		Displays the number of times the port was reactivated due to a fault.	
Interface name		Displays the name assigned to a port.	
description:<supplementary explanation>		<p>Displays the contents of the <code>description</code> configuration.</p> <p>The <code>description</code> configuration can be used to set comments, such as a comment about the purpose of the port. This item is not displayed if the description configuration has not been set.</p>	
Statistics	Category	<Out octets/packets counter>	Send statistics
		<In octets/packets counter>	Receive statistics
		<Out line error counter>	Send error statistics
		<In line error counter>	Receive error statistics
		<Line fault counter>	Failure statistics
	Detailed statistical items for sending and receiving	Octets	The number of octets Calculation of octet values is based on the range from the MAC header to the FCS field over the length of the frame.
		All packets	Number of packets (including error packets)

Item		Displayed information	
		Detailed information	Meaning
		Unicast packets	Number of unicast packets
		Multicast packets	Number of multicast packets
		Broadcast packets	Number of broadcast packets
		Pause packets	Number of pause packets
		64 packets	The number of packets whose frame length is 64 octets.
		65-127 packets	The number of packets whose frame length is from 65 to 127 octets.
		128-255 packets	The number of packets whose frame length is from 128 to 255 octets.
		256-511 packets	The number of packets whose frame length is from 256 to 511 octets.
		512-1023 packets	The number of packets whose frame length is from 512 to 1023 octets.
		1024-1518 packets	The number of packets whose frame length is from 1024 to 1518 octets. <sup>#4</sup>
	Detailed statistical items for send errors	Late collision	The number of collisions detected after the 512-bit time has elapsed
		Defer indication	The number of times the initial transmission was delayed because the transmit line was busy
		Single collision	The number of transmissions that were successful after one collision
		Excessive deferral	The number of times an excessive delay occurred
		Multiple collisions	The number of transmissions that were successful after two or more collisions
		Excessive collisions	The number of transfer failures due to excessive collisions (16 collisions)
		Error frames	The total number of frames discarded due to errors (total value of the following items: Late collision, Excessive deferral, Excessive collisions)
	Detailed statistical items for receive errors	CRC errors	The number of times the frame length was valid but an error was detected by the FCS check <sup>#5</sup>
		Symbol errors	The number of symbol errors that occurred
		Fragments	The number of times a short frame (whose length was shorter than 64 octets) was received and an FCS error or an alignment error occurred <sup>#5</sup>

Item		Displayed information	
		Detailed information	Meaning
		Jabber	The number of times a long frame (whose length exceeded the max frame length) was received and an FCS error or an alignment error occurred <sup>#5</sup>
		Short frames	The number of received packets that are shorter than the frame length <sup>#5</sup>
		Long frames	The number of received packets that exceed the frame length <sup>#5</sup>
		Error frames	The total number of frames discarded due to errors (total value of the following items: Short frames, Fragments, Jabber, CRC errors, Long frames, Symbol errors)
	Detailed statistical items for errors	Link down	The number of times a link was not established
		TX fault	The number of times a send line failure occurred
		Signal detect errors	The number of times a signal line could not be detected
		Transceiver notconnect	The number of times a transceiver was removed
		Link down in operational state	The number of link failures that occurred during communication (a link was not established)
		Signal detect errors in operational state	The number of failures that occurred during communication (signal line was not detected)
		Transceiver notconnect in operational state	The number of failures that occurred during communication (transceiver was removed)
		In limit over	The number of frames discarded due to exceeded receiving capacity

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

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

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

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

#4: The number of received long frames without VLAN Tag is included.

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

For details about frame formats, see *16.1.3 Control on the MAC and LLC sublayers* in the manual *Configuration Guide Vol. 1 For Version 11.10*.

### Example 3

The following shows an example of displaying the NIF information and detailed port information about the 1000BASE-X interface on SFP+/SFP ports.

*Figure 16-9: Execution result when 1000BASE-X is specified on SFP/SFP+ ports*

```
> show interfaces tengigabitethernet 1/0/52
Date 20XX/03/04 13:19:35 UTC
NIF0:
Port52: active up 1000BASE-SX full 0012.e222.1d55
SFP connect
Time-since-last-status-change:0:06:35
Bandwidth:1000000kbps Average out:0Mbps Average in:0Mbps
Peak out:65Mbps at 11:43:21 Peak in:51Mbps at 11:43:21
Output rate: 0bps 0pps
Input rate: 0bps 0pps
Flow control send :on
Flow control receive:off
TPID:8100
Frame size:1518 Octets retry:0 Interface name:tengeth1/0/52
description:test lab area network
<Out octets/packets counter>
Octets : 12750
All packets : 125
Unicast packets : 125
Multicast packets : 0
Broadcast packets : 0
Pause packets : 0
<In octets/packets counter>
Octets : 23502
All packets : 293
Unicast packets : 125
Multicast packets : 168
Broadcast packets : 0
Pause packets : 0
<In line error counter>
CRC errors : 0
Fragments : 0
Jabber : 0
Symbol errors : 0
Short frames : 0
Long frames : 0
Error frames : 0
<Line fault counter>
Link down : 0
TX fault : 0
Signal detect errors : 0
Transceiver notconnect : 0
Link down in operational state : 0
Signal detect errors in operational state : 0
Transceiver notconnect in operational state : 0
In limit over : 0
```

>

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

Example 4

The following shows an example of displaying the NIF information, detailed port information, and detailed statistics about the 1000BASE-X interface on SFP+/SFP ports.

Figure 16-10: Execution result of displaying detailed statistics when 1000BASE-X is specified on SFP/SFP+ ports

```
> show interfaces tengigabitethernet 1/0/52 detail
Date 20XX/03/04 13:19:36 UTC
NIF0:
Port52: active up 1000BASE-SX full 0012.e222.1d55
SFP connect
Time-since-last-status-change:0:06:36
Bandwidth:1000000kbps Average out:0Mbps Average in:0Mbps
Peak out:65Mbps at 11:43:21 Peak in:51Mbps at 11:43:21
Output rate: 0bps 0pps
Input rate: 500bps 1pps
Flow control send :off
Flow control receive:off
TPID:8100
Frame size:1518 Octets retry:0 Interface name:tengeth1/0/52
description:test lab area network
<Out octets/packets counter>
Octets : 12750
All packets : 125
Unicast packets : 125
Multicast packets : 0
Broadcast packets : 125
Pause packets : 0
64 packets : 0
65-127 packets : 0
128-255 packets : 0
256-511 packets : 0
512-1023 packets : 0
1024-1518 packets : 0
<In octets/packets counter>
Octets : 23566
All packets : 294
Unicast packets : 125
Multicast packets : 169
Broadcast packets : 0
Pause packets : 0
64 packets : 169
65-127 packets : 125
128-255 packets : 0
256-511 packets : 0
512-1023 packets : 0
1024-1518 packets : 0
:
:
>
```

- 1. NIF information
- 2. Summary port information
- 3. Detailed port information
- 4. Send statistics
- 5. Receive statistics

Display items in Example 3 and 4

The following tables describe the items displayed as the NIF information, detailed port information, and statistics about the 1000BASE-X interface on SFP+/SFP ports.

Table 16-15: NIF information about 1000BASE-X interface on SFP+/SFP ports

Item	Displayed information	
	Detailed information	Meaning
NIF<nif no.>	NIF number	

Table 16-16: Summary information about 1000BASE-X interface on SFP+/SFP ports

Item	Displayed information	
	Detailed information	Meaning
Port<port no.>	Port number	
<port status>	active up	Active (normal operating state)
	active down	Active (A line failure occurred.)
	initialize	Currently initializing or waiting for establishment of negotiation (auto-negotiation is operating)
	test	A line test is in progress.
	fault	Failed
	inactive	<ul style="list-style-type: none"> <li>Operation was stopped by the <code>inactivate</code> command.</li> <li>The port has been deactivated by the standby link functionality of link aggregation.</li> <li>The port has been deactivated by the BPDU guard functionality of the Spanning Tree Protocol.</li> <li>The port has been deactivated by the port resetting functionality of GSRP.</li> <li>The port has been deactivated by the unidirectional link failure detection functionality.</li> <li>The port has been deactivated by the L2 loop detection functionality.</li> <li>The port has been deactivated by storm control.</li> </ul>
	disable	Operation was stopped by using the <code>shutdown</code> or <code>schedule-power-control shutdown</code> configuration command.
<line type>	1000BASE-LX full	1000BASE-LX full duplex
	1000BASE-SX full	1000BASE-SX full duplex
	1000BASE-LH full	1000BASE-LH full duplex
	1000BASE-BX10-D full	1000BASE-BX-D (10 km) full duplex
	1000BASE-BX10-U full	1000BASE-BX-U (10 km) full duplex
	1000BASE-BX40-D full	1000BASE-BX-D (40 km) full duplex
	1000BASE-BX40-U full	1000BASE-BX-U (40 km) full duplex
	1000BASE-LHB full	1000BASE-LHB full duplex
	1000BASE-LX full(auto)	1000BASE-LX full duplex (Line type determined by auto-negotiation.)
	1000BASE-SX full(auto)	1000BASE-SX full duplex (Line type determined by auto-negotiation.)

Item	Displayed information	
	Detailed information	Meaning
	1000BASE-LH full(auto)	1000BASE-LH full duplex (Line type determined by auto-negotiation.)
	1000BASE-BX10-D full(auto)	1000BASE-BX-D (10 km) full duplex (Line type determined by auto-negotiation.)
	1000BASE-BX10-U full(auto)	1000BASE-BX-U (10 km) full duplex (Line type determined by auto-negotiation.)
	1000BASE-BX40-D full(auto)	1000BASE-BX-D (40 km) full duplex (Line type determined by auto-negotiation.)
	1000BASE-BX40-U full(auto)	1000BASE-BX-U (40 km) full duplex (Line type determined by auto-negotiation.)
	1000BASE-LHB full(auto)	1000BASE-LHB full duplex (Line type determined by auto-negotiation.)
	-	The line type is unknown. A hyphen is displayed in the following cases: <ul style="list-style-type: none"> <li>• A port is in the <code>initialize</code> status.</li> <li>• A port is in the <code>fault</code> status.</li> <li>• The transceiver status is not <code>connect</code>.</li> </ul>
<MAC address>	MAC address of the port	
<type of transceiver>	SFP	SFP
	-	The transceiver type is unknown.
<transceiver status>	connect	Installed
	notconnect	Not installed
	not support	An unsupported transceiver is installed.
	-	The transceiver status is unknown. A hyphen is displayed in the following cases: <ul style="list-style-type: none"> <li>• A port is in the <code>initialize</code> status.</li> <li>• A port is in the <code>fault</code> status.</li> </ul>

Table 16-17: Detailed information and statistics about 1000BASE-X interface on SFP+/SFP ports

Item	Displayed information	
	Detailed information	Meaning
Time-since-last-status-change	Displays the elapsed time since the last change in status. <code>hh:mm:ss</code> (when the elapsed time is 24 hours or less: <code>hh</code> = hours, <code>mm</code> = minutes, <code>ss</code> = seconds) <code>dd.hh:mm:ss</code> (when the elapsed time is more than 24 hours: <code>dd</code> = number of days, <code>hh</code> = hours, <code>mm</code> = minutes, <code>ss</code> = seconds) Over 100 days (when the elapsed time is more than 100 days)	
Bandwidth:<bandwidth of line>kbps	Displays the bandwidth of the line in kbps. If the <code>bandwidth</code> configuration command has not been executed, the line speed of the port is displayed. If the <code>bandwidth</code> configuration command has been executed, the setting value is displayed. Note that this setting does not control the bandwidth of the port.	

Item	Displayed information	
	Detailed information	Meaning
Average out:<average bandwidth used on sending side>Mbps	<p>Displays the average bandwidth (in Mbps) used on the sending side of the line for the one minute interval before the command was executed.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Average in:<average bandwidth used on receiving side>Mbps	<p>Displays the average bandwidth (in Mbps) used on the receiving side of the line for the one minute interval before the command was executed.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Peak out	<p>Displays the maximum bandwidth used on the sending side of the line for the 24-hour interval before the command was executed, and the relevant time.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Peak in	<p>Displays the maximum bandwidth used on the receiving side of the line for the 24-hour interval before the command was executed, and the relevant time.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Output rate <sup>#1</sup>	<p>Displays the send throughput of the line (in bps and pps) for the one second interval before the command was executed, rounded to two decimal places.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Input rate <sup>#1</sup>	<p>Displays the receive throughput of the line (in bps and pps) for the one second interval before the command was executed, rounded to two decimal places.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Flow control send <sup>#2</sup>	on [AX3650S]	A pause packet is sent.
	off	A pause packet is not sent.
Flow control receive <sup>#2</sup>	on [AX3650S]	A pause packet is received.
	off	A pause packet is not received.
TPID	<p>Displays a TagProtocolIdentifier value that is used on the port to identify the VLAN.</p>	

Item		Displayed information	
		Detailed information	Meaning
Frame size <sup>#3</sup>		<p>Displays the maximum frame length of a port in octets.</p> <p>The maximum frame length is calculated starting from the MAC header and ending with the DATA and PAD fields. For details about frame formats, see the description of frame formats in <i>16.1.3 Control on the MAC and LLC sublayers</i> in the manual <i>Configuration Guide Vol. 1 For Version 11.10</i>.</p> <p>- is displayed for a stack port.</p>	
retry:<Counts>		Displays the number of times the port was reactivated due to a fault.	
Interface name		Displays the name assigned to a port.	
description: <supplementary explanation>		<p>Displays the contents of the description configuration.</p> <p>The description configuration can be used to set comments, such as a comment about the purpose of the port. This item is not displayed if the description configuration has not been set.</p>	
Statistics	Category	<Out octets/packets counter>	Send statistics
		<In octets/packets counter>	Receive statistics
		<In line error counter>	Receive error statistics
		<Line fault counter>	Failure statistics
	Detailed statistical items for sending and receiving	Octets	<p>The number of octets</p> <p>Calculation of octet values is based on the range from the MAC header to the FCS field over the length of the frame.</p>
		All packets	Number of packets (including error packets)
		Unicast packets	Number of unicast packets
		Multicast packets	Number of multicast packets
		Broadcast packets	Number of broadcast packets
		Pause packets	Number of pause packets
		64 packets	The number of packets whose frame length is 64 octets.
		65-127 packets	The number of packets whose frame length is from 65 to 127 octets.
		128-255 packets	The number of packets whose frame length is from 128 to 255 octets.
		256-511 packets	The number of packets whose frame length is from 256 to 511 octets.
		512-1023 packets	The number of packets whose frame length is from 512 to 1023 octets.
		1024-1518 packets	The number of packets whose frame length is from 1024 to 1518 octets. <sup>#4</sup>
	Detailed statistical items for receive errors	CRC errors	The number of times the frame length was valid but an error was detected by the FCS check <sup>#5</sup>

Item		Displayed information	
		Detailed information	Meaning
		Fragments	The number of times a short frame (whose length is shorter than 64 octets) is received and an FCS error or an alignment error occurred <sup>#5</sup>
		Jabber	The number of times a long frame (whose length exceeds the max frame length) was received and an FCS error or an alignment error occurred <sup>#5</sup>
		Symbol errors	The number of symbol errors that occurred
		Short frames	The number of received packets that are shorter than the frame length <sup>#5</sup>
		Long frames	The number of received packets that exceed the frame length <sup>#5</sup>
		Error frames	The total number of frames discarded due to errors (total value of the following items: Short frames, Fragments, Jabber, CRC errors, Long frames, Symbol errors)
	Detailed statistical items for errors	Link down	The number of times a link was not established
		TX fault	The number of times a send line failure occurred
		Signal detect errors	The number of times a signal line could not be detected
		Transceiver notconnect	The number of times a transceiver was removed
		Link down in operational state	The number of link failures that occurred during communication (a link was not established)
		Signal detect errors in operational state	The number of failures that occurred during communication (signal line was not detected)
		Transceiver notconnect in operational state	The number of failures that occurred during communication (transceiver was removed)
		In limit over	The number of frames discarded due to exceeded receiving capacity

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

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

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

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

#4: The number of received long frames without VLAN Tag is included.

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

For details about frame formats, see *16.1.3 Control on the MAC and LLC sublayers* in the manual *Configuration Guide Vol. 1 For Version 11.10*.

## Impact on communication

None

## Response messages

*Table 16-18:* List of response messages for the show interfaces (1000BASE-X) (Ethernet) command

Message	Description
<switch no.>/<nif no.>/<port no.> is not gigabitethernet.	The interface of the specified port is not gigabitethernet. Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<switch no.>/<nif no.>/<port no.> is not tengigabitethernet.	The interface of the specified port is not tengigabitethernet. Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The port number is outside the valid range. Make sure the specified parameter is correct. <port no.>: Indicates the port number.

## Notes

All display items are cleared in the following cases:

- When the Switch starts up
- The `restart vlan` command is executed.
- When a device hardware failure occurs
- An error occurs in the network interface management program (nimd).

---

## show interfaces (10GBASE-R)

---

Displays Ethernet information.

### Syntax

```
show interfaces tengigabitethernet <switch no.>/<nif no.>/<port no.> [detail]
```

### Input mode

User mode and administrator mode

### Parameters

tengigabitethernet

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

<switch no.>/<nif no.>/<port no.>

Specifies the switch number, NIF number, and port number. For the specifiable range of values, see *Specifiable values for parameters*.

detail

Specifies that detailed statistics be displayed.

Operation when this parameter is omitted:

Detailed information is not displayed.

### Operation when a stack configuration is used

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

```
remote command <switch no.> show interfaces tengigabitethernet <switch no.>/<nif no.>/<port no.> [detail]
```

### Example 1

The following shows an example of displaying the NIF information and detailed port information about the 10GBASE-R interface.

*Figure 16-11: Execution results when the 10GBASE-R is specified*

```
> show interfaces tengigabitethernet 1/0/52
Date 20XX/03/04 12:41:55 UTC
NIF0:
Port52: active up 10GBASE-LR 0012.e222.1d55
SFP+ connect
Time-since-last-status-change:0:05:33
Bandwidth:10000000kbps Average out:0Mbps Average in:0Mbps
Peak out:65Mbps at 11:43:21 Peak in:51Mbps at 11:43:21
Output rate: 0bps 0pps
Input rate: 0bps 0pps
Flow control send :off
Flow control receive:on
TPID:8100
Frame size:1518 Octets retry:0 Interface name:tengeth1/0/52
<Out octets/packets counter>
Octets : 18653
All packets : 190
Unicast packets : 189
Multicast packets : 0
Broadcast packets : 1
Pause packets : 0
<In octets/packets counter>
Octets : 19172
```

```

All packets : 189 |
Unicast packets : 189 |
Multicast packets : 0 | 5
Broadcast packets : 0 |
Pause packets : 0 |
<In line error counter> : - |
CRC errors : 0 |
Fragments : 0 |
Jabber : 0 |
Symbol errors : 0 | 6
Short frames : 0 |
Long frames : 0 |
Error frames : 0 |
<Line fault counter> : - |
Link down : 0 |
TX fault : 0 |
Signal detect errors : 0 |
Transceiver notconnect : 0 | 7
Link down in operational state : 0 |
Signal detect errors in operational state : 0 |
Transceiver notconnect in operational state : 0 |
In limit over : 0 |
>

```

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

## Example 2

The following shows an example of displaying the NIF information, detailed port information, and detailed statistics about the 10BASE-R interface.

*Figure 16-12: Execution results for the specification of 10GBASE-R detailed statistics*

```

> show interfaces tengigabitethernet 1/0/52 detail
Date 20XX/03/04 12:42:22 UTC
NIF0: <-1
Port52: active up 10GBASE-LR 0012.e222.1d55 -| 2
SFP+ connect -|
Time-since-last-status-change:0:06:00 -|
Bandwidth:10000000kbps Average out:0Mbps Average in:0Mbps
Peak out:65Mbps at 11:43:21 Peak in:51Mbps at 11:43:21
Output rate: 0bps 0pps
Input rate: 0bps 0pps | 3
Flow control send :off
Flow control receive:on
TPID:8100
Frame size:1518 Octets retry:0 Interface name:tengeth1/0/52
<Out octets/packets counter> -|
Octets : 18653 |
All packets : 190 |
Unicast packets : 189 |
Multicast packets : 0 |
Broadcast packets : 1 |
Pause packets : 0 | 4
64 packets : 0 |
65-127 packets : 0 |
128-255 packets : 0 |
256-511 packets : 0 |

```

```

512-1023 packets      :      0
1024-1518 packets    :      0
<In octets/packets counter>
Octets                :    19172
All packets           :      189
Unicast packets       :      189
Multicast packets     :       0
Broadcast packets     :       0
Pause packets         :       0
64 packets            :       0
65-127 packets       :       0
128-255 packets       :       0
256-511 packets       :       0
512-1023 packets     :       0
1024-1518 packets     :       0
                    :
                    :
>

```

1. NIF information
2. Summary port information
3. Detailed port information
4. Send statistics
5. Receive statistics

## Display items in Example 1 and 2

The following tables describe the items displayed as the NIF information, detailed port information, and statistics about the 10GBASE-R interface.

*Table 16-19: NIF information about 10GBASE-R interfaces*

Item	Displayed information	
	Detailed information	Meaning
NIF< <i>nif no.</i> >	NIF number	

*Table 16-20: Summary information about 10GBASE-R interfaces*

Item	Displayed information	
	Detailed information	Meaning
Port< <i>port no.</i> >	Port number	
< <i>port status</i> >	active up	Active (normal operating state)
	active down	Active (A line failure occurred.)
	initialize	Currently initializing
	test	A line test is in progress.
	fault	Failed

Item	Displayed information	
	Detailed information	Meaning
	inactive	<ul style="list-style-type: none"> <li>Operation was stopped by the <code>inactivate</code> command.</li> <li>The port has been deactivated by the standby link functionality of link aggregation.</li> <li>The port has been deactivated by the BPDU guard functionality of the Spanning Tree Protocol.</li> <li>The port has been deactivated by the port resetting functionality of GSRP.</li> <li>The port has been deactivated by the unidirectional link failure detection functionality.</li> <li>The port has been deactivated by the L2 loop detection functionality.</li> <li>The port has been deactivated by storm control.</li> </ul>
	disable	Operation was stopped by using the <code>shutdown</code> or <code>schedule-power-control shutdown</code> configuration command.
<line type>	10GBASE-SR	10GBASE-SR
	10GBASE-LR	10GBASE-LR
	10GBASE-ER	10GBASE-ER
	10GBASE-CU30CM	10GBASE-CU (30cm)
	10GBASE-CU1M	10GBASE-CU (1m)
	10GBASE-CU3M	10GBASE-CU (3m)
	10GBASE-CU5M	10GBASE-CU (5m)
	-	<p>The line type is unknown. A hyphen is displayed in the following cases:</p> <ul style="list-style-type: none"> <li>A port is in the <code>initialize</code> status.</li> <li>A port is in the <code>fault</code> status.</li> <li>The transceiver status is not <code>connect</code>.</li> </ul>
<MAC address>	MAC address of the port	
<type of transceiver>	SFP+	SFP+
	-	The transceiver type is unknown.
<transceiver status>	connect	Installed
	notconnect	Not installed
	not support	An unsupported transceiver is installed.
	-	<p>The transceiver status is unknown. A hyphen is displayed in the following cases:</p> <ul style="list-style-type: none"> <li>A port is in the <code>initialize</code> status.</li> <li>A port is in the <code>fault</code> status.</li> </ul>

Table 16-21: Detailed information and statistics about 10GBASE-R interfaces

Item	Displayed information	
	Detailed information	Meaning
Time-since-last-status-change	<p>Displays the elapsed time since the last change in status.</p> <p><i>hh:mm:ss</i> (when the elapsed time is 24 hours or less: <i>hh</i> = hours, <i>mm</i> = minutes, <i>ss</i> = seconds)</p> <p><i>dd.hh:mm:ss</i> (when the elapsed time is more than 24 hours: <i>dd</i> = number of days, <i>hh</i> = hours, <i>mm</i> = minutes, <i>ss</i> = seconds)</p> <p>Over 100 days (when the elapsed time is more than 100 days)</p>	
Bandwidth:< <i>bandwidth of line</i> >kbps	<p>Displays the bandwidth of the line in kbps.</p> <p>If the <code>bandwidth</code> configuration command has not been executed, the line speed of the port is displayed. If the <code>bandwidth</code> configuration command has been executed, the setting value is displayed. Note that this setting does not control the bandwidth of the port.</p>	
Average out:< <i>average bandwidth used on sending side</i> >Mbps	<p>Displays the average bandwidth (in Mbps) used on the sending side of the line for the one minute interval before the command was executed.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Average in:< <i>average bandwidth used on receiving side</i> >Mbps	<p>Displays the average bandwidth (in Mbps) used on the receiving side of the line for the one minute interval before the command was executed.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Peak out	<p>Displays the maximum bandwidth used on the sending side of the line for the 24-hour interval before the command was executed, and the relevant time.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Peak in	<p>Displays the maximum bandwidth used on the receiving side of the line for the 24-hour interval before the command was executed, and the relevant time.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Output rate <sup>#1</sup>	<p>Displays the send throughput of the line (in bps and pps) for the one second interval before the command was executed, rounded to two decimal places.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Input rate <sup>#1</sup>	<p>Displays the receive throughput of the line (in bps and pps) for the one second interval before the command was executed, rounded to two decimal places.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Flow control send <sup>#2</sup>	on [AX3650S]	A pause packet is sent.

Item		Displayed information	
		Detailed information	Meaning
		off	A pause packet is not sent.
Flow control receive <sup>#2</sup>		on [AX3650S]	A pause packet is received.
		off	A pause packet is not received.
TPID		Displays a TagProtocolIdentifier value that is used on the port to identify the VLAN.	
Frame size <sup>#3</sup>		<p>Displays the maximum frame length of a port in octets.</p> <p>The maximum frame length is calculated starting from the MAC header and ending with the DATA and PAD fields. For details about frame formats, see the description of frame formats in <i>16.1.3 Control on the MAC and LLC sublayers</i> in the manual <i>Configuration Guide Vol. 1 For Version 11.10</i>.</p> <p>- is displayed for a stack port.</p>	
retry:<Counts>		Displays the number of times the port was reactivated due to a fault.	
Interface name		Displays the name assigned to a port.	
description:<supplementary explanation>		<p>Displays the contents of the description configuration.</p> <p>The description configuration can be used to set comments, such as a comment about the purpose of the port. This item is not displayed if the description configuration has not been set.</p>	
Statistics	Category	<Out octets/packets counter>	Send statistics
		<In octets/packets counter>	Receive statistics
		<In line error counter>	Receive error statistics
		<Line fault counter>	Failure statistics
	Detailed statistical items for sending and receiving	Octets	<p>The number of octets</p> <p>Calculation of octet values is based on the range from the MAC header to the FCS field over the length of the frame.</p>
		All packets	Number of packets (including error packets)
		Unicast packets	Number of unicast packets
		Multicast packets	Number of multicast packets
		Broadcast packets	Number of broadcast packets
		Pause packets	Number of pause packets
		64 packets	The number of packets whose frame length is 64 octets.
		65-127 packets	The number of packets whose frame length is from 65 to 127 octets.
		128-255 packets	The number of packets whose frame length is from 128 to 255 octets.
		256-511 packets	The number of packets whose frame length is from 256 to 511 octets.
		512-1023 packets	The number of packets whose frame length is from 512 to 1023 octets.

Item		Displayed information	
		Detailed information	Meaning
	Detailed statistical items for receive errors	1024-1518 packets	The number of packets whose frame length is from 1024 to 1518 octets.
		CRC errors	The number of times the frame length was valid but an error was detected by the FCS check <sup>#4</sup>
		Fragments	The number of times a short frame (whose length was shorter than 64 octets) was received and an FCS error or an alignment error occurred <sup>#4</sup>
		Jabber	The number of times a long frame (whose length exceeded the max frame length) was received and an FCS error or an alignment error occurred <sup>#4</sup>
		Symbol errors	The number of symbol errors that occurred
		Short frames	The number of received packets that are shorter than the frame length <sup>#4</sup>
		Long frames	The number of received packets that exceed the frame length <sup>#4#5</sup>
		Error frames	The total number of frames discarded due to errors (total value of the following items: Short frames, Fragments, Jabber, CRC errors, Long frames, Symbol errors)
	Detailed statistical items for errors	Link down	The number of times a link was not established
		TX fault	The number of times a send line failure occurred
		Signal detect errors	The number of times a signal line could not be detected
		Transceiver notconnect	The number of times a transceiver was removed
		Link down in operational state	The number of link failures that occurred during communication (a link was not established)
		Signal detect errors in operational state	The number of failures that occurred during communication (signal line was not detected)
		Transceiver notconnect in operational state	The number of failures that occurred during communication (transceiver was removed)
		In limit over	The number of frames discarded due to exceeded receiving capacity

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

If the displayed value is 10000 or larger, the display unit varies depending on the displayed value, as follows:

- If the displayed value is 10000 or larger, the unit is K.
- If the displayed value is 10000 K or larger, the unit is M.
- If the displayed value is 10000 M or larger, the unit is G.

In the above cases, one digit is displayed below the decimal point.

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

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

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

For details about frame formats, see *16.1.3 Control on the MAC and LLC sublayers* in the manual *Configuration Guide Vol. 1 For Version 11.10*.

#5: The number of times of Long frames includes the number of times of Jabber. [AX3800S]

## Impact on communication

None

## Response messages

*Table 16-22:* List of response messages for the show interfaces (10GBASE-R) (Ethernet) command

Message	Description
<switch no.>/<nif no.>/<port no.> is not tengigabitethernet.	The interface of the specified port is not tengigabitethernet. Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The port number is outside the valid range. Make sure the specified parameter is correct. <port no.>: Indicates the port number.

## Notes

All display items are cleared in the following cases:

- When the Switch starts up
- The `restart vlan` command is executed.
- When a device hardware failure occurs
- An error occurs in the network interface management program (nimd).

---

## show interfaces (40GBASE-R) [AX3800S]

---

Displays Ethernet information.

### Syntax

```
show interfaces fortygigabitethernet <switch no.>/<nif no.>/<port no.> [detail]
```

### Input mode

User mode and administrator mode

### Parameters

fortygigabitethernet

Specifies an Ethernet interface with a maximum line speed of 40 Gbit/s.

<switch no.>/<nif no.>/<port no.>

Specifies the switch number, NIF number, and port number. For the specifiable range of values, see *Specifiable values for parameters*.

detail

Specifies that detailed statistics be displayed.

Operation when this parameter is omitted:

Detailed information is not displayed.

### Operation when a stack configuration is used

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

```
remote command <switch no.> show interfaces fortygigabitethernet <switch no.>/<nif no.>/<port no.> [detail]
```

### Example 1

The following shows an example of displaying the NIF information and detailed port information about the 40GBASE-R interface.

*Figure 16-13: Execution results when the 40GBASE-R interface is specified*

```
> show interfaces fortygigabitethernet 1/0/52
Date 20XX/03/04 12:41:55 UTC
NIF0:
Port52: active up 40GBASE-SR4 full 0012.e222.1d55
      QSFP+ connect
      Time-since-last-status-change:0:05:33
      Bandwidth:40000000kbps Average out:0Mbps Average in:0Mbps
      Peak out:65Mbps at 11:43:21 Peak in:51Mbps at 11:43:21
      Output rate: 0bps 0pps
      Input rate: 0bps 0pps
      Flow control send :off
      Flow control receive:off
      TPID:8100
      Frame size:1518 Octets retry:0 Interface name:ftygeth1/0/52
      <Out octets/packets counter>
      Octets : 18653
      All packets : 190
      Unicast packets : 189
      Multicast packets : 0
      Broadcast packets : 1
      Pause packets : 0
      <In octets/packets counter>
      Octets : 19172
```

```

All packets : 189
Unicast packets : 189
Multicast packets : 0 5
Broadcast packets : 0
Pause packets : 0
<In line error counter>
CRC errors : 0
Fragments : 0
Jabber : 0
Symbol errors : 0 6
Short frames : 0
Long frames : 0
Error frames : 0
<Line fault counter>
Link down : 0
TX fault : 0
Signal detect errors : 0
Transceiver notconnect : 0 7
Link down in operational state : 0
Signal detect errors in operational state : 0
Transceiver notconnect in operational state : 0
In limit over : 0
>

```

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

## Example 2

The following shows an example of displaying the NIF information, detailed port information, and detailed statistics about the 40GBASE-R interface.

*Figure 16-14: Execution results for the specification of 40BASE-R detailed statistics*

```

> show interfaces fortygigabitethernet 1/0/52 detail
Date 20XX/03/04 12:42:22 UTC
NIF0:
Port52: active up 40GBASE-SR4 full 0012.e222.1d55
QSFP+ connect
Time-since-last-status-change:0:06:00
Bandwidth:40000000kbps Average out:0Mbps Average in:0Mbps
Peak out:65Mbps at 11:43:21 Peak in:51Mbps at 11:43:21
Output rate: 0bps 0pps
Input rate: 0bps 0pps
Flow control send :off
Flow control receive:off
TPID:8100
Frame size:1518 Octets retry:0 Interface name:ftygeth1/0/52
<Out octets/packets counter>
Octets : 18653
All packets : 190
Unicast packets : 189
Multicast packets : 0
Broadcast packets : 1
Pause packets : 0 4
64 packets : 0
65-127 packets : 0
128-255 packets : 0
256-511 packets : 0

```

```

512-1023 packets      :      0
1024-1518 packets     :      0
<In octets/packets counter>
Octets                :    19172
All packets           :     189
Unicast packets       :     189
Multicast packets     :      0
Broadcast packets     :      0
Pause packets         :      0
64 packets            :      0
65-127 packets        :      0
128-255 packets       :      0
256-511 packets       :      0
512-1023 packets      :      0
1024-1518 packets     :      0
                    :
                    :
>

```

1. NIF information
2. Summary port information
3. Detailed port information
4. Send statistics
5. Receive statistics

### Display items in Example 1 and 2

The following tables describe the items displayed as the NIF information, detailed port information, and statistics about 40GBASE-R interfaces.

*Table 16-23: Summary information about 40GBASE-R interfaces*

Item	Displayed information	
	Detailed information	Meaning
NIF<nif no.>	NIF number	

*Table 16-24: Summary information about 40GBASE-R interfaces*

Item	Displayed information	
	Detailed information	Meaning
Port<port no.>	Port number	
<port status>	active up	Active (normal operating state)
	active down	Active (A line failure occurred.)
	initialize	Currently initializing or waiting for establishment of negotiation (auto-negotiation is operating)
	test	A line test is in progress.
	fault	Failed

Item	Displayed information	
	Detailed information	Meaning
	inactive	<ul style="list-style-type: none"> <li>Operation was stopped by the <code>inactivate</code> command.</li> <li>The port has been deactivated by the standby link functionality of link aggregation.</li> <li>The port has been deactivated by the BPDU guard functionality of the Spanning Tree Protocol.</li> <li>The port has been deactivated by the port resetting functionality of GSRP.</li> <li>The port has been deactivated by the unidirectional link failure detection functionality.</li> <li>The port has been deactivated by the L2 loop detection functionality.</li> <li>The port has been deactivated by storm control.</li> </ul>
	disable	Operation was stopped by using the <code>shutdown</code> or <code>schedule-power-control shutdown</code> configuration command.
<line type>	40GBASE-SR4 full	40GBASE-SR4
	40GBASE-CU35CM full(auto)	40GBASE-CR4 (35cm) (Line type determined by auto-negotiation.)
	40GBASE-CU1M full(auto)	40GBASE-CR4 (1m) (Line type determined by auto-negotiation.)
	40GBASE-CU3M full(auto)	40GBASE-CR4 (3m) (Line type determined by auto-negotiation.)
	40GBASE-CU5M full(auto)	40GBASE-CR4 (5m) (Line type determined by auto-negotiation.)
	-	The line type is unknown. A hyphen is displayed in the following cases: <ul style="list-style-type: none"> <li>A port is in the <code>initialize</code> status.</li> <li>A port is in the <code>fault</code> status.</li> <li>The transceiver status is not <code>connect</code>.</li> </ul>
<MAC address>	MAC address of the port	
<type of transceiver>	QSFP+	QSFP+
<transceiver status>	connect	Installed
	notconnect	Not installed
	not support	An unsupported transceiver is installed.
	-	The transceiver status is unknown. A hyphen is displayed in the following cases: <ul style="list-style-type: none"> <li>A port is in the <code>initialize</code> status.</li> <li>A port is in the <code>fault</code> status.</li> </ul>

Table 16-25: Detailed information and statistics about 40GBASE-R interfaces

Item	Displayed information	
	Detailed information	Meaning
Time-since-last-status-change	<p>Displays the elapsed time since the last change in status.</p> <p><i>hh:mm:ss</i> (when the elapsed time is 24 hours or less: <i>hh</i> = hours, <i>mm</i> = minutes, <i>ss</i> = seconds)</p> <p><i>dd.hh:mm:ss</i> (when the elapsed time is more than 24 hours: <i>dd</i> = number of days, <i>hh</i> = hours, <i>mm</i> = minutes, <i>ss</i> = seconds)</p> <p>Over 100 days (when the elapsed time is more than 100 days)</p>	
Bandwidth:<bandwidth of line>kbps	<p>Displays the bandwidth of the line in kbps.</p> <p>If the <code>bandwidth</code> configuration command has not been executed, the line speed of the port is displayed. If the <code>bandwidth</code> configuration command has been executed, the setting value is displayed. Note that this setting does not control the bandwidth of the port.</p>	
Average out:<average bandwidth used on sending side>Mbps	<p>Displays the average bandwidth (in Mbps) used on the sending side of the line for the one minute interval before the command was executed.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Average in:<average bandwidth used on receiving side>Mbps	<p>Displays the average bandwidth (in Mbps) used on the receiving side of the line for the one minute interval before the command was executed.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Peak out	<p>Displays the maximum bandwidth used on the sending side of the line for the 24-hour interval before the command was executed, and the relevant time.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Peak in	<p>Displays the maximum bandwidth used on the receiving side of the line for the 24-hour interval before the command was executed, and the relevant time.</p> <p>0 Mbps is displayed if there is no communication (when not even 1 bit of data is transferred). 1 Mbps is displayed if the range of the transferred data is from 1 bit to 1.5 Mbit. If the transferred data is 1.5 Mbit or more, the displayed value is rounded to one decimal place.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Output rate <sup>#1</sup>	<p>Displays the send throughput of the line (in bps and pps) for the one second interval before the command was executed, rounded to two decimal places.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Input rate <sup>#1</sup>	<p>Displays the receive throughput of the line (in bps and pps) for the one second interval before the command was executed, rounded to two decimal places.</p> <p>The frame length used to calculate bps value starts from the MAC header and ends with the FCS field.</p>	
Flow control send <sup>#2</sup>	off	A pause packet is not sent.

Item		Displayed information	
		Detailed information	Meaning
Flow control receive <sup>#2</sup>		off	A pause packet is not sent.
TPID		Displays a <code>TagProtocolIdentifier</code> value that is used on the port to identify the VLAN.	
Frame size <sup>#3</sup>		<p>Displays the maximum frame length of a port in octets.</p> <p>The maximum frame length is calculated starting from the MAC header and ending with the DATA and PAD fields. For details about frame formats, see the description of frame formats in <i>16.1.3 Control on the MAC and LLC sublayers</i> in the manual <i>Configuration Guide Vol. 1 For Version 11.10</i>.</p> <p>- is displayed for a stack port.</p>	
retry:<Counts>		Displays the number of times the port was reactivated due to a fault.	
Interface name		Displays the name assigned to a port.	
description:<supplementary explanation>		<p>Displays the contents of the <code>description</code> configuration.</p> <p>The <code>description</code> configuration can be used to set comments, such as a comment about the purpose of the port. This item is not displayed if the description configuration has not been set.</p>	
Statistics	Category	<Out octets/packets counter>	Send statistics
		<In octets/packets counter>	Receive statistics
		<In line error counter>	Receive error statistics
		<Line fault counter>	Failure statistics
	Detailed statistical items for sending and receiving	Octets	<p>The number of octets</p> <p>Calculation of octet values is based on the range from the MAC header to the FCS field over the length of the frame.</p>
		All packets	Number of packets (including error packets)
		Unicast packets	Number of unicast packets
		Multicast packets	Number of multicast packets
		Broadcast packets	Number of broadcast packets
		Pause packets	Number of pause packets
		64 packets	The number of packets whose frame length is 64 octets.
		65-127 packets	The number of packets whose frame length is from 65 to 127 octets.
		128-255 packets	The number of packets whose frame length is from 128 to 255 octets.
		256-511 packets	The number of packets whose frame length is from 256 to 511 octets.
		512-1023 packets	The number of packets whose frame length is from 512 to 1023 octets.
		1024-1518 packets	The number of packets whose frame length is from 1024 to 1518 octets.

Item		Displayed information	
		Detailed information	Meaning
	Detailed statistical items for receive errors	CRC errors	The number of times the frame length was valid but an error was detected by the FCS check <sup>#4</sup>
		Fragments	The number of times a short frame (whose length was shorter than 64 octets) was received and an FCS error or an alignment error occurred <sup>#4</sup>
		Jabber	The number of times a long frame (whose length exceeded the max frame length) was received and an FCS error or an alignment error occurred <sup>#4</sup>
		Symbol errors	The number of symbol errors that occurred
		Short frames	The number of received packets that are shorter than the frame length <sup>#4</sup>
		Long frames	The number of received packets that exceed the frame length <sup>#4#5</sup>
		Error frames	The total number of frames discarded due to errors (total value of the following items: Short frames, Fragments, Jabber, CRC errors, Long frames, Symbol errors)
	Detailed statistical items for errors	Link down	The number of times a link was not established
		TX fault	The number of times a send line failure occurred
		Signal detect errors	The number of times a signal line could not be detected
		Transceiver notconnect	The number of times a transceiver was removed
		Link down in operational state	The number of link failures that occurred during communication (a link was not established)
		Signal detect errors in operational state	The number of failures that occurred during communication (signal line was not detected)
		Transceiver notconnect in operational state	The number of failures that occurred during communication (transceiver was removed)
		In limit over	The number of frames discarded due to exceeded receiving capacity

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

If the displayed value is 10000 or larger, the display unit varies depending on the displayed value, as follows:

- If the displayed value is 10000 or larger, the unit is K.
- If the displayed value is 10000 K or larger, the unit is M.
- If the displayed value is 10000 M or larger, the unit is G.

In the above cases, one digit is displayed below the decimal point.

#2: This item is always `off` regardless of the port status.

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

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

For details about frame formats, see *16.1.3 Control on the MAC and LLC sublayers* in the manual *Configuration Guide Vol. 1 For Version 11.10*.

#5: The number of times of Long frames includes the number of times of Jabber.

## Impact on communication

None

## Response messages

*Table 16-26:* List of response messages for the show interfaces (40GBASE-R) (Ethernet) command

Message	Description
<switch no.>/<nif no.>/<port no.> is not fortygigabitethernet.	The interface of the specified port is not fortygigabitethernet. Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The port number is outside the valid range. Make sure the specified parameter is correct. <port no.>: Indicates the port number.

## Notes

All display items are cleared in the following cases:

- When the Switch starts up
- The `restart vlan` command is executed.
- When a device hardware failure occurs
- An error occurs in the network interface management program (nimd).

---

## clear counters

---

Clears the Ethernet statistics counters to zero.

### Syntax

```
clear counters
clear counters {gigabitethernet | tengigabitethernet | fortygigabitethernet}
<switch no.>/<nif no.>/<port no.>
```

### Input mode

User mode and administrator mode

### Parameters

{gigabitethernet | tengigabitethernet | fortygigabitethernet}

gigabitethernet

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

tengigabitethernet

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

fortygigabitethernet [AX3800S]

Specifies an Ethernet interface with a maximum line speed of 40 Gbit/s.

<switch no.>/<nif no.>/<port no.>

Specifies the switch number, NIF number, and port number. For the specifiable range of values, see *Specifiable values for parameters*.

Operation when all parameters are omitted:

The statistics counters of all Ethernet interfaces are cleared to zero.

### Operation when a stack configuration is used

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

```
remote command all clear counters
```

```
remote command <switch no.> clear counters [{gigabitethernet | tengigabitethernet}
<switch no.>/<nif no.>/<port no.>]
```

### Example and display items

None

### Impact on communication

None

### Response messages

Table 16-27: List of response messages for the clear counters (Ethernet) command

Message	Description
<switch no.>/<nif no.>/<port no.> is not fortygigabitethernet.	<p>The interface of the specified port is not fortygigabitethernet. Make sure the specified parameter is correct.</p> <p>&lt;switch no.&gt;: Indicates the switch number.</p> <p>&lt;nif no.&gt;: Indicates the NIF number.</p> <p>&lt;port no.&gt;: Indicates the port number.</p>

Message	Description
<switch no.>/<nif no.>/<port no.> is not gigabitethernet.	The interface of the specified port is not gigabitethernet. Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<switch no.>/<nif no.>/<port no.> is not tengigabitethernet.	The interface of the specified port is not tengigabitethernet. Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The port number is outside the valid range. Make sure the specified parameter is correct. <port no.>: Indicates the port number.

## Notes

- Even if the statistics counter is cleared to zero, the value of the MIB information obtained by using SNMP is not cleared to zero.
- The following information items displayed by the `show interfaces` command are cleared to zero:
  - Send and receive statistics
  - Send error statistics
  - Receive error statistics
  - Failure statistics
- All display items are cleared in the following cases:
  - The `restart vlan` command is executed.
  - An error occurs in the network interface management program (nimd).

---

## show port

---

Lists information about the Ethernet ports implemented on the device.

### Syntax

```
show port [<port list>]
show port protocol [<port list>]
show port statistics [<port list>] [{ up | down }] [discard]
show port transceiver [<port list>] [detail]
show port vlan [<port list>] [{ access | trunk | protocol | mac | tunnel }]
```

### Input mode

User mode and administrator mode

### Parameters

<port list>

Lists information about the port numbers specified for Ethernet ports in list format. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

Note that, in a stack configuration, the port of other member switch cannot be specified.

Operation when this parameter is omitted:

Information is listed without any qualifications regarding ports.

protocol

Displays the protocol information of the port.

statistics

Displays the number of sent, received, and discarded packets for ports implemented on the device.

{ up | down }

up

Displays information for ports whose status is up.

down

Displays information for ports whose status is not up. The statuses other than up are as follows:

- down: A line failure has occurred.
- init: Initialization or auto-negotiation is in progress.
- test: A line test is in progress.
- fault: A fault has occurred.
- inact: Operation has been stopped by the `inactivate` command.
- dis: Operation has been stopped by using the `shutdown` or `schedule-power-control shutdown` configuration command.

Operation when this parameter is omitted:

Information is listed without any qualifications regarding ports.

discard

Displays only the information for ports on which the number of discarded packets is 1 or more.

Operation when this parameter is omitted:

Information is listed with no conditions applied.

transceiver

Lists information about whether transceivers are installed on ports that can use removable transceivers and provides type and identification information.

This parameter allows you to check the identification information of each transceiver.

detail

Displays detailed information about transceivers.

Operation when this parameter is omitted:

Normal information about transceivers is displayed.

vlan

Displays VLAN information for ports.

{ access | trunk | protocol | mac | tunnel }

Specifies one of the above keywords as the type of port for which information is to be displayed.

access

Displays VLAN information for access ports.

trunk

Displays VLAN information for trunk ports.

protocol

Displays VLAN information for protocol ports.

mac

Displays VLAN information for MAC ports.

tunnel

Displays VLAN information for tunneling ports.

Operation when this parameter is omitted:

Displays information for all kinds of ports.

Operation when all parameters are omitted:

Lists information for all implemented Ethernet ports.

## Operation when a stack configuration is used

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

```
remote command all show port
```

```
remote command all show port protocol
```

```
remote command all show port statistics [{ up | down }] [discard]
```

```
remote command all show port transceiver [detail]
```

```
remote command all show port vlan [{ access | trunk | protocol | mac | tunnel }]
```

```
remote command <switch no.> show port [<port list>]
```

```
remote command <switch no.> show port protocol [<port list>]
```

```
remote command <switch no.> show port statistics [<port list>] [{ up | down }]
[discard]
```

```
remote command <switch no.> show port transceiver [<port list>] [detail]
remote command <switch no.> show port vlan [<port list>] [{ access | trunk | protocol
| mac | tunnel }]
```

## Example 1

**Figure 16-15:** Example of listing link information for ports (model with QSFP+ port)  
[AX3800S]

```
> show port
Date 20XX/10/29 11:52:49 UTC
Port Counts: 52
Port Name Status Speed Duplex FCtl FrLen ChGr/Status
0/ 1 tengeth1/0/1 up 10GBASE-LR full off 1518 -/-
0/ 2 tengeth1/0/2 inact 1000BASE-SX full(auto) off 1518 1/up
0/ 3 tengeth1/0/3 down - - - -/-
0/ 4 tengeth1/0/4 up 1000BASE-SX full(auto) off 1518 1/up
0/ 5 tengeth1/0/5 down - - - -/-
0/ 6 tengeth1/0/6 down - - - -/-
0/ 7 tengeth1/0/7 down - - - -/-
0/ 8 tengeth1/0/8 inact - - - -/-
0/ 9 tengeth1/0/9 down - - - -/-
0/10 tengeth1/0/10 inact - - - -/-
0/11 tengeth1/0/11 up 10GBASE-CU1M full off 1518 -/-
0/12 tengeth1/0/12 inact - - - -/-
0/13 tengeth1/0/13 down - - - -/-
0/14 tengeth1/0/14 down - - - -/-
0/15 tengeth1/0/15 down - - - -/-
0/16 tengeth1/0/16 down - - - -/-
0/17 tengeth1/0/17 down - - - -/-
0/18 tengeth1/0/18 down - - - -/-
0/19 tengeth1/0/19 down - - - -/-
0/20 tengeth1/0/20 down - - - -/-
0/21 tengeth1/0/21 down - - - -/-
0/22 tengeth1/0/22 down - - - -/-
0/23 tengeth1/0/23 down - - - -/-
0/24 tengeth1/0/24 down - - - -/-
0/25 tengeth1/0/25 down - - - -/-
0/26 tengeth1/0/26 down - - - -/-
0/27 tengeth1/0/27 up 1000BASE-SX full(auto) off 1518 -/-
0/28 tengeth1/0/28 up 1000BASE-SX full(auto) off 1518 -/-
0/29 tengeth1/0/29 down - - - -/-
0/30 tengeth1/0/30 inact - - - 1/up
0/31 tengeth1/0/31 down - - - -/-
0/32 tengeth1/0/32 inact - - - 1/up
0/33 tengeth1/0/33 down - - - -/-
0/34 tengeth1/0/34 inact 1000BASE-SX full(auto) off 1518 1/up
0/35 tengeth1/0/35 down - - - -/-
0/36 tengeth1/0/36 up 1000BASE-SX full(auto) off 1518 1/up
0/37 tengeth1/0/37 down - - - -/-
0/38 tengeth1/0/38 up 1000BASE-SX full(auto) off 1518 1/up
0/39 tengeth1/0/39 down - - - -/-
0/40 tengeth1/0/40 up 1000BASE-SX full(auto) off 1518 1/up
0/41 tengeth1/0/41 up 1000BASE-SX full(auto) off 1518 -/-
0/42 tengeth1/0/42 up 1000BASE-SX full(auto) off 1518 -/-
0/43 tengeth1/0/43 down - - - -/-
0/44 tengeth1/0/44 up 10GBASE-SR full off 1518 -/-
0/45 geth1/0/45 up 1000BASE-T full(auto) off 1518 -/-
0/46 geth1/0/46 up 1000BASE-T full(auto) off 1518 -/-
0/47 geth1/0/47 down - - - -/-
0/48 geth1/0/48 down - - - -/-
0/49 ftygeth1/0/49 up 40GBASE-CU35CM full(auto) off 1518 -/-
0/50 ftygeth1/0/50 down - - - -/-
0/51 ftygeth1/0/51 up 40GBASE-SR4 full off 1518 32/up
0/52 ftygeth1/0/52 up 40GBASE-SR4 full off 1518 32/up
>
```

*Figure 16-16: Example of listing link information for ports (standalone configuration)*

```
>show port
Date 20XX/10/29 11:33:51 UTC
Port Counts: 26
Port  Name           Status   Speed           Duplex          Fctl  FrLen  ChGr/Status
0/ 1  geth1/0/1       up       1000BASE-SX     full(auto)     off   1518   -/-
0/ 2  geth1/0/2       inact    1000BASE-SX     full(auto)     -     -     32/up
0/ 3  geth1/0/3       up       1000BASE-BX10-U full(auto)     off   1518   1/up
0/ 4  geth1/0/4       down     1000BASE-SX     full(auto)     -     -     -/-
0/ 5  geth1/0/5       up       10BASE-T        half(auto)     off   1518   -/-
0/ 6  geth1/0/6       down     -               -               -     -     -/-
0/ 7  geth1/0/7       up       1000BASE-T      full(auto)     off   1518   1/up
0/ 8  geth1/0/8       inact    -               -               -     -     32/up
0/ 9  geth1/0/9       down     -               -               -     -     -/-
0/10  geth1/0/10      inact    -               -               -     -     32/up
0/11  geth1/0/11      down     -               -               -     -     -/-
0/12  geth1/0/12      inact    -               -               -     -     32/up
0/13  geth1/0/13      down     -               -               -     -     -/-
0/14  geth1/0/14      up       1000BASE-T      full(auto)     off   1518   32/up
0/15  geth1/0/15      down     -               -               -     -     -/-
0/16  geth1/0/16      up       1000BASE-T      full(auto)     off   1518   32/up
0/17  geth1/0/17      down     -               -               -     -     -/-
0/18  geth1/0/18      up       1000BASE-T      full(auto)     off   1518   32/up
0/19  geth1/0/19      down     -               -               -     -     -/-
0/20  geth1/0/20      up       1000BASE-T      full(auto)     off   1518   32/up
0/21  geth1/0/21      down     -               -               -     -     -/-
0/22  geth1/0/22      down     -               -               -     -     -/-
0/23  geth1/0/23      up       100BASE-TX      half(auto)     off   1518   -/-
0/24  geth1/0/24      down     -               -               -     -     -/-
0/25  tengeth1/0/25    down     -               -               -     -     -/-
0/26  tengeth1/0/26    up       10GBASE-LR      full(auto)     off   1518   32/up
>
```

*Figure 16-17: Example of listing link information for ports (stack configuration)*

```
> remote command all show port
Switch 1 (Master)
-----
Date 20XX/10/29 11:33:51 UTC
Port Counts: 26
Port  Name           Status   Speed           Duplex          Fctl  FrLen  ChGr/Status
0/ 1  geth1/0/1       up       1000BASE-SX     full(auto)     off   1518   -/-
0/ 2  geth1/0/2       up       1000BASE-SX     full(auto)     -     -     32/up
0/ 3  geth1/0/3       up       1000BASE-BX10-U full(auto)     off   1518   1/up
0/ 4  geth1/0/4       down     1000BASE-SX     full(auto)     -     -     -/-
0/ 5  geth1/0/5       up       10BASE-T        half(auto)     off   1518   -/-
0/ 6  geth1/0/6       down     -               -               -     -     -/-
0/ 7  geth1/0/7       up       1000BASE-T      full(auto)     off   1518   1/up
0/ 8  geth1/0/8       inact    -               -               -     -     32/up
0/ 9  geth1/0/9       down     -               -               -     -     -/-
0/10  geth1/0/10      inact    -               -               -     -     32/up
0/11  geth1/0/11      down     -               -               -     -     -/-
0/12  geth1/0/12      inact    -               -               -     -     32/up
0/13  geth1/0/13      down     -               -               -     -     -/-
0/14  geth1/0/14      up       1000BASE-T      full(auto)     off   1518   -/-
0/15  geth1/0/15      down     -               -               -     -     -/-
0/16  geth1/0/16      up       1000BASE-T      full(auto)     off   1518   -/-
0/17  geth1/0/17      down     -               -               -     -     -/-
0/18  geth1/0/18      up       1000BASE-T      full(auto)     off   1518   -/-
0/19  geth1/0/19      down     -               -               -     -     -/-
0/20  geth1/0/20      up       1000BASE-T      full(auto)     off   1518   -/-
0/21  geth1/0/21      down     -               -               -     -     -/-
0/22  geth1/0/22      down     -               -               -     -     -/-
0/23  geth1/0/23      up       100BASE-TX      half(auto)     off   1518   -/-
0/24  geth1/0/24      down     -               -               -     -     -/-
0/25  tengeth1/0/25    down     -               -               -     -     -/-
0/26  tengeth1/0/26    up       10GBASE-LR      full(auto)     off   -     -/-
```

Switch 2 (Backup)

-----

Port Counts: 26

Port	Name	Status	Speed	Duplex	Fctl	FrLen	ChGr/Status
0/ 1	geth2/0/1	up	1000BASE-SX	full (auto)	off	1518	-/-
0/ 2	geth2/0/2	up	1000BASE-SX	full (auto)	-	-	32/-
0/ 3	geth2/0/3	up	1000BASE-BX10-U	full (auto)	off	1518	1/-
0/ 4	geth2/0/4	down	1000BASE-SX	full (auto)	-	-	-/-
0/ 5	geth2/0/5	up	10BASE-T	half (auto)	off	1518	-/-
0/ 6	geth2/0/6	down	-	-	-	-	-/-
0/ 7	geth2/0/7	up	1000BASE-T	full (auto)	off	1518	1/-
0/ 8	geth2/0/8	inact	-	-	-	-	32/-
0/ 9	geth2/0/9	down	-	-	-	-	-/-
0/10	geth2/0/10	inact	-	-	-	-	32/-
0/11	geth2/0/11	down	-	-	-	-	-/-
0/12	geth2/0/12	inact	-	-	-	-	32/-
0/13	geth2/0/13	down	-	-	-	-	-/-
0/14	geth2/0/14	up	1000BASE-T	full (auto)	off	1518	-/-
0/15	geth2/0/15	down	-	-	-	-	-/-
0/16	geth2/0/16	up	1000BASE-T	full (auto)	off	1518	-/-
0/17	geth2/0/17	down	-	-	-	-	-/-
0/18	geth2/0/18	up	1000BASE-T	full (auto)	off	1518	-/-
0/19	geth2/0/19	down	-	-	-	-	-/-
0/20	geth2/0/20	up	1000BASE-T	full (auto)	off	1518	-/-
0/21	geth2/0/21	down	-	-	-	-	-/-
0/22	geth2/0/22	down	-	-	-	-	-/-
0/23	geth2/0/23	up	100BASE-TX	half (auto)	off	1518	-/-
0/24	geth2/0/24	down	-	-	-	-	-/-
0/25	tengeth2/0/25	down	-	-	-	-	-/-
0/26	tengeth2/0/26	down	10GBASE-LR	full (auto)	off	-	-/-

>

## Display items in Example 1

Table 16-28: Explanation of the display of the link information list for ports

Item	Meaning	Displayed information
Switch	Switch number. The switch status is displayed in parentheses.	Switch number Master: Configures a stack (Master) Backup: Configures a stack (Backup)
Port Counts	Number of target ports	-
Port	Port	NIF number/port number
Name	Port name	The name assigned to a port is displayed.

Item	Meaning	Displayed information
Status	Port state	<p>up: Active (normal operating state).  down: Active (a line failure has occurred).  init: Currently initializing or waiting for establishment of negotiation (auto-negotiation is operating).  test: During line test  fault: Failed  inact: Operation has been stopped by the <code>inactivate</code> command.</p> <ul style="list-style-type: none"> <li>- The standby link functionality of link aggregation</li> <li>- The BPDU guard functionality of a Spanning Tree Protocol</li> <li>- Port resetting of GSRP</li> <li>- The port has been deactivated by the unidirectional link failure detection functionality.</li> <li>- The port has been deactivated by the L2 loop detection functionality.</li> <li>- The port has been deactivated by storm control.</li> </ul> <p>dis: Operation has been stopped by using the <code>shutdown</code> or <code>schedule-power-control shutdown</code> configuration command.</p>
Speed	Line speed	<p>10BASE-T: 10BASE-T  100BASE-TX: 100BASE-TX  1000BASE-T: 1000BASE-T  100BASE-FX: 100BASE-FX [AX3650S]  1000BASE-LX: 1000BASE-LX  1000BASE-SX: 1000BASE-SX  1000BASE-SX2: 1000BASE-SX2 [AX3650S]  1000BASE-LH: 1000BASE-LH  1000BASE-BX10-D: 1000BASE-BX10-D  1000BASE-BX10-U: 1000BASE-BX10-U  1000BASE-BX40-D: 1000BASE-BX40-D  1000BASE-BX40-U: 1000BASE-BX40-U  1000BASE-LHB: 1000BASE-LHB  10GBASE-SR: 10GBASE-SR  10GBASE-LR: 10GBASE-LR  10GBASE-ER: 10GBASE-ER  10GBASE-CU30CM: 10GBASE-CU (30cm)  10GBASE-CU1M: 10GBASE-CU (1m)  10GBASE-CU3M: 10GBASE-CU (3m)  10GBASE-CU5M: 10GBASE-CU (5m)  40GBASE-SR4: 40GBASE-SR4 [AX3800S]  40GBASE-CU35CM: 40GBASE-CR4 (35cm) [AX3800S]  40GBASE-CU1M: 40GBASE-CR4 (1m) [AX3800S]  40GBASE-CU3M: 40GBASE-CR4 (3m) [AX3800S]  40GBASE-CU5M: 40GBASE-CR4 (5m) [AX3800S]</p> <p>-: The speed is unknown (If auto-negotiation is enabled for a 10BASE-T/100BASE-TX/1000BASE-T port and Status is neither up nor test, if Status is init or fault, or if the transceiver status is not connect, a hyphen (-) is displayed.)</p>
Duplex	Full duplex/half duplex	<p>full: Full duplex  full (auto): Full duplex (resulting from auto-negotiation)  half: Half duplex  half (auto): Half duplex (resulting from auto-negotiation)</p> <p>-: The duplex mode is unknown (If auto-negotiation is enabled for a 10BASE-T/100BASE-TX/1000BASE-T port and Status is neither up nor test, if Status is init or fault, or if the transceiver status is not connect, a hyphen (-) is displayed.)</p>

Item	Meaning	Displayed information
FCtl	Flow control	on: Flow control is enabled. off: Flow control is disabled. -: Status is neither up nor test.
FrLen	Maximum frame length	Displays the maximum frame length of a port in octets. -: Status is neither up nor test, or a stack port is used.
ChGr /Status	Channel group and status	The channel group to which the port belongs and the status. Channel group number: 1 to 32 (In a stack configuration, the number is between 1 and 52.) up: Data packets can be sent and received. down: Data packets cannot be sent or received. dis: Link aggregation is disabled. For a port that does not belong to link aggregation, -/- is displayed. In a stack configuration, - is displayed as the status of the backup switch.

## Example 2

Figure 16-18: Example of listing protocol information for ports

```
> show port protocol
Date 20XX/01/26 17:01:40 UTC
Port Counts: 30
Port  Name                Type      VLAN  STP   QoS  Filter  MACTbl  Ext.
0/ 1  geth1/0/1            Trunk     1      0     0     0       0      - - - - -
0/ 2  geth1/0/2            Trunk    1024    0    100    100     7      - - - - -
0/ 3  geth1/0/3            Trunk    256     0     0     0       0      - - - - -
0/ 4  geth1/0/4            Protocol  16      0     1     1       0      - - - - -
0/ 5  geth1/0/5            Access     1     0     0     0       0      - - - - -
0/ 6  geth1/0/6            Access     1     0     0     0       0      - - - - -
0/ 7  geth1/0/7            Access   1000    0     0     0       0      - - - - -
0/ 8  geth1/0/8            Access     1     0     0     0       0      - - - - -
0/ 9  geth1/0/9            Access     1     0     0     0       0      - - - - -
0/10  geth1/0/10           Access     1     0     0     0       0      - - - - -
0/11  geth1/0/11           Access     1     0     0     0       0      - - - - -
0/12  geth1/0/12           Trunk   4000    0     1     1    8000      - - T - -
0/13  geth1/0/13           Trunk   4000    0     1     1       3      - - T - -
0/14  geth1/0/14           Trunk   4000    0     1     1       0      - - T - -
0/15  geth1/0/15           Access     1     0     0     0       0      - - T - -
0/16  geth1/0/16           Access     1     0     0     0       0      - - - - -
0/17  geth1/0/17           Access     1     0     0     0       0      - - - - -
0/18  geth1/0/18           Access     1     0     0     0       0      - - - - -
0/19  geth1/0/19           Access     1     0     0     0       0      - - - - -
0/20  geth1/0/20           Access     1     0     0     0       0      - - - - -
0/21  geth1/0/21           Access     1     0     0     0       0      - - - - -
0/22  geth1/0/22           Access     1     0     0     0       0      - - - - -
0/23  geth1/0/23           Access     1     0     0     0       0      - - - - -
0/24  geth1/0/24           Access     1     0     0     0       0      - - - - -
0/25  tengeth1/0/25         Access     1     0     0     0       0      - - - - -
0/26  tengeth1/0/26         Access     1     0     0     0       0      - - - - -
0/27  tengeth1/0/27         Access     1     0     0     0       0      - - - - -
0/28  tengeth1/0/28         Access     1     0     0     0       0      - - - - -
0/29  tengeth1/0/29         Stack      0      -     -     -       -      - - - - -
0/30  tengeth1/0/30         Stack      0      -     -     -       -      - - - - -
>
```

Figure 16-19: Example of listing protocol information for ports (model with QSFP+ port) [AX3800S]

```
> show port protocol
Date 20XX/10/29 11:52:49 UTC
Port Counts: 52
Port  Name                Type      VLAN  STP   QoS  Filter  MACTbl  Ext.
0/ 1  geth1/0/1            Trunk     1      0     0     0       0      - - - - -
0/ 2  geth1/0/2            Trunk    1024    0    100    100     7      - - - - -
0/ 3  geth1/0/3            Trunk    256     0     0     0       0      - - - - -
0/ 4  geth1/0/4            Protocol  16      0     1     1       0      - - - - -
0/ 5  geth1/0/5            Access     1     0     0     0       0      - - - - -
0/ 6  geth1/0/6            Access     1     0     0     0       0      - - - - -
0/ 7  geth1/0/7            Access   1000    0     0     0       0      - - - - -
0/ 8  geth1/0/8            Access     1     0     0     0       0      - - - - -
0/ 9  geth1/0/9            Access     1     0     0     0       0      - - - - -
0/10  geth1/0/10           Access     1     0     0     0       0      - - - - -
0/11  geth1/0/11           Access     1     0     0     0       0      - - - - -
0/12  geth1/0/12           Trunk   4000    0     1     1    8000      - - T - -
0/13  geth1/0/13           Trunk   4000    0     1     1       3      - - T - -
0/14  geth1/0/14           Trunk   4000    0     1     1       0      - - T - -
0/15  geth1/0/15           Access     1     0     0     0       0      - - T - -
0/16  geth1/0/16           Access     1     0     0     0       0      - - - - -
0/17  geth1/0/17           Access     1     0     0     0       0      - - - - -
0/18  geth1/0/18           Access     1     0     0     0       0      - - - - -
0/19  geth1/0/19           Access     1     0     0     0       0      - - - - -
0/20  geth1/0/20           Access     1     0     0     0       0      - - - - -
0/21  geth1/0/21           Access     1     0     0     0       0      - - - - -
0/22  geth1/0/22           Access     1     0     0     0       0      - - - - -
0/23  geth1/0/23           Access     1     0     0     0       0      - - - - -
0/24  geth1/0/24           Access     1     0     0     0       0      - - - - -
0/25  tengeth1/0/25         Access     1     0     0     0       0      - - - - -
0/26  tengeth1/0/26         Access     1     0     0     0       0      - - - - -
0/27  tengeth1/0/27         Access     1     0     0     0       0      - - - - -
0/28  tengeth1/0/28         Access     1     0     0     0       0      - - - - -
0/29  tengeth1/0/29         Stack      0      -     -     -       -      - - - - -
0/30  tengeth1/0/30         Stack      0      -     -     -       -      - - - - -
>
```

```

0/ 1 tengeth1/0/1   Trunk      1      0      0      0      0      - - - - -
0/ 2 tengeth1/0/2   Trunk    1024    0    100    100    7      - - - - -
0/ 3 tengeth1/0/3   Trunk     256    0      0      0      0      - - - - -
0/ 4 tengeth1/0/4   Protocol  16     0      1      1      0      - - - - -
0/ 5 tengeth1/0/5   Access     1     0      0      0      0      - - - - -
0/ 6 tengeth1/0/6   Access     1     0      0      0      0      - - - - -
0/ 7 tengeth1/0/7   Access   1000    0      0      0      0      - - - - -
0/ 8 tengeth1/0/8   Access     1     0      0      0      0      - - - - -
0/ 9 tengeth1/0/9   Access     1     0      0      0      0      - - - - -
0/10 tengeth1/0/10  Access     1     0      0      0      0      - - - - -
0/11 tengeth1/0/11  Access     1     0      0      0      0      - - - - -
0/12 tengeth1/0/12  Trunk    4000    0      1      1    8000      - - T - -
0/13 tengeth1/0/13  Trunk    4000    0      1      1      3      - - T - -
0/14 tengeth1/0/14  Trunk    4000    0      1      1      0      - - T - -
0/15 tengeth1/0/15  Access     1     0      0      0      0      - - T - -
0/16 tengeth1/0/16  Access     1     0      0      0      0      - - - - -
0/17 tengeth1/0/17  Access     1     0      0      0      0      - - - - -
0/18 tengeth1/0/18  Access     1     0      0      0      0      - - - - -
0/19 tengeth1/0/19  Access     1     0      0      0      0      - - - - -
0/20 tengeth1/0/20  Access     1     0      0      0      0      - - - - -
0/21 tengeth1/0/21  Access     1     0      0      0      0      - - - - -
0/22 tengeth1/0/22  Access     1     0      0      0      0      - - - - -
0/23 tengeth1/0/23  Access     1     0      0      0      0      - - - - -
0/24 tengeth1/0/24  Access     1     0      0      0      0      - - - - -
0/25 tengeth1/0/25  Access     1     0      0      0      0      - - - - -
0/26 tengeth1/0/26  Access     1     0      0      0      0      - - - - -
0/27 tengeth1/0/27  Access     1     0      0      0      0      - - - - -
0/28 tengeth1/0/28  Access     1     0      0      0      0      - - - - -
0/29 tengeth1/0/29  Access     1     0      0      0      0      - - - - -
0/30 tengeth1/0/30  Access     1     0      0      0      0      - - - - -
0/31 tengeth1/0/31  Access     1     0      0      0      0      - - - - -
0/32 tengeth1/0/32  Access     1     0      0      0      0      - - - - -
0/33 tengeth1/0/33  Access     1     0      0      0      0      - - - - -
0/34 tengeth1/0/34  Access     1     0      0      0      0      - - - - -
0/35 tengeth1/0/35  Access     1     0      0      0      0      - - - - -
0/36 tengeth1/0/36  Access     1     0      0      0      0      - - - - -
0/37 tengeth1/0/37  Access     1     0      0      0      0      - - - - -
0/38 tengeth1/0/38  Access     1     0      0      0      0      - - - - -
0/39 tengeth1/0/39  Access     1     0      0      0      0      - - - - -
0/40 tengeth1/0/40  Access     1     0      0      0      0      - - - - -
0/41 tengeth1/0/41  Access     1     0      0      0      0      - - - - -
0/42 tengeth1/0/42  Access     1     0      0      0      0      - - - - -
0/43 tengeth1/0/43  Access     1     0      0      0      0      - - - - -
0/44 tengeth1/0/44  Access     1     0      0      0      0      - - - - -
0/45 geth1/0/45     Access     1     0      0      0      0      - - - - -
0/46 geth1/0/46     Access     1     0      0      0      0      - - - - -
0/47 geth1/0/47     Access     1     0      0      0      0      - - - - -
0/48 geth1/0/48     Access     1     0      0      0      0      - - - - -
0/49 ftygeth1/0/49  Access     1     0      0      0      0      - - - - -
0/50 ftygeth1/0/50  Access     1     0      0      0      0      - - - - -
0/51 ftygeth1/0/51  Access     1     0      0      0      0      - - - - -
0/52 ftygeth1/0/52  Access     1     0      0      0      0      - - - - -

```

&gt;

## Display items in Example 2

Table 16-29: Explanation of the display of the protocol information list for ports

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

Item	Meaning	Displayed information
Type	Port type	Protocol: Protocol VLAN port Trunk: Trunk port Access: Access port MAC: MAC VLAN port Tunnel: Tunneling port Stack: Stack port
VLAN	Number of VLANs that share the port	Number of VLANs that share the port (including the default VLAN and VLANs in suspend status.)
STP	The number used in the Spanning Tree topology calculation	When single is used: 1 When pvst+ is used: The number of VLANs set by pvst+ When mstp is used: The number of instances (When single and pvst+ are mixed, the number of VLANs set by pvst+ + 1) - is displayed for a stack port.
QoS	The number of QoS flow lists	Displays the number of QoS flow lists set for the port. This number includes the number of QoS flow lists set for the VLAN to which the port belongs. - is displayed for a stack port.
Filter	The number of access lists	Displays the number of access lists set for the port. This number includes the number of access lists set for the VLAN to which the port belongs. Note that this value does not include the number of implicitly discarded access lists. - is displayed for a stack port.
MACTbl	The number of dynamically learned entries in the MAC address table	Displays the number of dynamically learned MAC address table entries. - is displayed for a stack port.
Ext.	Extended functionality information	I: Indicates that relay blocking information is set. S: Indicates that storm control information is set. T: Indicates that tag translation is set. L: Indicates that LLDP is running. O: Indicates that OADP is running. A: Indicates that the Ring Protocol is running. - is displayed if the relevant extended functionality is not set or is not running, or a stack port is used.

### Example 3

*Figure 16-20:* Example of displaying the number of sent, received, and discarded packets for ports

```

show port statistics
Date 20XX/10/29 11:33:53 UTC
Port Counts: 26
Port  Name           Status T/R  All packets  Multicast  Broadcast  Discard
0/ 1  geth1/0/1      up    Tx    339          318         10         0
           Rx    31          31         0         0
0/ 2  geth1/0/2      inact Tx    128          120         3         0
           Rx    154         153         1         0
0/ 3  geth1/0/3      up    Tx    63           56         4         0
           Rx    933         933         0         0
0/ 4  geth1/0/4      down  Tx    0            0         0         0
           Rx    0           0         0         0
0/ 5  geth1/0/5      up    Tx    327          310         6         0
           Rx    5           0         4         1
0/ 6  geth1/0/6      down  Tx    0            0         0         0
           Rx    0           0         0         0
0/ 7  geth1/0/7      up    Tx    54           49         2         0
           Rx    32          32         0         0

```

```

0/ 8 geth1/0/8      inact Tx      103      96      2      0
                        Rx      0      0      0      0
0/ 9 geth1/0/9      down Tx      0      0      0      0
                        Rx      0      0      0      0
0/10 geth1/0/10     inact Tx      103      96      2      0
                        Rx      1      1      0      0
0/11 geth1/0/11     down Tx      0      0      0      0
                        Rx      0      0      0      0
0/12 geth1/0/12     inact Tx      103      96      2      0
                        Rx      1      1      0      0
0/13 geth1/0/13     down Tx      0      0      0      0
                        Rx      0      0      0      0
0/14 geth1/0/14     up    Tx      103      96      2      0
                        Rx      62     62      0      0
0/15 geth1/0/15     down Tx      0      0      0      0
                        Rx      0      0      0      0
0/16 geth1/0/16     up    Tx      103      96      2      0
                        Rx      0      0      0      0
0/17 geth1/0/17     down Tx      0      0      0      0
                        Rx      0      0      0      0
0/18 geth1/0/18     up    Tx      103      96      2      0
                        Rx      0      0      0      0
0/19 geth1/0/19     down Tx      0      0      0      0
                        Rx      0      0      0      0
0/20 geth1/0/20     up    Tx      103      96      2      0
                        Rx      0      0      0      0
0/21 geth1/0/21     down Tx      0      0      0      0
                        Rx      0      0      0      0
0/22 geth1/0/22     down Tx      0      0      0      0
                        Rx      0      0      0      0
0/23 geth1/0/23     up    Tx      34      29      5      0
                        Rx     2551    394     12      6
0/24 geth1/0/24     down Tx      0      0      0      0
                        Rx      0      0      0      0
0/25 tengeth1/0/25  down Tx      0      0      0      0
                        Rx      0      0      0      0
0/26 tengeth1/0/26  up    Tx     5679      0     10      0
                        Rx     5158      0     11      0
>

```

### Display items in Example 3

*Table 16-30:* Display of the number of sent, received, and discarded packets for ports

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

Item	Meaning	Displayed information
Status	Port state	<p>up: Active (normal operating state).  down: Active (a line failure has occurred).  init: Currently initializing or waiting for establishment of negotiation (auto-negotiation is operating).  test: During line test  fault: Failed  inact: Operation has been stopped by the <code>inactivate</code> command.</p> <ul style="list-style-type: none"> <li>- The standby link functionality of link aggregation</li> <li>- The BPDU guard functionality of a Spanning Tree Protocol</li> <li>- Port resetting of GSRP</li> <li>- The port has been deactivated by the unidirectional link failure detection functionality.</li> <li>- The port has been deactivated by the L2 loop detection functionality.</li> <li>- The port has been deactivated by storm control.</li> </ul> <p>dis: Operation has been stopped by using the <code>shutdown</code> or <code>schedule-power-control shutdown</code> configuration command.</p>
T/R	Receiving/sending	<p>Tx: Sending  Rx: Receiving</p>
All packets	Number of all packets (including error packets)	
Multicast	Number of multicast packets	
Broadcast	Number of broadcast packets	
Discard	Number of discarded packets	

### Example 4

Figure 16-21: Example of listing transceiver information

```
> show port transceiver
Date 20XX/01/26 12:00:00
Port Counts: 6
Port: 0/ 1 Status:connect Type:SFP Speed:1000BASE-SX
      Vendor name:xxxxxxxxxxxxxxxxx Vendor SN :xxxxxxxxxxxxxxxxx
      Vendor PN :xxxxxxxxxxxxxxxxx Vendor rev:xxxx
Port: 0/ 2 Status:notconnect Type:SFP Speed:-
      Vendor name:- Vendor SN :-
      Vendor PN :- Vendor rev:-
Port: 0/ 3 Status:not support Type:SFP Speed:-
      Vendor name:- Vendor SN :-
      Vendor PN :- Vendor rev:-
Port: 0/ 4 Status:connect Type:SFP Speed:1000BASE-BX10-D
      Vendor name:xxxxxxxxxxxxxxxxx Vendor SN :xxxxxxxxxxxxxxxxx
      Vendor PN :xxxxxxxxxxxxxxxxx Vendor rev:xxxx
(data omitted)
>
```

### Example 5

Figure 16-22: Example of listing detailed transceiver information

```
> show port transceiver detail
Date 20XX/10/06 12:00:00 UTC
Port Counts: 4
Port: 0/ 1 Status:connect Type:SFP Speed:1000BASE-SX
      Vendor name:xxxxxxxxxxxxxxxxx Vendor SN :xxxxxxxxxxxxxxxxx
      Vendor PN :xxxxxxxxxxxxxxxxx Vendor rev:xxxx
      Tx power :-4.7dBm Rx power :-40.0dBm
```

```

Port: 0/ 2 Status:notconnect Type:SFP Speed:-
      Vendor name:-           Vendor SN :-
      Vendor PN  :-           Vendor rev:-
      Tx power   :-           Rx power  :-
Port: 0/ 3 Status:not support Type:SFP Speed:-
      Vendor name:-           Vendor SN :-
      Vendor PN  :-           Vendor rev:-
      Tx power   :-           Rx power  :-
Port: 0/ 4 Status:connect Type:SFP Speed:1000BASE-SX
      Vendor name:xxxxxxxxxxxxxxxxx Vendor SN :xxxxxxxxxxxxxxxxxxx
      Vendor PN  :xxxxxxxxxxxxxxxxx Vendor rev:xxxx
      Tx power   :-4.7dBm           Rx power  :-40.0dBm

```

## Display items in Example 4 and 5

Table 16-31: Display of the transceiver information list

Item	Meaning	Displayed information
Port Counts	Number of target ports	-
Port	Port	NIF number/port number
Status	Status of the transceiver	connect: A transceiver is installed. notconnect: Not installed not support: An unsupported transceiver is installed. -: The status of the transceiver is unknown (- is displayed if the port status is init or fault).
Type	Type of transceiver	SFP: SFP SFP+: SFP+ -: The type of the transceiver is unknown (- is displayed if the transceiver status is notconnect on SFR/SFP+ ports).
Speed	Line speed	10BASE-T/100BASE-TX/1000BASE-T: 10BASE-T/ 100BASE-TX/1000BASE-T 100BASE-FX: 100BASE-FX [AX3650S] 1000BASE-LX: 1000BASE-LX 1000BASE-SX: 1000BASE-SX 1000BASE-SX2: 1000BASE-SX2 [AX3650S] 1000BASE-LH: 1000BASE-LH 1000BASE-BX10-D: 1000BASE-BX10-D 1000BASE-BX10-U: 1000BASE-BX10-U 1000BASE-BX40-D: 1000BASE-BX40-D 1000BASE-BX40-U: 1000BASE-BX40-U 1000BASE-LHB: 1000BASE-LHB 10GBASE-SR: 10GBASE-SR 10GBASE-LR: 10GBASE-LR 10GBASE-ER: 10GBASE-ER 10GBASE-CU30CM: 10GBASE-CU (30cm) 10GBASE-CU1M: 10GBASE-CU (1m) 10GBASE-CU3M: 10GBASE-CU (3m) 10GBASE-CU5M: 10GBASE-CU (5m) -: Unknown line speed (- is displayed if the port status is init or fault, or if the transceiver state is not connect).
Vendor name	Vendor name	Displays the vendor's name. <sup>#1#2</sup>
Vendor SN	Vendor serial number	Displays the serial number added by the vendor. <sup>#1#2</sup>
Vendor PN	Vendor part number	Displays the part number added by the vendor. <sup>#1#2</sup>
Vendor rev	Vendor revision	Displays a part number revision added by the vendor. <sup>#1#2</sup>
Tx power	Sending optical power	Displays the sending optical power in dBm. <sup>#1#2#3#4</sup>

Item	Meaning	Displayed information
Rx power	Receiving optical power	Displays the receiving optical power in dBm. <sup>#1#2#3#4</sup>

#1: - is displayed if the transceiver status is neither connect nor fault.

#2: \*\*\*\* is displayed while transceiver information is being loaded even if the transceiver status is neither connect nor fault. Information is displayed when you re-execute the command. If transceiver information could not be loaded, a hyphen (-) is displayed.

#3: If the optical power is outside the range from -40 to 8.2 dBm, a hyphen (-) is displayed.

#4: An error might arise depending on the environmental requirements. For checking the correct value, use an optical power meter.

### Example 6 [AX3800S]

Figure 16-23: Example of listing transceiver information (QSFP+ port)

```
> show port transceiver 1/0/49-52
Date 20XX/10/06 12:00:00 UTC
Port Counts: 4
Port: 0/49 Status:connect Type:QSFP+ Speed:40GBASE-SR4
      Vendor name:xxxxxxxxxxxxxxxxx Vendor SN :xxxxxxxxxxxxxxxxx
      Vendor PN :xxxxxxxxxxxxxxxxx Vendor rev:xxxx
Port: 0/50 Status:notconnect Type:QSFP+ Speed:-
      Vendor name:- Vendor SN :-
      Vendor PN :- Vendor rev:-
Port: 0/51 Status:not support Type:QSFP+ Speed:-
      Vendor name:- Vendor SN :-
      Vendor PN :- Vendor rev:-
Port: 0/52 Status:connect Type:QSFP+ Speed:40GBASE-SR4
      Vendor name:xxxxxxxxxxxxxxxxx Vendor SN :xxxxxxxxxxxxxxxxx
      Vendor PN :xxxxxxxxxxxxxxxxx Vendor rev:xxxx
>
```

### Example 7 [AX3800S]

Figure 16-24: Example of listing detailed transceiver information (QSFP+ port)

```
> show port transceiver 1/0/49-52 detail
Date 20XX/10/06 12:00:00 UTC
Port Counts: 4
Port: 0/49 Status:connect Type:QSFP+ Speed:40GBASE-SR4
      Vendor name:xxxxxxxxxxxxxxxxx Vendor SN :xxxxxxxxxxxxxxxxx
      Vendor PN :xxxxxxxxxxxxxxxxx Vendor rev:xxxx
      Tx1 power :-4.7dBm Rx1 power :-40.0dBm
      Tx2 power :-4.7dBm Rx2 power :-40.0dBm
      Tx3 power :-4.7dBm Rx3 power :-40.0dBm
      Tx4 power :-4.7dBm Rx4 power :-40.0dBm
Port: 0/50 Status:notconnect Type:QSFP+ Speed:-
      Vendor name:- Vendor SN :-
      Vendor PN :- Vendor rev:-
      Tx1 power :- Rx1 power :-
      Tx2 power :- Rx2 power :-
      Tx3 power :- Rx3 power :-
      Tx4 power :- Rx4 power :-
Port: 0/51 Status:not support Type:QSFP+ Speed:-
      Vendor name:- Vendor SN :-
      Vendor PN :- Vendor rev:-
      Tx1 power :- Rx1 power :-
      Tx2 power :- Rx2 power :-
      Tx3 power :- Rx3 power :-
      Tx4 power :- Rx4 power :-
Port: 0/52 Status:connect Type:QSFP+ Speed:40GBASE-SR4
      Vendor name:xxxxxxxxxxxxxxxxx Vendor SN :xxxxxxxxxxxxxxxxx
      Vendor PN :xxxxxxxxxxxxxxxxx Vendor rev:xxxx
      Tx1 power :-4.7dBm Rx1 power :-40.0dBm
      Tx2 power :-4.7dBm Rx2 power :-40.0dBm
```

Tx3 power : -4.7dBm  
Tx4 power : -4.7dBm

Rx3 power : -40.0dBm  
Rx4 power : -40.0dBm

>

## Display items in Example 6 and 7 [AX3800S]

Table 16-32: Display of the transceiver information list (QSFP+ port)

Item	Meaning	Displayed information
Port Counts	Number of target ports	-
Port	Port	NIF number/port number
Status	Status of the transceiver	connect: A transceiver is installed. notconnect: Not installed not-support: An unsupported transceiver is installed. -: The status of the transceiver is unknown (- is displayed if the port status is init or fault).
Type	Type of transceiver	QSFP+: QSFP+
Speed	Line speed	40GBASE-SR4: 40GBASE-SR4 40GBASE-CU35CM: 40GBASE-CR4 (35cm) 40GBASE-CU1M: 40GBASE-CR4 (1m) 40GBASE-CU3M: 40GBASE-CR4 (3m) 40GBASE-CU5M: 40GBASE-CR4 (5m) -: Unknown line speed (- is displayed if the port status is init or fault, or if the transceiver state is not connect).
Vendor name	Vendor name	Displays the vendor's name. #1#2
Vendor SN	Vendor serial number	Displays the serial number added by the vendor. #1#2
Vendor PN	Vendor part number	Displays the part number added by the vendor. #1#2
Vendor rev	Vendor revision	Displays a part number revision added by the vendor. #1#2
Tx1 power	Lane 1 sending optical power	Displays the sending optical power of Lane 1 in dBm. #1#2#3#4
Rx1 power	Lane 1 receiving optical power	Displays the receiving optical power of Lane 1 in dBm. #1#2#3#4
Tx2 power	Lane 2 sending optical power	Displays the sending optical power of Lane 2 in dBm. #1#2#3#4
Rx2 power	Lane 2 receiving optical power	Displays the receiving optical power of Lane 2 in dBm. #1#2#3#4
Tx3 power	Lane 3 sending optical power	Displays the sending optical power of Lane 3 in dBm. #1#2#3#4
Rx3 power	Lane 3 receiving optical power	Displays the receiving optical power of Lane 3 in dBm. #1#2#3#4
Tx4 power	Lane 4 sending optical power	Displays the sending optical power of Lane 4 in dBm. #1#2#3#4
Rx4 power	Lane 4 receiving optical power	Displays the receiving optical power of Lane 4 in dBm. #1#2#3#4

#1: - is displayed if the transceiver status is neither connect nor fault.

#2: \*\*\*\* is displayed while transceiver information is being loaded even if the transceiver status is neither connect nor fault. Information is displayed when you re-execute the command. If transceiver information could not be loaded, a hyphen (-) is displayed.

#3: If the optical power is outside the range from -40 to 8.2 dBm, a hyphen (-) is displayed.

#4: An error might arise depending on the environmental requirements. To check the correct value, use an optical power meter.

## Example 8

*Figure 16-25: Example of listing VLAN information for ports (standalone configuration)*

```
> show port vlan
Date 20XX/11/15 14:15:00
Port Counts: 26
Port  Name                Status Type      VLAN
0/ 1 geth1/0/1            up      Protocl   100,1100-1103
0/ 2 geth1/0/2            up      Mac       200,1200,1204,1205
0/ 3 geth1/0/3            up      Trunk     1-4094
0/ 4 geth1/0/4            up      Trunk     1,3,5,7,9,11,13,15,17,19,21,23,25,27,
                                   29,31,33,35,37,39,41,43,45,47,49,120,
                                   130,140
0/ 5 geth1/0/5            up      Access    100 (Global IP Network VLAN)
0/ 6 geth1/0/6            down    Access    100 (Global IP Network VLAN)
0/ 7 geth1/0/7            down    Access    100 (Global IP Network VLAN)
0/ 8 geth1/0/8            up      Access    1 (DefaultVLAN)
0/ 9 geth1/0/9            up      Access    1 (DefaultVLAN)
0/10 geth1/0/10           up      Access    1 (DefaultVLAN)
0/11 geth1/0/11           up      Access    1 (DefaultVLAN)
0/12 geth1/0/12           up      Access    1 (DefaultVLAN)
0/13 geth1/0/13           up      Access    1 (DefaultVLAN)
0/14 geth1/0/14           up      Access    1 (DefaultVLAN)
0/15 geth1/0/15           up      Access    1 (DefaultVLAN)
0/16 geth1/0/16           up      Access    1 (DefaultVLAN)
0/17 geth1/0/17           up      Access    1 (DefaultVLAN)
0/18 geth1/0/18           up      Access    1 (DefaultVLAN)
0/19 geth1/0/19           up      Access    1 (DefaultVLAN)
0/20 geth1/0/20           up      Access    1 (DefaultVLAN)
0/21 geth1/0/21           up      Access    1 (DefaultVLAN)
0/22 geth1/0/22           up      Access    1 (DefaultVLAN)
0/23 geth1/0/23           up      Access    1 (DefaultVLAN)
0/24 geth1/0/24           up      Access    1 (DefaultVLAN)
0/25 tengeth1/0/25        up      Access    1 (DefaultVLAN)
0/26 tengeth1/0/26        up      Access    1 (DefaultVLAN)
```

*Figure 16-26: Example of listing VLAN information for ports (stack configuration)*

```
> remote command all show port vlan
Switch 1 (Master)
-----
Date 20XX/11/15 14:15:00
Port Counts: 26
Port  Name                Status Type      VLAN
0/ 1 geth1/0/1            up      Protocl   100,1100-1103
0/ 2 geth1/0/2            up      Mac       200,1200,1204,1205
0/ 3 geth1/0/3            up      Trunk     1-4093
0/ 4 geth1/0/4            up      Trunk     1,3,5,7,9,11,13,15,17,19,21,23,25,27,
                                   29,31,33,35,37,39,41,43,45,47,49,120,
                                   130,140
0/ 5 geth1/0/5            up      Access    100 (Global IP Network VLAN)
0/ 6 geth1/0/6            down    Access    100 (Global IP Network VLAN)
0/ 7 geth1/0/7            down    Access    100 (Global IP Network VLAN)
0/ 8 geth1/0/8            up      Access    1 (DefaultVLAN)
0/ 9 geth1/0/9            up      Access    1 (DefaultVLAN)
0/10 geth1/0/10           up      Access    1 (DefaultVLAN)
0/11 geth1/0/11           up      Access    1 (DefaultVLAN)
0/12 geth1/0/12           up      Access    1 (DefaultVLAN)
0/13 geth1/0/13           up      Access    1 (DefaultVLAN)
0/14 geth1/0/14           up      Access    1 (DefaultVLAN)
0/15 geth1/0/15           up      Access    1 (DefaultVLAN)
0/16 geth1/0/16           up      Access    1 (DefaultVLAN)
0/17 geth1/0/17           up      Access    1 (DefaultVLAN)
```

```

0/18 geth1/0/18      up      Access  1      (DefaultVLAN)
0/19 geth1/0/19      up      Access  1      (DefaultVLAN)
0/20 geth1/0/20      up      Access  1      (DefaultVLAN)
0/21 geth1/0/21      up      Access  1      (DefaultVLAN)
0/22 geth1/0/22      up      Access  1      (DefaultVLAN)
0/23 geth1/0/23      up      Access  1      (DefaultVLAN)
0/24 geth1/0/24      up      Access  1      (DefaultVLAN)
0/25 tengeth1/0/25   up      Access  1      (DefaultVLAN)
0/26 tengeth1/0/26   up      Stack   -

```

#### Switch 2 (Backup)

-----

Port Counts: 26

```

Port  Name      Status Type      VLAN
0/ 1 geth2/0/1   up    Protocl  100,1100-1103
0/ 2 geth2/0/2   up    Mac      200,1200,1204,1205
0/ 3 geth2/0/3   up    Trunk    1-4093
0/ 4 geth2/0/4   up    Trunk    1,3,5,7,9,11,13,15,17,19,21,23,25,27,
                                29,31,33,35,37,39,41,43,45,47,49,120,
                                130,140
0/ 5 geth2/0/5   up    Access   100 (Global IP Network VLAN)
0/ 6 geth2/0/6   down  Access   100 (Global IP Network VLAN)
0/ 7 geth2/0/7   down  Access   100 (Global IP Network VLAN)
0/ 8 geth2/0/8   up    Access   1 (DefaultVLAN)
0/ 9 geth2/0/9   up    Access   1 (DefaultVLAN)
0/10 geth2/0/10  up    Access   1 (DefaultVLAN)
0/11 geth2/0/11  up    Access   1 (DefaultVLAN)
0/12 geth2/0/12  up    Access   1 (DefaultVLAN)
0/13 geth2/0/13  up    Access   1 (DefaultVLAN)
0/14 geth2/0/14  up    Access   1 (DefaultVLAN)
0/15 geth2/0/15  up    Access   1 (DefaultVLAN)
0/16 geth2/0/16  up    Access   1 (DefaultVLAN)
0/17 geth2/0/17  up    Access   1 (DefaultVLAN)
0/18 geth2/0/18  up    Access   1 (DefaultVLAN)
0/19 geth2/0/19  up    Access   1 (DefaultVLAN)
0/20 geth2/0/20  up    Access   1 (DefaultVLAN)
0/21 geth2/0/21  up    Access   1 (DefaultVLAN)
0/22 geth2/0/22  up    Access   1 (DefaultVLAN)
0/23 geth2/0/23  up    Access   1 (DefaultVLAN)
0/24 geth2/0/24  up    Access   1 (DefaultVLAN)
0/25 tengeth2/0/25 up    Access   1 (DefaultVLAN)
0/26 tengeth2/0/26 up    Stack    -

```

Figure 16-27: Example of listing VLAN information for trunk ports

```

> show port vlan trunk
Date 20XX/11/15 14:15:00
Port Counts: 2
Port  Name      Status Type      VLAN
0/ 3 geth1/0/3   up    Trunk    1-4094
0/ 4 geth1/0/4   up    Trunk    1,3,5,7,9,11,13,15,17,19,21,23,25,27,
                                29,31,33,35,37,39,41,43,45,47,49,120,
                                130,140

```

## Display items in Example 8

Table 16-33: Description of displayed items (VLAN information for ports)

Item	Meaning	Displayed information
Switch	Switch number. The switch status is displayed in parentheses.	Switch number Master: Configures a stack (Master) Backup: Configures a stack (Backup)
Port counts	Number of target ports	-

Item	Meaning	Displayed information
Port	Port number	NIF number/port number of the port whose information is to be displayed
Name	Model name	The name assigned to a port
Status	Port state	<p>up: Active (normal operating state).  down: Active (a line failure has occurred).  init: Currently initializing or waiting for establishment of negotiation (auto-negotiation is operating).  test: During line test  fault: Failed  inact: Operation has been stopped by the <code>inactivate</code> command.</p> <ul style="list-style-type: none"> <li>- The standby link functionality of link aggregation</li> <li>- The BPDU guard functionality of a Spanning Tree Protocol</li> <li>- Port resetting of GSRP</li> <li>- The port has been deactivated by the unidirectional link failure detection functionality.</li> <li>- The port has been deactivated by the L2 loop detection functionality.</li> <li>- The port has been deactivated by storm control.</li> </ul> <p>dis: Operation has been stopped by using the <code>shutdown</code> or <code>schedule-power-control shutdown</code> configuration command.</p>
Type	Port type	<p>Access: Access port  Trunk: Trunk port  Protocol: Protocol VLAN port  Mac: MAC VLAN port  Tunnel: Tunneling port  Stack: Stack port</p>
VLAN	VLAN ID	<p>The list of VLANs set for a port.  If only one VLAN has been set, the VLAN name is also displayed.  If no VLAN exists, a hyphen (-) is displayed.</p>

## Impact on communication

None

## Response messages

Table 16-34: List of response messages for the show port command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Manager.	Communication with the <code>L2Manager</code> program failed. Re-execute the command. If this message is output frequently, execute the <code>restart vlan</code> command to restart the <code>L2Manager</code> program.
Connection failed to Link Aggregation.	Communication with the link aggregation program failed. Re-execute the command. If this message is output frequently, execute the <code>restart link-aggregation</code> command to restart the link aggregation program.
Connection failed to LLDP.	Communication with the LLDP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart lldp</code> command to restart the LLDP program.

Message	Description
Connection failed to OADP.	Communication with the OADP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart oadp</code> command to restart the OADP program.
Connection failed to Ring Protocol.	Communication with the Ring Protocol program failed. Re-execute the command. If this message is output frequently, execute the <code>restart axrp</code> command to restart the Ring Protocol program.
Connection failed to Spanning Tree.	Communication with the Spanning Tree program failed. Re-execute the command. If this message is output frequently, execute the <code>restart spanning-tree</code> command to restart the Spanning Tree program.
No operational Port.	There are no available ports. Make sure the specified parameter is correct.

## Notes

- The displayed number of discarded packets is the total of the values for the items listed in the following table.

*Table 16-35: Statistical items used for calculating the number of discarded packets*

Port	Statistical item	
	Sending	Receiving
Ethernet	Late collision Excessive collisions Excessive deferral	CRC errors Alignment Fragments Jabber Symbol errors Short frames Long frames

- The statistic counter is cleared in the following cases:
  - When the Switch starts up
  - When the `clear counters` command is executed
  - The `restart vlan` command is executed.
  - When a device hardware failure occurs
  - An error occurs in the network interface management program (nimd).

---

## activate

---

Returns the status of the Ethernet port to active from inactive when the `inactivate` command has been used to set inactive.

### Syntax

```
activate {gigabitethernet | tengigabitethernet | fortygigabitethernet} <switch
no.>/<nif no.>/<port no.>
```

### Input mode

User mode and administrator mode

### Parameters

{gigabitethernet | tengigabitethernet | fortygigabitethernet}

gigabitethernet

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

tengigabitethernet

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

fortygigabitethernet [AX3800S]

Specifies an Ethernet interface with a maximum line speed of 40 Gbit/s.

<switch no.>/<nif no.>/<port no.>

Specifies the switch number, NIF number, and port number. For the specifiable range of values, see *Specifiable values for parameters*.

### Operation when a stack configuration is used

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

```
remote command <switch no.> activate {gigabitethernet | tengigabitethernet}
<switch no.>/<nif no.>/<port no.>
```

### Example

In the following example, the status of the port whose switch number is 1, NIF number is 0, and port number is 1 is reset to active.

```
activate gigabitethernet 1/0/1
```

### Display items

None

### Impact on communication

Communication using the relevant Ethernet port resumes.

### Response messages

Table 16-36: List of response messages for the activate command

Message	Description
<switch no.>/<nif no.>/<port no.> is already active.	The specified port is already active. The command does not need to be executed if you correctly specified the port. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.

Message	Description
<switch no.>/<nif no.>/<port no.> is already initializing.	The specified port is already being initialized. The command does not need to be executed if you correctly specified the port. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<switch no.>/<nif no.>/<port no.> is disabled.	The specified port is in <code>disable</code> status due to the configuration. Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<switch no.>/<nif no.>/<port no.> is failed.	A failure has occurred or a line test is being conducted on the specified port. Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<switch no.>/<nif no.>/<port no.> is not fortygigabitethernet.	The interface of the specified port is not <code>fortygigabitethernet</code> . Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<switch no.>/<nif no.>/<port no.> is not gigabitethernet.	The interface of the specified port is not <code>gigabitethernet</code> . Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<switch no.>/<nif no.>/<port no.> is not tengigabitethernet.	The interface of the specified port is not <code>tengigabitethernet</code> . Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The port number is outside the valid range. Make sure the specified parameter is correct. <port no.>: Indicates the port number.

## Notes

Executing this command does not change the configuration.

---

## inactivate

---

Changes the status of an Ethernet port from *active* to *inactive* without changing the configuration.

### Syntax

```
inactivate {gigabitethernet | tengigabitethernet | fortygigabitethernet} <switch
no.>/<nif no.>/<port no.>
```

### Input mode

User mode and administrator mode

### Parameters

{gigabitethernet | tengigabitethernet | fortygigabitethernet}

gigabitethernet

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

tengigabitethernet

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

fortygigabitethernet [AX3800S]

Specifies an Ethernet interface with a maximum line speed of 40 Gbit/s.

<switch no.>/<nif no.>/<port no.>

Specifies the switch number, NIF number, and port number. For the specifiable range of values, see *Specifiable values for parameters*.

### Operation when a stack configuration is used

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

```
remote command <switch no.> inactivate {gigabitethernet | tengigabitethernet}
<switch no.>/<nif no.>/<port no.>
```

### Example

In the following example, the status of the port whose switch number is 1, NIF number is 0, and port number is 1 is changed to *inactive*.

```
inactivate gigabitethernet 1/0/1
```

### Display items

None

### Impact on communication

Communication using the relevant Ethernet port becomes unavailable.

### Response messages

Table 16-37: List of response messages for the inactivate command

Message	Description
<switch no.>/<nif no.>/<port no.> is already inactive.	The specified port is already <i>inactive</i> . The command does not need to be executed if you correctly specified the port. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.

Message	Description
<switch no.>/<nif no.>/<port no.> is disabled.	The specified port is in <code>disable</code> status due to the configuration. Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<switch no.>/<nif no.>/<port no.> is failed.	The specified port is not in the <code>active</code> status. Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<switch no.>/<nif no.>/<port no.> is not fortygigabitethernet.	The interface of the specified port is not <code>fortygigabitethernet</code> . Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<switch no.>/<nif no.>/<port no.> is not gigabitethernet.	The interface of the specified port is not <code>gigabitethernet</code> . Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<switch no.>/<nif no.>/<port no.> is not tengigabitethernet.	The interface of the specified port is not <code>tengigabitethernet</code> . Make sure the specified parameter is correct. <switch no.>: Indicates the switch number. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The port number is outside the valid range. Make sure the specified parameter is correct. <port no.>: Indicates the port number.
Line test executing.	A line test is being conducted. To change the status of the specified port to <code>inactive</code> , cancel the line test, and then re-execute the command (for details about canceling a line test, see <i>no test interfaces</i> ).

## Notes

- Executing this command does not change the configuration.
- If the device is restarted after command execution, the `inactive` status is canceled.
- To re-activate an Ethernet port that has been inactivated by this command, use the `activate` command.
- This command cannot be executed for a port for which a line test is being conducted. Before executing the command, make sure you use the `no test interfaces` command to stop the line test.

---

## test interfaces

---

If an error occurs in communication over an Ethernet network, this command can be used to identify the faulty part. After the faulty part (such as a cable) has been replaced, this command can also be used to verify operation (conduct a line test) on a frame basis.

Before you conduct a line test, make sure you use the `inactivate` command to change the status of the port to `inactive`. For details about line tests, see the *Troubleshooting Guide*.

### Syntax

```
test interfaces gigabitethernet <nif no.>/<port no.> {internal | connector}
    [auto_negotiation {10base-t | 100base-tx | 1000base-t}]
    [interval <interval time>] [pattern <test pattern no.>]
    [length <data length>]
test interfaces tengigabitethernet <nif no.>/<port no.> {internal | connector}
    [interval <interval time>] [pattern <test pattern no.>]
    [length <data length>]
test interfaces fortygigabitethernet <nif no.>/<port no.> {internal | connector}
    [interval <interval time>] [pattern <test pattern no.>]
    [length <data length>]
```

### Input mode

User mode and administrator mode

### Parameters

`gigabitethernet`

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

`tengigabitethernet`

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

`fortygigabitethernet [AX3800S]`

Specifies an Ethernet interface with a maximum line speed of 40 Gbit/s.

`<nif no.>/<port no.>`

Specifies the NIF number and the port number. For the specifiable range of values, see *Specifiable values for parameters*.

`internal`

Specifies that an internal loopback test will be conducted.

`connector`

Specifies that a loop connector loopback test will be conducted.

Before you conduct a loop connector loopback test, make sure that the loop connector has been connected.

`auto_negotiation {10base-t | 100base-tx | 1000base-t}`

Specifies the segment standard that will be used for a line test conducted when `auto` is specified in the `speed` configuration command.

Note that this parameter can be specified only when `auto` is specified in the `speed` command. Also note that this parameter can be specified for RJ45 ports only when the line type is 10BASE-T/100BASE-TX/1000BASE-T.

Operation when this parameter is omitted:

The command assumes that `100base-tx` is specified.

`interval <interval time>`

Specifies the number of seconds as the sending interval. You can specify a decimal number from 1 to 30.

Operation when this parameter is omitted:

The sending interval defaults to 1 second.

`pattern <test pattern no.>`

Specifies the number of the test pattern. You can specify a value from 0 to 4.

0: Repeats using test patterns 1 to 4.

1: all 0xff

2: all 0x00

3:

**\*\* THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG.0123456789 \*\*** pattern repeated

4: Send a data corruption detection pattern.

Operation when this parameter is omitted:

Test pattern 3 is used.

`length <data length>`

Specifies in octets the data length of the frame (excluding the MAC header and the FCS field) to be used for the test. For the value that you can specify, see the following table.

*Table 16-38: Specifiable range of values for each test*

#	Test	Data length (in octets)	Default (in octets)
1	Internal loopback test	46 to 1500	500
2	Loop connector loopback test	46 to 9216 <sup>#</sup>	500

<sup>#</sup>: If `10base-t` is set for the `auto_negotiation` parameter, the maximum that can be specified is 1500 octets.

Operation when all parameters are omitted:

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

## Operation when a stack configuration is used

This command is not supported.

## Example

The following figure shows an example of the screen displayed at the start of an Ethernet line test. This example starts an internal loopback test that sends a 100-octet frame in the all-0xff test pattern at five-second intervals to the port number of 2.

*Figure 16-28: Example of a screen displayed at the start of a line test*

```
> test interfaces gigabitethernet 0/2 internal interval 5 pattern 1 length 100
```

## Display items

None

## Impact on communication

None

## Response messages

Table 16-39: List of response messages for the test interfaces command

Message	Description
<nif no.>/<port no.> is disabled.	The specified port is in <code>disable</code> status due to the configuration. Make sure the specified parameter is correct. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<nif no.>/<port no.> is failed.	The specified port has failed. Make sure the specified parameter is correct. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<nif no.>/<port no.> is not fortygigabitethernet.	The interface of the specified port is not <code>fortygigabitethernet</code> . Make sure the specified parameter is correct. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<nif no.>/<port no.> is not gigabitethernet.	The interface of the specified port is not <code>gigabitethernet</code> . Make sure the specified parameter is correct. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<nif no.>/<port no.> is not tengigabitethernet.	The interface of the specified port is not <code>tengigabitethernet</code> . Make sure the specified parameter is correct. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
Can't execute this commad in all switches configured stack.	In a stack configuration, the command cannot be executed.
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The port number is outside the valid range. Make sure the specified parameter is correct. <port no.>: Indicates the port number.
No auto negotiation Port <nif no.>/<port no.>	The specified port is not subject to auto-negotiation. Make sure the specified parameter is correct. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
No operational Port <port no.>.	The specified port is not in a state in which commands can be executed. Make sure the specified parameter is correct. <port no.>: Indicates the port number.
No support auto negotiation parameter.	The specified port does not support auto-negotiation parameters. Make sure the specified parameter is correct.
Test already executing.	A test is already being conducted on the specified port or another port. The command does not need to be executed if you correctly specified the port. Alternatively, stop the test for the other port, and then re-execute the command.

## Notes

- Before you insert or remove a loop connector, make sure that the port is in `inactive` status.

- After a line test has started, the test processing is repeated until a request to stop the test is issued.
- To conduct a loop connector loopback test by specifying `1000base-t` for the `auto_negotiation` parameter, an eight-core, four-pair loop connector of category 5 or higher is required.
- Please conduct a line test for each port.
- To conduct a loop connector loopback test on a 1000BASE-LH, 1000BASE-LHB, or 10GBASE-ER port, an optical attenuator is required. For details about optical attenuation, see the following table.

*Table 16-40: Optical attenuation*

Line type	Attenuation value (dB)
1000BASE-LH	5 to 22
1000BASE-LHB	17 to 36
10GBASE-ER	5 to 11

- You cannot conduct a normal loop connector loopback test on a 1000BASE-BX port because the port uses different wavelengths for sending and receiving and uses a one-core optical fiber cable.
- If you connect or disconnect a transceiver while a line test is being conducted, all count values displayed in the test results might be 0. In addition, when you connect or disconnect a transceiver, if you start a line test before a log message indicating that a transceiver was connected or disconnected is displayed, the log message might not be output. In both cases, you can continue operation because the normal operating status is restored after you execute the `no test interface` command.

---

## no test interfaces

---

Stops an Ethernet line test, and displays the test results.

For details about line tests, see the *Troubleshooting Guide*.

### Syntax

```
no test interfaces gigabitethernet <nif no.>/<port no.>
no test interfaces tengigabitethernet <nif no.>/<port no.>
no test interfaces fortygigabitethernet <nif no.>/<port no.>
```

### Input mode

User mode and administrator mode

### Parameters

gigabitethernet

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

tengigabitethernet

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

fortygigabitethernet [AX3800S]

Specifies an Ethernet interface with a maximum line speed of 40 Gbit/s.

<nif no.>/<port no.>

Specifies the NIF number and the port number. For the specifiable range of values, see *Specifiable values for parameters*.

### Operation when a stack configuration is used

This command is not supported.

### Example

This example starts an internal loopback test that sends a 100-octet frame in the all-0xff test pattern at five-second intervals. The following figure shows the result of executing a line test for the Ethernet board.

*Figure 16-29: Result of executing line tests*

```
>test interfaces gigabitethernet 0/2 internal interval 5 pattern 1 length 100
>no test interfaces gigabitethernet 0/2
Date 20XX/10/23 12:00:00 UTC
Interface type           :1000BASE-LX
Test count               :60
Send-OK                  :60          Send-NG                  :0
Receive-OK               :60          Receive-NG              :0
Data compare error       :0
Out buffer hunt error     :0          Out line error          :0
In CRC error              :0          In alignment            :0
In monitor time out      :0          In line error           :0
H/W error                 :none
>
```

## Display items

Table 16-41: Items displayed as line test results

Item	Meaning	Presumed cause	Measures
Interface type	Line type <ul style="list-style-type: none"> <li>• 10BASE-T</li> <li>• 100BASE-TX</li> <li>• 1000BASE-T</li> <li>• 100BASE-FX [AX3650S]</li> <li>• 1000BASE-LX</li> <li>• 1000BASE-SX</li> <li>• 1000BASE-SX2 [AX3650S]</li> <li>• 1000BASE-LH</li> <li>• 1000BASE-BX10-D</li> <li>• 1000BASE-BX10-U</li> <li>• 1000BASE-BX40-D</li> <li>• 1000BASE-BX40-U</li> <li>• 1000BASE-LHB</li> <li>• 10GBASE-SR</li> <li>• 10GBASE-LR</li> <li>• 10GBASE-ER</li> <li>• 10GBASE-CU30CM</li> <li>• 10GBASE-CU1M</li> <li>• 10GBASE-CU3M</li> <li>• 10GBASE-CU5M</li> <li>• 40GBASE-SR4 [AX3800S]</li> <li>• 40GBASE-CU35CM [AX3800S]</li> <li>• 40GBASE-CU1M [AX3800S]</li> <li>• 40GBASE-CU3M [AX3800S]</li> <li>• 40GBASE-CU5M [AX3800S]</li> <li>• ----#1</li> </ul>	--	--
Test count	Number of times a test was conducted	--	--
Send-OK	Number of times data was sent normally	--	--
Send-NG	Number of times data was sent abnormally	Sum of frames discarded due to a line error	For a loop connector loopback test, verify that a loopback connector is correctly connected to the port.
Receive-OK	Number of times data was received normally	--	--
Receive-NG	Number of times data was received abnormally	Sum of the number of times a data compare error occurred and the number of times reception monitoring timed out	See <i>Data compare error</i> and subsequent items in this table.
Data compare error	Number of data compare errors (number of received frames that did not match the sent frames)	Line error	Replace the switch.
Out buffer hunt error	Number of times a send buffer could not be secured	Congestion on another port	Resolve the congestion on the other port, and then try again.

Item	Meaning	Presumed cause	Measures
Out line error	Number of send line errors that occurred	Line error	Replace the switch.
In CRC error	The number of times the frame length was valid but an error was detected by the FCS check <sup>#2</sup>	Line error	Replace the switch.
In alignment	The number of times the frame length was invalid and an error was detected by the FCS check <sup>#2</sup>	Line error	Replace the switch.
In monitor time out	Timeout for the reception monitoring timer	Line error	For a loop connector loopback test, verify that a loopback connector is correctly connected to the port. <sup>#3</sup>
In line error	Number of receive line errors that occurred	Line error	For a loop connector loopback test, verify that a loopback connector is correctly connected to the port.
H/W error	Whether a hardware error has occurred. none: No hardware error occurred. occurred: A hardware error occurred.	Line error	Replace the switch.

#1: The line type is unknown. This is indicated in the following cases:

- The transceiver status is not `connect`.
- A line test was stopped immediately after it started.
- A line failure occurred.

#2: The frame length indicates the length starting from the MAC header and ending with the FCS field. For details about frame formats, see *16.1.3 Control on the MAC and LLC sublayers* in the manual *Configuration Guide Vol. 1 For Version 11.10*.

#3: If the loop connector is connected correctly, packets for the line test might have accumulated in the device. Make sure that the packet forwarding load on the device on which the line test is being conducted is low, and then try again.

## Impact on communication

None

## Response messages

Table 16-42: List of response messages for the no test interfaces command

Message	Description
<nif no.>/<port no.> is not fortygigabitethernet.	The interface of the specified port is not fortygigabitethernet. Make sure the specified parameter is correct. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
<nif no.>/<port no.> is not gigabitethernet.	The interface of the specified port is not gigabitethernet. Make sure the specified parameter is correct. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.

Message	Description
<nif no.>/<port no.> is not tengigabitethernet.	The interface of the specified port is not tengigabitethernet. Make sure the specified parameter is correct. <nif no.>: Indicates the NIF number. <port no.>: Indicates the port number.
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The port number is outside the valid range. Make sure the specified parameter is correct. <port no.>: Indicates the port number.
No operational port--<port no.>.	The specified port is not in a state in which commands can be executed. Make sure the specified parameter is correct. <port no.>: Indicates the port number.
Test not executing.	No line test has been conducted. Make sure the specified parameter is correct.

## Notes

- Before you insert or remove a loop connector, make sure that the port is in `inactive` status.
- When a line test is stopped, depending on the timing, the test might stop while the command is waiting for the response to a test frame that was sent. Therefore, in the displayed test results, the total of `Receive-OK` and `Receive-NG` values could be one smaller than the `Send-OK` value.

## Chapter

---

# 17. Link Aggregation

---

```
show channel-group  
show channel-group statistics  
clear channel-group statistics lacp  
restart link-aggregation  
dump protocols link-aggregation
```

---

## show channel-group

---

Displays link aggregation information.

### Syntax

```
show channel-group [{ [<channel group list>] [detail] | summary}]
```

### Input mode

User mode and administrator mode

### Parameters

```
{ [<channel group list>] [detail] | summary}
```

<channel group list>

Displays link aggregation information for the channel group numbers specified in list format. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

All link aggregation information is displayed.

detail

Displays detailed link aggregation information.

Operation when this parameter is omitted:

Link aggregation information is displayed.

summary

Displays summary information about link aggregation.

Operation when this parameter is omitted:

Complete link aggregation information is displayed.

### Operation when a stack configuration is used

The command can display information only for the master switch.

### Example 1

The following shows an example of displaying information about link aggregation.

*Figure 17-1: Example of displaying information about link aggregation*

```
>show channel-group
Date 20XX/12/10 12:00:00 UTC
channel-group Counts:4
ChGr:1    Mode:LACP
  CH Status    :Up           Elapsed Time:10:10:39
  Multi Speed  :Off          Load Balance:src-dst-port
  Max Active Port:8
  Max Detach Port:7
  Description  : 6 ports aggregated.
  MAC address: 0012.e2ac.8301   VLAN ID:
  Periodic Timer:Short
  Actor information: System Priority:1    MAC: 0012.e212.ff02
                        KEY:1
  Partner information: System Priority:10000 MAC: 0012.e2f0.69be
                        KEY:10
  Port (6)      :1/0/1-3,10,12-13
  Up Port (2)   :1/0/1-2
  Down Port (4) :1/0/3,10,12-13
```

```

ChGr:11   Mode:LACP
  CH Status      :Down      Elapsed Time:-
  Multi Speed    :Off        Load Balance:src-dst-port
  Max Active Port:8
  Max Detach Port:7
  MAC address: 0012.e2ac.8302      VLAN ID:30-35,40
  Periodic Timer:Long
  Actor information: System Priority:1      MAC: 0012.e212.ff02
                                   KEY:11
  Partner information: System Priority:10000 MAC: 0012.e2f0.69bd
                                   KEY:20
  Port(3)        :1/0/4-6
  Up Port(0)      :
  Down Port(3)    :1/0/4-6
ChGr:21   Mode:Static
  CH Status      :Disabled   Elapsed Time:-
  Multi Speed    :Off        Load Balance:src-dst-port
  Max Active Port:8
  Max Detach Port:7
  MAC address: 0012.e2ac.8304      VLAN ID:200
  Port(2)        :1/0/7-8
  Up Port(0)      :
  Down Port(2)    :1/0/7-8
ChGr:22   Mode:Static
  CH Status      :Up         Elapsed Time:160.11:45:10
  Multi Speed    :Off        Load Balance:src-dst-port
  Max Active Port:2 (no-link-down mode)
  Max Detach Port:7
  MAC address: 0012.e2ac.8305      VLAN ID:250
  Port(3)        :1/0/9,14-15
  Up Port(2)      :1/0/9,14
  Down Port(1)    :1/0/15
  Standby Port(1) :1/0/15
>

```

The following shows an example of displaying the link aggregation information for a specific channel group number.

*Figure 17-2: Example of displaying the link aggregation information for a specific channel group number*

```

>show channel-group 21-30
Date 20XX/12/10 12:00:00 UTC
channel-group Counts:2
  ChGr:21   Mode:Static
    CH Status      :Disabled   Elapsed Time:-
    Multi Speed    :Off        Load Balance:src-dst-port
    Max Active Port:8
    Max Detach Port:7
    MAC address: 0012.e2ac.8304      VLAN ID:200
    Port(2)        :1/0/7-8
    Up Port(0)      :
    Down Port(2)    :1/0/7-8
  ChGr:22   Mode:Static
    CH Status      :Up         Elapsed Time:160.11:45:10
    Multi Speed    :Off        Load Balance:src-dst-port
    Max Active Port:2 (no-link-down mode)
    Max Detach Port:7
    MAC address: 0012.e2ac.8305      VLAN ID:250
    Port(3)        :1/0/9,14-15
    Up Port(2)      :1/0/9,14
    Down Port(1)    :1/0/15
    Standby Port(1) :1/0/15
>

```

## Display items in Example 1

Table 17-1: Display items for link aggregation information

Item	Meaning	Displayed information
channel-group Counts	Number of channel groups to be displayed	Number of channel groups
ChGr	Channel group number	Channel group number
Mode	Link aggregation mode	LACP: LACP link aggregation mode
		Static: Static link aggregation mode
		-: Link aggregation mode is not set.
CH Status	Channel group status	Up: Data packets can be sent and received.
		Down: Data packets cannot be sent or received.
		Disabled: Link aggregation is disabled.
Elapsed Time	Time the channel group has been up	hh:mm:ss (when the elapsed time is less than 24 hours) ddd.hh:mm:ss (when the elapsed time exceeds 24 hours) Over 1000 days (when the elapsed time is more than 1000 days) - is displayed when the channel group status is not Up.
Max Active Port	Maximum number of ports used by link aggregation	1 to 8 (8 is displayed as the initial value.) - is displayed when link aggregation mode is not set.
	Standby link mode	Standby link link-down mode
		(link-down mode): Link-down mode
		(no-link-down mode): Link-not-down mode
Max Detach Port	Restriction on the number of detached ports	0 or 7 (7 is displayed as the initial value.) - is displayed when link aggregation mode is not set.
Load Balance	Distribution method	dst-ip: The load is distributed according to the destination IP addresses. dst-mac: The load is distributed according to the destination MAC addresses. dst-port: The load is distributed according to the destination port numbers. src-dst-ip: The load is distributed according to the source and destination IP addresses. src-dst-mac: The load is distributed according to the source and destination MAC addresses. src-dst-port: The load is distributed according to the source and destination port numbers. src-ip: The load is distributed according to the source IP addresses. src-mac: The load is distributed according to the source MAC addresses. src-port: The load is distributed according to the source port numbers.
Multi Speed	Mixed-speed mode	Off: Does not permit a channel group to consist of ports with different transmission speeds. On: Permits a channel group to consist of ports with different transmission speeds.
Description	Supplementary explanation regarding the channel group	This item is not displayed if a supplementary explanation has not been set in the configuration.

Item	Meaning	Displayed information
MAC Address	Channel group's MAC address	The MAC address of the group. One of the MAC addresses of the ports that belong to the group is used.
VLAN ID	VLAN ID to which the channel group belongs	VLAN ID
Periodic Time	Sending interval for LACPDU	This item is displayed only when LACP mode is enabled.
		Short: The sending interval is 1 second.
		Long: The sending interval is 30 seconds.
Actor information	Information about the actor system	Information about the actor system. This item is displayed only when LACP mode is enabled.
System Priority	System priority	Priority of the LACP system ID 1 to 65535 can be specified as the priority value (1 indicates the highest priority).
MAC	MAC address	The MAC address of the LACP system ID
KEY	Group key	Group key This value is the same as the channel group number.
Partner information	Information about the partner system	Information about the partner system. This item is displayed only when LACP mode is enabled. - is displayed if the partner system is not defined for LACP.
System Priority	System priority	Priority of the LACP system ID 0 to 65535 can be specified as the priority value (0 indicates the highest priority).
MAC	MAC address	MAC address
KEY	Group key	0 to 65535
Port(n)	Port information of a channel group	n: Number of ports Switch number/NIF number/port number of a channel group
Up Port(n)	Information about ports that can be used for sending or receiving in a channel group	n: Number of ports that can be used for sending and receiving Switch number/NIF number/port number of a port that can be used for sending or receiving
Down Port(n)	Information about ports that cannot be used for sending or receiving in a channel group	n: Number of ports that cannot be used for sending and receiving Switch number/NIF number/port number of a port that cannot be used for sending or receiving (For a standby link in link-not-down mode, sending is impossible but receiving is possible.)
Standby Port(n)	Information about standby ports in a channel group	n: Number of standby ports Switch number/NIF number/port number of a port in a standby state

## Example 2

The following shows an example of displaying summary information about link aggregation.

*Figure 17-3: Example of displaying summary information about link aggregation*

```
>show channel-group summary
Date 20XX/07/14 12:00:00 UTC
CH Status          :ChGr ID
Up(2)              :1,22
```

```

Down(1)           :11
Disabled(1)       :21
>

```

## Display items in Example 2

Table 17-2: Display items for the summary information about link aggregation

Item	Meaning	Displayed information
Up(n)	Information about link aggregations in Up status	n: Number of link aggregations IDs of link aggregations in Up status
Down(n)	Information about link aggregations in Down status	n: Number of link aggregations IDs of link aggregations in Down status
Disabled(n)	Information about link aggregations in Disabled status	n: Number of link aggregations IDs of link aggregations in Disabled status

## Example 3

The following shows an example of displaying detailed information about link aggregation.

Figure 17-4: Example of displaying detailed information about link aggregation

```

>show channel-group detail
Date 20XX/12/10 12:00:00 UTC
channel-group Counts:4
ChGr:1    Mode:LACP
  CH Status      :Up          Elapsed Time:10:10:39
  Multi Speed    :Off         Load Balance:src-dst-port
  Max Active Port:8
  Max Detach Port:7
  Description    : All 100M Full-Duplex
  MAC address: 0012.e2ac.8301   VLAN ID:
  Periodic Timer:Short
  Actor information: System Priority:1    MAC: 0012.e212.ff02
                        KEY:1
  Partner information: System Priority:10000 MAC: 0012.e2f0.69be
                        KEY:10
  Port Counts:6      Up Port Counts:2
  Port:1/0/1    Status:Up    Reason: Partner-
                        Speed :100M Duplex:Full LACP Activity:Active
                        Actor Priority:128    Partner Priority:100
  Port:1/0/2    Status:Up    Reason:-
                        Speed :100M Duplex:Full LACP Activity:Active
                        Actor Priority:128    Partner Priority:100
  Port:1/0/3    Status:Down  Reason:LACPDU Expired
                        Speed :100M Duplex:Full LACP Activity:Active
                        Actor Priority:128    Partner Priority:100
  Port:1/0/10   Status:Down  Reason:LACPDU Expired
                        Speed: 100M Duplex:Full LACP Activity:Active
                        Actor Priority:128    Partner Priority:100
  Port:1/0/12   Status:Down  Reason:Partner Aggregation Individual
                        Speed: 100M Duplex:Full LACP Activity:Active
                        Actor Priority:128    Partner Priority:100
  Port:1/0/13   Status:Down  Reason:Synchronization OUT_OF_SYNC
                        Speed: 100M Duplex:Full LACP Activity:Active
                        Actor Priority:128    Partner Priority:100
ChGr:11    Mode:LACP
  CH Status      :Down        Elapsed Time:-
  Multi Speed    :Off         Load Balance:src-dst-port
  Max Active Port:8
  Max Detach Port:7
  MAC address: 0012.e2ac.8302   VLAN ID:30-35,40
  Periodic Timer:Long
  Actor information: System Priority:1    MAC: 0012.e212.ff02
                        KEY:11

```

```

Partner information: System Priority:10000 MAC: 0012.e2f0.69bd
                      KEY:20
Port Counts:3        Up Port Counts:0
Port:1/0/4   Status:Down Reason:Port Down
              Speed :100M Duplex:Full LACP Activity:Active
              Actor Priority:128 Partner Priority:100
Port:1/0/5   Status:Down Reason:Partner Key Unmatch
              Speed :100M Duplex:Full LACP Activity:Active
              Actor Priority:128 Partner Priority:100
              Unmatched Partner Key:201
Port:1/0/6   Status:Down Reason:Partner System ID Unmatch
              Speed :100M Duplex:Full LACP Activity:Active
              Actor Priority:128 Partner Priority:1
              Unmatched System ID: Priority:5000 MAC:0012.e2f0.69ba
ChGr:21 Mode:Static
CH Status :Disabled Elapsed Time:-
Multi Speed :Off Load Balance:src-dst-port
Max Active Port:8
Max Detach Port:7
MAC address: 0012.e2ac.8304 VLAN ID:200
Port Counts:2        Up Port Counts:0
Port:1/0/7   Status:Down Reason:CH Disabled
              Speed :100M Duplex:Full Priority:128
Port:1/0/8   Status:Down Reason:CH Disabled
              Speed :100M Duplex:Full Priority:128
ChGr:22 Mode:Static
CH Status :Up Elapsed Time:160.11:45:10
Multi Speed :Off Load Balance:src-dst-port
Max Active Port:2 (no-link-down mode)
Max Detach Port:7
MAC address: 0012.e2ac.8305 VLAN ID:250
Port Counts:3        Up Port Counts:2
Port:1/0/9   Status:Up Reason:-
              Speed :100M Duplex:Full Priority:0
Port:1/0/14  Status:Up Reason:-
              Speed :100M Duplex:Full Priority:0
Port:1/0/15  Status:Down Reason:Standby
              Speed :100M Duplex:Full Priority:0
>

```

The following shows an example of displaying the detailed link aggregation information for a specific channel group number.

*Figure 17-5:* Example of displaying the detailed link aggregation information for a specific channel group number

```

>show channel-group 10-21 detail
Date 20XX/12/10 12:00:00 UTC
channel-group Counts:2
ChGr:11 Mode:LACP
CH Status :Down Elapsed Time:-
Multi Speed :Off Load Balance:src-dst-port
Max Active Port:8
Max Detach Port:7
MAC address: 0012.e2ac.8302 VLAN ID:30-35,40
Periodic Timer:Long
Actor information: System Priority:1 MAC: 0012.e212.ff02
                  KEY:11
Partner information: System Priority:10000 MAC: 0012.e2f0.69bd
                  KEY:20
Port Counts:3        Up Port Counts:0
Port:1/0/4   Status:Down Reason:Port Down
              Speed :100M Duplex:Full LACP Activity:Active
              Actor Priority:128 Partner Priority:100
Port:1/0/5   Status:Down Reason:Partner Key Unmatch
              Speed :100M Duplex:Full LACP Activity:Active
              Actor Priority:128 Partner Priority:100
              Unmatched Partner Key:201

```

```

Port:1/0/6   Status:Down Reason:Partner System ID Unmatch
              Speed :100M Duplex:Full LACP Activity:Active
              Actor Priority:128 Partner Priority:1
              Unmatched System ID: Priority:5000 MAC:0012.e2f0.69ba
ChGr:21      Mode:Static
CH Status    :Disabled Elapsed Time:-
Multi speed  :Off Load Balance:src-dst-port
Max Active Port:8
Max Detach Port:7
MAC address: 0012.e2ac.8304 VLAN ID:200
Port Counts:2 Up Port Counts:0
Port:1/0/7   Status:Down Reason:CH Disabled
              Speed :100M Duplex:Full Priority:128
Port:1/0/8   Status:Down Reason:CH Disabled
              Speed :100M Duplex:Full Priority:128
>

```

### Display items in Example 3

Table 17-3: Display items for the detailed link aggregation information

Item	Meaning	Displayed information
channel-group Counts	Number of channel groups to be displayed	Number of channel groups
ChGr	Channel group number	Channel group number
Mode	Link aggregation mode	LACP: LACP link aggregation mode
		Static: Static link aggregation mode
		-: Link aggregation mode is not set.
CH Status	Channel group status	Up: Data packets can be sent and received.
		Down: Data packets cannot be sent or received. (For a standby link in link-not-down mode, sending is impossible but receiving is possible.)
		Disabled: Link aggregation is disabled.
Elapsed Time	Time the channel group has been up	hh:mm:ss (when the elapsed time is less than 24 hours) ddd.hh:mm:ss (when the elapsed time exceeds 24 hours) Over 1000 days (when the elapsed time is more than 1000 days) - is displayed when the channel group status is not Up.
Max Active Port	Maximum number of ports used by link aggregation	1 to 8 (8 is displayed as the initial value.) - is displayed when link aggregation mode is not set.
	Standby link mode	Standby link link-down mode
		(link-down mode): Link-down mode
		(no-link-down mode): Link-not-down mode
Max Detach Port	Restriction on the number of detached ports	0 or 7 (7 is displayed as the initial value.) - is displayed when link aggregation mode is not set.

Item	Meaning	Displayed information
Load Balance	Distribution method	<p>dst-ip: The load is distributed according to the destination IP addresses.</p> <p>dst-mac: The load is distributed according to the destination MAC addresses.</p> <p>dst-port: The load is distributed according to the destination port numbers.</p> <p>src-dst-ip: The load is distributed according to the source and destination IP addresses.</p> <p>src-dst-mac: The load is distributed according to the source and destination MAC addresses.</p> <p>src-dst-port: The load is distributed according to the source and destination port numbers.</p> <p>src-ip: The load is distributed according to the source IP addresses.</p> <p>src-mac: The load is distributed according to the source MAC addresses.</p> <p>src-port: The load is distributed according to the source port numbers.</p>
Multi Speed	Mixed-speed mode	<p>off: Does not permit a channel group to consist of ports with different transmission speeds.</p> <p>on: Permits a channel group to consist of ports with different transmission speeds.</p>
Description	Supplementary explanation regarding the channel group	This item is not displayed if a supplementary explanation has not been set in the configuration.
MAC Address	Channel group's MAC address	The MAC address of the group. One of the MAC addresses of the ports that belong to the group is used.
VLAN ID	VLAN ID to which the channel group belongs	VLAN ID
Periodic Time	Sending interval for LACPDU	This item is displayed only when LACP mode is enabled.
		Short: The sending interval is 1 second.
		Long: The sending interval is 30 seconds.
Actor information	Information about the actor system	Information about the actor system. This item is displayed only when LACP mode is enabled.
System Priority	System priority	Priority of the LACP system ID 1 to 65535 can be specified as the priority value (1 indicates the highest priority).
MAC	MAC address	The MAC address of the LACP system ID
KEY	Group key	Group key This value is the same as the channel group number.
Partner information	Information about the partner system	Information about the partner system. This item is displayed only when LACP mode is enabled. - is displayed if the partner system is not defined for LACP.
System Priority	System priority	Priority of the LACP system ID 0 to 65535 can be specified as the priority value (0 indicates the highest priority).
MAC	MAC address	MAC address
KEY	Group key	0 to 65535
Port Counts	Number of ports that have been set up	Number of ports that have been set up by configuration

Item	Meaning	Displayed information
Up Port Counts	Number of ports that can be used for sending and receiving data packets	Number of ports that can be used for sending and receiving data
Port	Port information	Switch number/NIF number/port number
Status	Status of the port aggregation	Up: Data packets can be sent and received.
		Down: Data packets cannot be sent or received.
Reason	Cause of the failure	-: Status is Up.
		Standby: The ports in the local channel group are in Standby status.
		CH Disabled: The status of the local channel group is Disable.
		Port Down: The ports in the local channel group are in Down status.
		Port Speed Unmatch: Ports in the local channel group do not use the same line speed.
		Duplex Half: The ports in the local channel group are in half duplex mode.
		Port Selecting: A port aggregation condition check is being conducted on the local channel group.
		Waiting Partner Synchronization: The port aggregation condition check on the local channel group has finished, and the channel group is waiting for the connected port to synchronize.
		LACPDU Expired: The valid time period of the LACPDU received from the connected port expired.
		Partner System ID Unmatch: The partner system ID received from the connected port is different from the partner system ID of the group. The unmatched partner system ID is also displayed.
		Partner Key Unmatch: The key received from the connected port is different from the partner key of the group. The unmatched partner key is also displayed.
		Partner Aggregation Individual: The connected port cannot be a member of link aggregation.
		Partner Synchronization OUT_OF_SYNC: The port connected to the local port cannot synchronize with the local port.
		Port Moved: A port moved in the channel group.
		Operation of Detach Port Limit: The maximum number of ports that can be detached is limited.
Speed	Line speed	10M: 10 Mbit/s
		100M: 100 Mbit/s
		1G: 1 Gbit/s
		10G: 10 Gbit/s
		40G: 40 Gbit/s [AX3800S]

Item	Meaning	Displayed information
Duplex	Duplex mode	Full: Full duplex
		Half: Half duplex
LACP Activity	LACP activation method	This item is displayed only when LACP mode is enabled.
		Active: LACPDU are always sent.
		Passive: An LACPDU is sent after an LACPDU is received.
Actor Priority	Priority of the actor system port	0 to 65535 can be specified as the priority value (0 indicates the highest priority). This item is displayed only when LACP mode is enabled.
Partner Priority	Priority of the partner system port	0 to 65535 can be specified as the priority value (0 indicates the highest priority). This item is displayed only when LACP mode is enabled.
Priority	Priority of the actor system port	0 to 65535 can be specified as the priority value (0 indicates the highest priority). This item is displayed only in static mode.
Unmatched Partner Key	Partner key that is unmatched	1 to 65535 This item is displayed only when Status is Down and Reason is Unmatched Partner Key.
Unmatched Partner System ID	Partner system ID that is unmatched	This item is displayed only when Status is Down and Reason is Unmatched Partner System ID.
Priority	System priority	0 to 65535 can be specified as the priority value (0 indicates the highest priority).
MAC Address	MAC address	The MAC address for the system ID

## Impact on communication

None

## Response messages

Table 17-4: List of response messages for the show channel-group command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Manager.	Communication with the L2Manager program failed. Re-execute the command. If this message is output frequently, execute the restart vlan command to restart the L2Manager program.
Connection failed to Link Aggregation.	Communication with the link aggregation program failed. Re-execute the command. If this message is output frequently, execute the restart link-aggregation command to restart the link aggregation program.
Specified channel-group is not configured.	The channel group has not been configured. Check the configuration.

## Notes

If the standby link functionality is used in link-down mode, as many ports as the maximum number of available ports are used for operation and the rest of the ports become standby ports. For `Reason` (cause of failure), `Standby` is displayed regardless of the status of the standby ports. If the status of a port changes to `Standby` due to a failure, a message to that effect is not logged, but the port will operate as a standby port after the failure is corrected.

---

## show channel-group statistics

---

Displays link aggregation statistics.

### Syntax

```
show channel-group statistics [lacp] [<channel group list>]
```

### Input mode

User mode and administrator mode

### Parameters

lacp

Displays for each port the statistics for sent and received LACPDUs in link aggregation. Information is not displayed if static link aggregation mode is enabled or link aggregation mode has not been set.

<channel group list>

Displays link aggregation statistics for the channel group numbers specified in list format. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Statistics for all link aggregations are displayed.

Operation when all parameters are omitted:

Statistics for sent and received data packets (for each port) in all link aggregations are displayed.

### Operation when a stack configuration is used

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

```
remote command {<switch no.> | all} show channel-group statistics
```

### Example 1

The following shows examples of displaying statistics on sent and received data packets for link aggregation (by port).

*Figure 17-6:* Example of displaying statistics on sent and received data packets for link aggregation (standalone configuration)

```
>show channel-group statistics
Date 20XX/07/14 12:00:00 UTC
channel-group counts:4
ChGr:1 (Up)
  Total:      Octets      Tx:          12760301  Rx:          9046110
             Frames      Tx:           71483  Rx:           64377
             Discards    Tx:             96  Rx:             9
  Port:0/1    Octets      Tx:         12745991  Rx:         9033008
             Frames      Tx:           71432  Rx:           64332
             Discards    Tx:             95  Rx:             5
  Port:0/2    Octets      Tx:          14310  Rx:         13102
             Frames      Tx:             51  Rx:             45
             Discards    Tx:              1  Rx:              4
  Port:0/3    Octets      Tx:              0  Rx:              0
             Frames      Tx:              0  Rx:              0
             Discards    Tx:              0  Rx:              0
  Port:0/10   Octets      Tx:              0  Rx:              0
             Frames      Tx:              0  Rx:              0
             Discards    Tx:              0  Rx:              0
```

## 17. Link Aggregation

```

Port:0/12  Octets  Tx:          0 Rx:          0
           Frames  Tx:          0 Rx:          0
           Discards Tx:          0 Rx:          0
Port:0/13  Octets  Tx:          0 Rx:          0
           Frames  Tx:          0 Rx:          0
           Discards Tx:          0 Rx:          0
ChGr:11 (Up)
Total:     Octets  Tx:      2031141 Rx:      1643359
           Frames  Tx:       3344 Rx:       2353
           Discards Tx:        14 Rx:        25
Port:0/4   Octets  Tx:      2008831 Rx:      1623147
           Frames  Tx:       3312 Rx:       2332
           Discards Tx:        10 Rx:        22
Port:0/5   Octets  Tx:       22310 Rx:       20212
           Frames  Tx:         32 Rx:         21
           Discards Tx:          4 Rx:          3
Port:0/6   Octets  Tx:          0 Rx:          0
           Frames  Tx:          0 Rx:          0
           Discards Tx:          0 Rx:          0
ChGr:21 (Down)
Total:     Octets  Tx:          0 Rx:          0
           Frames  Tx:          0 Rx:          0
           Discards Tx:          0 Rx:          0
Port:0/7   Octets  Tx:          0 Rx:          0
           Frames  Tx:          0 Rx:          0
           Discards Tx:          0 Rx:          0
Port:0/8   Octets  Tx:          0 Rx:          0
           Frames  Tx:          0 Rx:          0
           Discards Tx:          0 Rx:          0
ChGr:22 (Up)
Total:     Octets  Tx:      5971370 Rx:      5205702
           Frames  Tx:      11133 Rx:      10286
           Discards Tx:         12 Rx:         32
Port:0/9   Octets  Tx:      4023121 Rx:      3403392
           Frames  Tx:       7211 Rx:       6884
           Discards Tx:          0 Rx:          0
Port:0/14  Octets  Tx:      1948249 Rx:      1802310
           Frames  Tx:       3922 Rx:       3402
           Discards Tx:         12 Rx:         32
Port:0/15  Octets  Tx:          0 Rx:          0
           Frames  Tx:          0 Rx:          0
           Discards Tx:          0 Rx:          0
>

```

*Figure 17-7: Example of displaying statistics on sent and received data packets for link aggregation (stack configuration)*

```

>remote command all show channel-group statistics
Switch 1 (Master)
-----
Date 20XX/07/14 12:00:00 UTC
channel-group counts:4
ChGr:1 (Up)
Total:     Octets  Tx:      12760301 Rx:      9046110
           Frames  Tx:       71483 Rx:       64377
           Discards Tx:         96 Rx:         9
Port:0/1   Octets  Tx:      12745991 Rx:      9033008
           Frames  Tx:       71432 Rx:       64332
           Discards Tx:         95 Rx:         5
Port:0/2   Octets  Tx:       14310 Rx:       13102
           Frames  Tx:         51 Rx:         45
           Discards Tx:          1 Rx:          4
Port:0/3   Octets  Tx:          0 Rx:          0
           Frames  Tx:          0 Rx:          0
           Discards Tx:          0 Rx:          0
Port:0/10  Octets  Tx:          0 Rx:          0
           Frames  Tx:          0 Rx:          0
           Discards Tx:          0 Rx:          0

```

```

Port:0/12  Octets  Tx:          0  Rx:          0
           Frames  Tx:          0  Rx:          0
           Discards Tx:          0  Rx:          0
Port:0/13  Octets  Tx:          0  Rx:          0
           Frames  Tx:          0  Rx:          0
           Discards Tx:          0  Rx:          0
ChGr:11 (Up)
Total:     Octets  Tx:      2031141  Rx:      1643359
           Frames  Tx:       3344  Rx:       2353
           Discards Tx:        14  Rx:        25
Port:0/4   Octets  Tx:      2008831  Rx:      1623147
           Frames  Tx:       3312  Rx:       2332
           Discards Tx:        10  Rx:        22
Port:0/5   Octets  Tx:       22310  Rx:       20212
           Frames  Tx:         32  Rx:         21
           Discards Tx:          4  Rx:          3
Port:0/6   Octets  Tx:          0  Rx:          0
           Frames  Tx:          0  Rx:          0
           Discards Tx:          0  Rx:          0
ChGr:21 (Down)
Total:     Octets  Tx:          0  Rx:          0
           Frames  Tx:          0  Rx:          0
           Discards Tx:          0  Rx:          0
Port:0/7   Octets  Tx:          0  Rx:          0
           Frames  Tx:          0  Rx:          0
           Discards Tx:          0  Rx:          0
Port:0/8   Octets  Tx:          0  Rx:          0
           Frames  Tx:          0  Rx:          0
           Discards Tx:          0  Rx:          0
ChGr:22 (Up)
Total:     Octets  Tx:      5971370  Rx:      5205702
           Frames  Tx:      11133  Rx:      10286
           Discards Tx:         12  Rx:         32
Port:0/9   Octets  Tx:      4023121  Rx:      3403392
           Frames  Tx:       7211  Rx:       6884
           Discards Tx:          0  Rx:          0
Port:0/14  Octets  Tx:      1948249  Rx:      1802310
           Frames  Tx:       3922  Rx:       3402
           Discards Tx:         12  Rx:         32
Port:0/15  Octets  Tx:          0  Rx:          0
           Frames  Tx:          0  Rx:          0
           Discards Tx:          0  Rx:          0

Switch 2 (Backup)
-----
Date 20XX/07/14 12:00:00 UTC
channel-group counts:1
ChGr:1
Total:     Octets  Tx:      12760301  Rx:      9046110
           Frames  Tx:       71483  Rx:       64377
           Discards Tx:         96  Rx:         9
Port:0/1   Octets  Tx:      12745991  Rx:      9033008
           Frames  Tx:       71432  Rx:       64332
           Discards Tx:         95  Rx:         5
Port:0/2   Octets  Tx:       14310  Rx:       13102
           Frames  Tx:         51  Rx:         45
           Discards Tx:          1  Rx:          4
Port:0/3   Octets  Tx:          0  Rx:          0
           Frames  Tx:          0  Rx:          0
           Discards Tx:          0  Rx:          0
>

```

The following shows examples of displaying statistics on sent and received data packets for a specific channel group number (by port).

*Figure 17-8: Example of displaying statistics on sent and received data packets for a specific channel group number (standalone configuration)*

```
>show channel-group statistics 22-30
Date 20XX/07/14 12:00:00 UTC
channel-group counts:1
ChGr:22 (Up)
  Total:      Octets   Tx:      5971370 Rx:      5205702
              Frames   Tx:      11133  Rx:      10286
              Discards Tx:      12    Rx:      32
  Port:0/9    Octets   Tx:      4023121 Rx:      3403392
              Frames   Tx:      7211  Rx:      6884
              Discards Tx:      0    Rx:      0
  Port:0/14   Octets   Tx:      1948249 Rx:      1802310
              Frames   Tx:      3922  Rx:      3402
              Discards Tx:      12    Rx:      32
  Port:0/15   Octets   Tx:      0      Rx:      0
              Frames   Tx:      0      Rx:      0
              Discards Tx:      0      Rx:      0
>
```

*Figure 17-9: Example of displaying statistics on sent and received data packets for a specific channel group number (stack configuration)*

```
>remote command all show channel-group statistics 22-30
Switch 1 (Master)
-----
Date 20XX/07/14 12:00:00 UTC
channel-group counts:1
ChGr:22 (Up)
  Total:      Octets   Tx:      5971370 Rx:      5205702
              Frames   Tx:      11133  Rx:      10286
              Discards Tx:      12    Rx:      32
  Port:0/9    Octets   Tx:      4023121 Rx:      3403392
              Frames   Tx:      7211  Rx:      6884
              Discards Tx:      0    Rx:      0
  Port:0/14   Octets   Tx:      1948249 Rx:      1802310
              Frames   Tx:      3922  Rx:      3402
              Discards Tx:      12    Rx:      32
  Port:0/15   Octets   Tx:      0      Rx:      0
              Frames   Tx:      0      Rx:      0
              Discards Tx:      0      Rx:      0

Switch 2 (Backup)
-----
Date 20XX/07/14 12:00:00 UTC
channel-group counts:1
ChGr:22
  Total:      Octets   Tx:      5971370 Rx:      5205702
              Frames   Tx:      11133  Rx:      10286
              Discards Tx:      12    Rx:      32
  Port:0/9    Octets   Tx:      4023121 Rx:      3403392
              Frames   Tx:      7211  Rx:      6884
              Discards Tx:      0    Rx:      0
  Port:0/14   Octets   Tx:      1948249 Rx:      1802310
              Frames   Tx:      3922  Rx:      3402
              Discards Tx:      12    Rx:      32
  Port:0/15   Octets   Tx:      0      Rx:      0
              Frames   Tx:      0      Rx:      0
              Discards Tx:      0      Rx:      0
>
```

## Display items in Example 1

*Table 17-5:* Display items for the statistics for sent and received data packets related to link aggregation

Item	Meaning	Displayed information
Switch	Switch number. The switch status is displayed in parentheses.	Switch number Master: Configures a stack (Master) Backup: Configures a stack (Backup)
channel-group counts	Number of channel groups to be displayed	Number of channel groups per switch
ChGr	Channel group number. The status of the channel group is displayed enclosed in parentheses.	Channel group number Up: Data packets can be sent and received. Down: Data packets cannot be sent or received. Disabled: Link aggregation is disabled. The status of the channel group is displayed only for the master switch.
Total	Total statistics	Statistics are displayed for each channel group.
Port	Port information	Statistics are displayed for each port. NIF number/port number
Octets	Data size of the sent and received data packets	Tx: Total number of sent bytes Rx: Total number of received bytes This item is displayed in octets starting with the MAC header and ending with the FCS.
Frames	Number of sent and received data frames	Tx: Total number of sent data frames Rx: Total number of received data frames
Discards	Number of discarded sent and received data frames	Tx: Total number of discarded sent data frames Rx: Total number of discarded received data frames For details about the items used for counting the number of discarded frames, see <i>Table 16-35: Statistical items used for calculating the number of discarded packets.</i>

## Example 2

The following shows examples of displaying statistics for sent and received LACPDU in link aggregation.

*Figure 17-10:* Displaying statistics for sent and received LACPDUs in link aggregation (standalone configuration)

```
>show channel-group statistics lacp
Date 20XX/07/14 12:00:00 UTC
channel-group counts:2
ChGr:1      Port Counts:6
  Port:0/1
    TxLACPDUs      : 50454011  RxLACPDUs      : 16507650
    TxMarkerResponsePDUs: 10    RxMarkerPDUs: 10
    RxDiscards      : 8
  Port:0/2
    TxLACPDUs      : 50454011  RxLACPDUs      : 16507650
    TxMarkerResponsePDUs: 10    RxMarkerPDUs: 10
    RxDiscards      : 8
  Port:0/3
    TxLACPDUs      : 100    RxLACPDUs      : 100
    TxMarkerResponsePDUs: 10    RxMarkerPDUs: 10
    RxDiscards      : 8
  Port:0/10
    TxLACPDUs      : 100    RxLACPDUs      : 100
    TxMarkerResponsePDUs: 10    RxMarkerPDUs: 10
```

```

    RxDiscards      :      8
Port:0/12
    TxLACPDUs       :    100  RxLACPDUs      :    100
    TxMarkerResponsePDUs:    10  RxMarkerPDUs:     10
    RxDiscards      :      8
Port:0/13
    TxLACPDUs       :    100  RxLACPDUs      :    100
    TxMarkerResponsePDUs:    10  RxMarkerPDUs:     10
    RxDiscards      :      8
ChGr:11    Port counts:3
Port:0/4
    TxLACPDUs       :    100  RxLACPDUs      :    100
    TxMarkerResponsePDUs:    10  RxMarkerPDUs:     10
    RxDiscards      :      8
Port:0/5
    TxLACPDUs       :    100  RxLACPDUs      :    100
    TxMarkerResponsePDUs:    10  RxMarkerPDUs:     10
    RxDiscards      :      8
Port:0/6
    TxLACPDUs       :    100  RxLACPDUs      :    100
    TxMarkerResponsePDUs:    10  RxMarkerPDUs:     10
    RxDiscards      :      8
>

```

*Figure 17-11: Displaying statistics for sent and received LACPDUs in link aggregation (stack configuration)*

```

>show channel-group statistics lacp
Date 20XX/07/14 12:00:00 UTC
channel-group counts:2
ChGr:1    Port Counts:6
Port:1/0/1
    TxLACPDUs       : 50454011  RxLACPDUs      : 16507650
    TxMarkerResponsePDUs:    10  RxMarkerPDUs:     10
    RxDiscards      :      8
Port:1/0/2
    TxLACPDUs       : 50454011  RxLACPDUs      : 16507650
    TxMarkerResponsePDUs:    10  RxMarkerPDUs:     10
    RxDiscards      :      8
Port:1/0/3
    TxLACPDUs       :    100  RxLACPDUs      :    100
    TxMarkerResponsePDUs:    10  RxMarkerPDUs:     10
    RxDiscards      :      8
Port:1/0/10
    TxLACPDUs       :    100  RxLACPDUs      :    100
    TxMarkerResponsePDUs:    10  RxMarkerPDUs:     10
    RxDiscards      :      8
Port:1/0/12
    TxLACPDUs       :    100  RxLACPDUs      :    100
    TxMarkerResponsePDUs:    10  RxMarkerPDUs:     10
    RxDiscards      :      8
Port:1/0/13
    TxLACPDUs       :    100  RxLACPDUs      :    100
    TxMarkerResponsePDUs:    10  RxMarkerPDUs:     10
    RxDiscards      :      8
ChGr:11    Port counts:3
Port:1/0/4
    TxLACPDUs       :    100  RxLACPDUs      :    100
    TxMarkerResponsePDUs:    10  RxMarkerPDUs:     10
    RxDiscards      :      8
Port:1/0/5
    TxLACPDUs       :    100  RxLACPDUs      :    100
    TxMarkerResponsePDUs:    10  RxMarkerPDUs:     10
    RxDiscards      :      8
Port:1/0/6
    TxLACPDUs       :    100  RxLACPDUs      :    100
    TxMarkerResponsePDUs:    10  RxMarkerPDUs:     10
    RxDiscards      :      8

```

&gt;

The following shows examples of displaying statistics for sent and received LACPDUs for a specific channel group number.

*Figure 17-12: Displaying statistics for sent and received LACPDUs for a specific channel group number (standalone configuration)*

```
>show channel-group statistics lacp 10-20
Date 20XX/07/14 12:00:00 UTC
channel-group counts:1
ChGr:11    Port counts:3
  Port:0/4
    TxLACPDUs      :      100  RxLACPDUs      :      100
    TxMarkerResponsePDUs:      10  RxMarkerPDUs:      10
    RxDiscards     :          8
  Port:0/5
    TxLACPDUs      :      100  RxLACPDUs      :      100
    TxMarkerResponsePDUs:      10  RxMarkerPDUs:      10
    RxDiscards     :          8
  Port:0/6
    TxLACPDUs      :      100  RxLACPDUs      :      100
    TxMarkerResponsePDUs:      10  RxMarkerPDUs:      10
    RxDiscards     :          8
>
```

*Figure 17-13: Displaying statistics for sent and received LACPDUs for a specific channel group number (stack configuration)*

```
>show channel-group statistics lacp 10-20
Date 20XX/07/14 12:00:00 UTC
channel-group counts:1
ChGr:11    Port counts:3
  Port:1/0/4
    TxLACPDUs      :      100  RxLACPDUs      :      100
    TxMarkerResponsePDUs:      10  RxMarkerPDUs:      10
    RxDiscards     :          8
  Port:1/0/5
    TxLACPDUs      :      100  RxLACPDUs      :      100
    TxMarkerResponsePDUs:      10  RxMarkerPDUs:      10
    RxDiscards     :          8
  Port:1/0/6
    TxLACPDUs      :      100  RxLACPDUs      :      100
    TxMarkerResponsePDUs:      10  RxMarkerPDUs:      10
    RxDiscards     :          8
>
```

## Display items in Example 2

*Table 17-6: Display items for the statistics for sent and received LACPDUs in link aggregation*

Item	Meaning	Displayed information
channel-group counts	Number of channel groups to be displayed	Number of channel groups
ChGr	Channel group number	Channel group number
Port Counts	Number of ports to be displayed	Number of ports
Port	Port information	Switch number/NIF number/port number
TxLACPDUs	Number of sent LACPDUs	--
RxLACPDUs	Number of received LACPDUs	--
Tx MarkerResponsePDUs	Number of sent marker response PDUs	--
RxMarkerPDUs	Number of received marker PDUs	--

Item	Meaning	Displayed information
RxDiscards	Number of discarded received PDUs	Number of LACPDUs discarded due to parameter errors

### Impact on communication

None

### Response messages

*Table 17-7:* List of response messages for the show channel-group statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Manager.	Communication with the network interface management program failed. Re-execute the command. If this message is output frequently, execute the <code>restart vlan</code> command to restart the network interface management program.
Connection failed to Link Aggregation.	Communication with the link aggregation program failed. Re-execute the command. If this message is output frequently, execute the <code>restart link-aggregation</code> command to restart the link aggregation program.
Specified channel-group is not configured.	The channel group has not been configured. Check the configuration.

### Notes

- Statistics are cleared when the device starts up or when the following commands are executed:  
 Statistics for sent and received data packets: `clear counters`  
 Information about sent and received LACPs: `clear channel-group statistics lacp`
- The statistics for the sent and received data packets displayed by this command are the sum of the statistics on the Ethernet lines for each channel group. To clear the statistics for sent and received data packets, use a command that clears Ethernet lines. The following are related commands:  
 Related commands: `show interfaces`, `clear counters`

---

## clear channel-group statistics lacp

---

Clears the statistics for sent and received LACPDUs in link aggregation.

### Syntax

```
clear channel-group statistics lacp [<channel group list>]
```

### Input mode

User mode and administrator mode

### Parameters

<channel group list>

Specifies a list of the channel group numbers for which you want to clear LACPDU statistics. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

The statistics on the sent and received LACPDUs for all channel groups are cleared.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 17-14:* Clearing statistics on sent and received LACPDUs for link aggregation

```
>clear channel-group statistics lacp
>
```

*Figure 17-15:* Clearing statistics on sent and received LACPDUs for a specific channel group

```
>clear channel-group statistics lacp 11
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 17-8:* List of response messages for the clear channel-group statistics lacp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Link Aggregation.	Communication with the link aggregation program failed. Re-execute the command. If this message is output frequently, execute the <code>restart link-aggregation</code> command to restart the link aggregation program.
Specified channel-group is not configured.	The channel group has not been configured. Check the configuration.

### Notes

- This command clears only LACPDU statistics. It cannot clear the statistics for the data packets for each channel group. Also see *Notes* for the `show channel-group statistics` command.

- Even if statistics are cleared, the value for the MIB information obtained by using SNMP is not cleared.
- If deletion or addition is performed in the configuration, the relevant LACPDU statistical items are cleared to zero.

---

## restart link-aggregation

---

Restarts the link aggregation program.

### Syntax

```
restart link-aggregation [-f] [core-file]
```

### Input mode

User mode and administrator mode

### Parameters

**-f**

Restarts the link aggregation program without outputting any confirmation messages.

Operation when this parameter is omitted:

A confirmation message is displayed.

**core-file**

Outputs the link aggregation program's core file (`LAd.core`) when restarting the link aggregation program.

Operation when this parameter is omitted:

A core file is not output.

Operation when all parameters are omitted:

After a restart confirmation message is output, the link aggregation program is restarted.

### Operation when a stack configuration is used

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

```
remote command {<switch no.> | all} restart link-aggregation [-f] [core-file]
```

### Example

*Figure 17-16: Restarting the link aggregation program*

```
> restart link-aggregation
Link Aggregation restart OK? (y/n):y
>
```

*Figure 17-17: Restarting the link aggregation program (-f parameter specified)*

```
> restart link-aggregation -f
>
```

### Impact on communication

Ports for which link aggregation is enabled temporarily become unable to send or receive data.

### Response messages

*Table 17-9: List of response messages for the restart link-aggregation command*

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

Message	Description
Link Aggregation doesn't seem to be running.	Because the link aggregation program has not started, the command could not be executed. The link aggregation program starts only when link aggregations are set up. If no link aggregations are set up, this message is output. If this message is output when link aggregations have been set up, wait until the link aggregation program is restarted, and then re-execute the command.

## Notes

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

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

File name: `LAd.core`

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

---

## dump protocols link-aggregation

---

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

### Syntax

```
dump protocols link-aggregation
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

```
remote command {<switch no.> | all} dump protocols link-aggregation
```

### Example

*Figure 17-18: Obtaining a link aggregation dump*

```
> dump protocols link-aggregation
>
```

### Impact on communication

None

### Response messages

*Table 17-10: List of response messages for the dump protocols link-aggregation command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Link-Aggregation.	Communication with the link aggregation program failed. Re-execute the command. If this message is output frequently, execute the <code>restart link-aggregation</code> command to restart the link aggregation program.
Specified channel-group is not configured.	The channel group 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/LA/`

File name: `LAd_dump.gz`

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



## Chapter

---

# 18. MAC Address Table

---

```
show mac-address-table  
clear mac-address-table
```

---

## show mac-address-table

---

Displays information about the MAC address table.

### Syntax

```
show mac-address-table [ <mac> ] [ vlan <vlan id list> ] [ port <port list> ]
                        [channel-group-number <channel group list>]
                        [{ static | dynamic | snoop | dot1x | wa | macauth }]
show mac-address-table learning-counter [ port <port list> ]
                        [channel-group-number <channel group list>]
show mac-address-table learning-counter vlan [<vlan id list>]
```

### Input mode

User mode and administrator mode

### Parameters

<mac>

Displays the information in the MAC address table for the specified MAC address.

vlan <vlan id list>

Displays the information in the MAC address table for the VLAN IDs specified in list format.

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

[port <port list>] [channel-group-number <channel group list>]

Displays the information in the MAC address table for the specified ports or the specified channel groups. If you specify both a list of ports and a list of channel groups, the information in the MAC address table for either the specified ports or channel groups is displayed.

port <port list>

Displays the information in the MAC address table for the ports specified in list format. The MAC address table entries that include at least one of the ports specified in the list are displayed. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Displays the information in the MAC address table for the channel groups specified in list format for the specified link aggregation. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Even if the command is executed with this parameter set, information about the MAC address table is displayed in port-list format.

Operation when this parameter is omitted:

The information in the MAC address table for all ports and channel groups is displayed.

{ static | dynamic | snoop | dot1x | wa | macauth }

Displays the information in the MAC address table that was registered under the specified condition.

static

Displays the information in the MAC address table registered by the `mac-address-table static` configuration command.

dynamic

Displays the information in the MAC address table registered dynamically through MAC address learning.

snoop

Displays the information in the MAC address table registered by using the IGMP snooping or MLD snooping functionality.

dot1x

Displays the information in the MAC address table registered by using the IEEE 802.1X.

wa

Displays the information in the MAC address table registered by using the Web authentication functionality.

macauth

Displays the information in the MAC address table registered by using the MAC-based authentication functionality.

learning-counter

Displays the number of learned addresses in the MAC address table for each port.

learning-counter vlan [*<vlan id list>*]

Displays the number of learned addresses in the MAC address table for each VLAN. For details about how to specify *<vlan id list>*, see *Specifiable values for parameters*. If *<vlan id list>* is omitted, the number of learned addresses for all VLANs is displayed.

Operation when each parameter is omitted:

This command can display only information relevant to the condition applied by a parameter that has been set. If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information conforming to the conditions will be displayed.

Operation when all parameters are omitted:

Displays all information about the MAC address table.

## Operation when a stack configuration is used

Automatically synchronizes the information of the MAC address table of the master switch with that of other member switches.

When specifying the `learning-counter` parameter for member switches other than the master switch, use the `remote command` command.

remote command {*<switch no.>* | all} show mac-address-table learning-counter [ port *<port list>* ] [channel-group-number *<channel group list>*]

## Example 1

Figure 18-1: Displaying all information in a MAC address table

```
> show mac-address-table
Date 20XX/10/29 11:33:50 UTC
MAC address      VLAN    Type      Port-list
0012.e280.5cbf    3       Static    1/0/5
0012.e205.0558    1       Dynamic   1/0/23
0012.e28e.0602    1       Dynamic   1/0/23
0012.e2a8.250c    1       Dynamic   1/0/23
0012.e205.0642    100     Dynamic   1/0/2-3,10
0012.e205.0643    103     Dynamic   1/0/4,7
0012.e205.0643    104     Dynamic   1/0/4,7
>
```

## Display items in Example 1

Table 18-1: Display items for the information in the MAC address table

Item	Meaning	Displayed information
MAC address	MAC address	--
VLAN	VLAN ID	--
Type	Type of MAC address table entry	Dynamic: Entry registered dynamically Snoop: Entry registered by using the IGP snooping or MLD snooping functionality Static: Entry registered statically or registered via IEEE 802.1X Dot1x: Entry registered via IEEE 802.1X Wa: Entry registered via Web authentication Macauth: Entry registered via MAC-based authentication
Port-list	Port (<Switch number>/<NIF number>/<Port number>)	Note that items other than ports are displayed in the following cases: Drop: Drop (discarded MAC address) specified -: Entry whose type is Snoop and that is being deleted from the MAC address table

## Example 2

Figure 18-2: Displaying the status of learning in the MAC address table (for each port)

```
>show mac-address-table learning-counter port 1/0/1-10
Date 20XX/09/21 20:00:57 UTC
Port counts:10
Port      Count
1/0/1      3
1/0/2     1000
1/0/3       0
1/0/4      50
1/0/5      45
1/0/6       0
1/0/7      22
1/0/8       0
1/0/9       0
1/0/10      0
>
```

Figure 18-3: Displaying the status of learning in the MAC address table (for each VLAN)

```
>show mac-address-table learning-counter vlan
Date 20XX/12/10 20:00:57 UTC
VLAN counts:4
ID        Count  Maximum
1          3       -
100       1000    1000
200        0       -
4094       90     100
>
```

## Display items in Example 2

Table 18-2: Display items for the status of learning in the MAC address table

Item	Meaning	Displayed information
VLAN counts	Number of target VLANs	--
Port counts	Number of target ports	--

Item	Meaning	Displayed information
Port	Port ( <i>&lt;Switch number&gt;/&lt;NIF number&gt;/&lt;Port number&gt;</i> )	--
ID	VLAN ID	VLAN ID
Count	Number of learnt entries in the current MAC address table	--
Maximum	Maximum number of addresses that can be learned in the MAC address table	0: Learning is prohibited. -: The maximum number of addresses that can be learned is not set.

## Impact on communication

None

## Response messages

*Table 18-3:* List of response messages for the show mac-address-table command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Mac Manager.	Communication with the L2 Mac Manager program failed. Re-execute the command. If this message is output frequently, execute the <code>restart vlan</code> command to restart the L2 Mac Manager program.
Connection failed to L2 Manager.	Communication with the L2Manager program failed. Re-execute the command. If this message is output frequently, execute the <code>restart vlan</code> command to restart the L2Manager program.
Connection failed to Snoopd.	Communication with the IGMP or MLD snooping program failed. Re-execute the command. If this message is output frequently, execute the <code>restart snooping</code> command to restart the IGMP or MLD snooping program.
No mac-address-table entry.	There is no information in the MAC address table. Make sure the specified parameter is correct, and then try again.
No operational Port.	There are no available ports. Make sure the specified parameter is correct, and then try again.
Specified VLAN is not configured.	The specified VLAN has not been configured. Make sure the specified parameter is correct, and then try again.

## Notes

If the `learning-counter` parameter is specified when a stack is configured, the port information of all the member switches are displayed, but the learning address count of the ports of other member switches will be 0.

---

## clear mac-address-table

---

Clears the information in the MAC address table registered dynamically through MAC address learning.

### Syntax

```
clear mac-address-table [ vlan <vlan id list> ]
                        [ port <port list> ] [channel-group-number <channel group list>] [-f]
```

### Input mode

User mode and administrator mode

### Parameters

vlan <vlan id list>

Specifies a list of VLAN IDs for which you want to clear the MAC address table entries.

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

[port <port list>] [channel-group-number <channel group list>]

Specifies a list of ports or channel groups for which you want to clear the information in the MAC address table. If you specify both a list of ports and a list of channel groups, the information in the MAC address table for either the specified ports or channel groups will be cleared.

port <port list>

Specifies a list of ports for which you want to clear the information in the MAC address table that have been learned. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Specifies a list of channel groups in the link aggregation for which you want to clear the information in the MAC address table that have been learned. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

-f

Clears information in the MAC address table without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

Operation when each parameter is omitted:

This command can clear only the information in the MAC address table that meets the conditions specified by the parameter. If no parameter is specified, information in the MAC address table is cleared without being limited by any conditions. If multiple parameters are specified, the information in the MAC address table conforming to the conditions will be cleared.

Operation when all parameters are omitted:

All dynamically learned MAC address table information is cleared.

### Operation when a stack configuration is used

Automatically synchronizes the information of the MAC address table of the master switch with that of other member switches.

## Example

*Figure 18-4:* Example of clearing MAC address table information when the VLAN ID and port is specified

```
>clear mac-address-table vlan 90 port 1/0/9
mac-address-table clear OK? (y/n): y
>
```

*Figure 18-5:* Example of clearing MAC address table without displaying a confirmation message

```
>clear mac-address-table vlan 100-200 -f
>
```

## Display items

None

## Impact on communication

For L2 forwarding, frames are flooded until learning is completed again. Execute this command at a time when flooding will have a minimal impact.

For L3 forwarding, communication might temporarily be interrupted.

## Response messages

*Table 18-4:* List of response messages for the clear mac-address-table command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Can't execute.	The command could not be executed. Re-execute the command.
Command is accepted, but it takes time for setting to hardware.	The command was executed, but it takes time for the settings to be applied to hardware (you do not need to re-execute the command).
Connection failed to L2 Manager.	Communication with the L2Manager program failed. Re-execute the command. If this message is output frequently, execute the restart vlan command to restart the L2Manager program.
No operational Port.	There are no available ports. Make sure the specified parameter is correct, and then try again.
Specified VLAN is not configured.	The specified VLAN has not been configured. Make sure the specified parameter is correct, and then try again.

## Notes

None



## Chapter

---

# 19. VLAN

---

```
show vlan
show vlan mac-vlan
restart vlan
dump protocols vlan
```

---

## show vlan

---

Displays various VLAN statuses and the status of accommodated lines.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

{ summary | detail | list | configuration }

summary

Displays the VLAN summary information.

detail

Displays detailed information about VLANs.

list

Displays VLAN information with the information for one VLAN being displayed on one line.

configuration

Displays information about the ports assigned in a VLAN.

Operation when this parameter is omitted:

VLAN information is displayed.

<vlan id list>

Displays the VLAN information for the VLAN IDs specified in list format.

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

Operation when this parameter is omitted:

Information about all VLANs is displayed.

[port <port list>] [channel-group-number <channel group list>]

Specify a list of ports or channel groups for which you want to display VLAN information. If you specify both a list of ports and a list of channel groups, the VLAN information for either the specified ports or channel groups is displayed.

port <port list>

Specify a list of ports for which you want to display VLAN information. The information about all VLANs that contain one or more specified ports is displayed. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Specify a list of channel groups for which you want to display VLAN information. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

All VLAN information, not limited by port or channel group, is displayed.

Operation when all parameters are omitted:

All VLAN information is displayed.

### Operation when a stack configuration is used

The command can display information only for the master switch.

### Example 1

The following shows an example of displaying summary information about all configured VLANs.

*Figure 19-1: Example of displaying VLAN summary information*

```
> show vlan summary
Date 20XX/09/21 14:15:00 UTC
Total(18)           :1,3-5,8,10-20,100,2000
Port based(10)      :1,3-5,8,10,12,14,16,18
Protocol based(8)    :11,13,15,17,19-20,100,2000
MAC based(0)        :
>
```

### Display items in Example 1

*Table 19-1: Display items of VLAN summary*

Item	Meaning	Displayed information
Total( <i>n</i> )	Applicable VLAN information	<i>n</i> : Number of applicable VLANs VLAN ID list
Port based( <i>n</i> )	Port VLAN information	<i>n</i> : Number of applicable VLANs VLAN ID list
Protocol based( <i>n</i> )	Protocol VLAN information	<i>n</i> : Number of applicable VLANs VLAN ID list
MAC based( <i>n</i> )	MAC VLAN information	<i>n</i> : Number of applicable VLANs VLAN ID list

### Example 2

The following shows an example of displaying the statuses of all configured VLANs and the status of accommodated ports.

*Figure 19-2: Example of displaying VLAN information*

```
> show vlan
Date 20XX/01/26 17:01:40 UTC
VLAN counts:4
VLAN ID:1      Type:Port based      Status:Up
  Learning:On      Tag-Translation:
  BPDU Forwarding:  EAPOL Forwarding:
  Router Interface Name:VLAN0001
  IP Address:10.215.201.1/24
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0001
  Spanning Tree:PVST+(802.1D)
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:           GSRP VLAN group:  L3:
  IGMP snooping:     MLD snooping:
  Untagged(18)      :1/0/1-4,13-26
VLAN ID:3      Type:Port based      Status:Up
  Learning:On      Tag-Translation:On
  BPDU Forwarding:  EAPOL Forwarding:
  Router Interface Name:VLAN0003
  IP Address:10.215.196.1/23
```

```

3ffe:501:811:ff08::5/64
Source MAC address: 0012.e212.ad1e(System)
Description:VLAN0003
Spanning Tree:Single(802.1D)
AXRP RING ID:      AXRP VLAN group:
GSRP ID:          GSRP VLAN group:   L3:
IGMP snooping:    MLD snooping:
Untagged(8)       :1/0/5-12
Tagged(2)         :1/0/25-26
Tag-Trans(2)      :1/0/25-26
VLAN ID:120      Type:Protocol based  Status:Up
Protocol VLAN Information Name:ipv6
EtherType:08dd  LLC: Snap-EtherType:
Learning:On      Tag-Translation:On
BPDU Forwarding:  EAPOL Forwarding:
Router Interface Name:VLAN0120
IP Address:
Source MAC address: 0012.e212.ad1e(System)
Description:VLAN0120
Spanning Tree:
AXRP RING ID:      AXRP VLAN group:
GSRP ID:          GSRP VLAN group:   L3:
IGMP snooping:    MLD snooping:
Untagged(3)       :1/0/5,7,9
Tagged(2)         :1/0/25-26
Tag-Trans(2)      :1/0/25-26
VLAN ID:1340     Type:Mac based       Status:Up
Learning:On      Tag-Translation:On
BPDU Forwarding:  EAPOL Forwarding:
Router Interface Name:VLAN1340
IP Address:10.215.202.1/24
Source MAC address: 0012.e2de.053c(VLAN)
Description:VLAN1340
Spanning Tree:
AXRP RING ID:      AXRP VLAN group:
GSRP ID:          GSRP VLAN group:   L3:
IGMP snooping:    MLD snooping:
Untagged(6)       :1/0/13-18
Tagged(2)         :1/0/25-26
Tag-Trans(2)      :1/0/25-26
>

```

*Figure 19-3: Example of displaying VLAN information in list format (when the Ring Protocol is used)*

```

> show vlan 3,5
Date 20XX/11/15 17:01:40 UTC
VLAN counts:2
VLAN ID:3      Type:Port based      Status:Up
Learning:On    Tag-Translation:
BPDU Forwarding:  EAPOL Forwarding:
Router Interface Name:VLAN0003
IP Address:
Source MAC address: 0012.e212.ad1e(System)
Description:VLAN0003
Spanning Tree:
AXRP RING ID:1      AXRP VLAN group:2
AXRP RING ID:100    AXRP VLAN group:1
AXRP RING ID:500    AXRP VLAN group:2
AXRP RING ID:1000   AXRP VLAN group:2
AXRP Virtual-Link-VLAN
GSRP ID:        GSRP VLAN group:   L3:
IGMP snooping:  MLD snooping:
Untagged(8)     :1/0/5-12
Tagged(8)       :1/0/25-32
VLAN ID:5      Type:Port based      Status:Up
Learning:On    Tag-Translation:
BPDU Forwarding:  EAPOL Forwarding:

```

```

Router Interface Name:VLAN0005
IP Address:
Source MAC address: 0012.e212.ad1e(System)
Description:VLAN0005
Spanning Tree:
AXRP RING ID:100    AXRP VLAN group:Control-VLAN
GSRP ID:          GSRP VLAN group:    L3:
IGMP snooping:    MLD snooping:
Tagged(2)         :1/0/25-26
>

```

*Figure 19-4: Example of displaying VLAN information for a specific port*

```

> show vlan port 1/0/5
Date 20XX/12/10 12:00:00 UTC
VLAN counts:2
VLAN ID:3      Type:Port based      Status:Up
  Learning:On      Tag-Translation:On
  BPDU Forwarding:      EAPOL Forwarding:
  Router Interface Name:VLAN0003
  VRF:3
  IP Address:10.215.196.1/23
                3ffe:501:811:ff08::5/64
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0003
  Spanning Tree:Single(802.1D)
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:          GSRP VLAN group:    L3:
  IGMP snooping:    MLD snooping:
  Untagged(8)      :1/0/5-12
  Tagged(2)        :1/0/25-26
  Tag-Trans(2)     :1/0/25-26
VLAN ID:120    Type:Protocol based  Status:Up
  Protocol VLAN Information Name:ipv6
  EtherType:08dd  LLC:  Snap-EtherType:
  Learning:On      Tag-Translation:On
  BPDU Forwarding:      EAPOL Forwarding:
  Router Interface Name:VLAN0120
  IP Address:
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0120
  Spanning Tree:
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:          GSRP VLAN group:    L3:
  IGMP snooping:    MLD snooping:
  Untagged(3)      :1/0/5,7,9
  Tagged(2)        :1/0/25-26
  Tag-Trans(2)     :1/0/25-26
>

```

## Display items in Example 2

*Table 19-2: Basic display items for VLANs*

Item	Meaning	Displayed information
VLAN counts	Number of applicable VLANs	--
VLAN tunneling enabled	VLAN tunneling information	VLAN tunneling is enabled. (This item is displayed only when VLAN tunneling is used.)
VLAN ID	VLAN information	VLAN ID
Type	VLAN type	Port based: Port VLAN Protocol based: Protocol VLAN Mac based: MAC VLAN

Item	Meaning	Displayed information
Status	VLAN status	Up: Indicates Up status. Down: Indicates Down status. Disabled: The VLAN is disabled.
Protocol VLAN Information	Protocol VLAN information	This item is displayed only for a protocol VLAN.
Name	Name	--
EtherType	EtherType value of Ethernet V2 frames	Displayed as a four-digit hexadecimal number
LLC	LLC value of 802.3 frames	Displayed as a four-digit hexadecimal number
Snap-EtherType	EtherType value of 802.3 SNAP frames	Displayed as a four-digit hexadecimal number
Learning	Status of MAC address learning	On: MAC address learning is enabled. Off: MAC address learning is disabled.
Tag-Translation	Tag translation	Blank: No setting On: Tag translation is being used.
BPDU Forwarding	BPDU forwarding	Blank: No setting On: BPDU forwarding functionality is being used.
EAPOL Forwarding	EAPOL forwarding	Blank: The setting for this item does not exist. On: EAPOL forwarding functionality is being used.
Router Interface Name	Interface name	Displays the name of the interface assigned to the VLAN.
VRF [OS-L3SA]	VRF ID	This item is displayed only when VRF is assigned to the VLAN interface.
IP Address	IP address (/mask)	Blank: No setting
Source MAC address	Source MAC address used during Layer 3 communication	System: The MAC address for the device is used. VLAN: The MAC address of each VLAN is used.
Description	Description	The character string set for the VLAN name is displayed. VLANxxx is displayed if this item is not set. (xxx: VLAN ID)
Spanning Tree	Spanning Tree Protocol being used	Single (802.1D): IEEE 802.1D is used for the entire Switch. Single (802.1w): IEEE 802.1w is used for the entire Switch. PVST+ (802.1D): IEEE 802.1D is used for the VLAN. PVST+ (802.1w): IEEE 802.1w is used for the VLAN. MSTP (802.1s): Multiple Spanning Tree is used.
AXRP RING ID	Ring Protocol ring ID	Blank: No setting (Information about a maximum of 24 IDs is displayed.)
AXRP VLAN group	ID of the VLAN group using the Ring Protocol functionality or the control VLAN	Blank: No setting 1 or 2: ID of the assigned VLAN group Control-VLAN: The control VLAN is assigned.
AXRP Virtual-Link-VLAN	The VLAN is a virtual link VLAN for the Ring Protocol functionality.	This item is displayed when the VLAN is assigned to the virtual link VLAN for the Ring Protocol functionality.
GSRP ID	GSRP ID	Blank: The setting for this item does not exist. Alternatively, no VLAN group is assigned when GSRP VLAN group-only control functionality is used.

Item	Meaning	Displayed information
GSRP VLAN group	GSRP VLAN group ID	Blank: The setting for this item does not exist. Alternatively, no VLAN group is assigned when GSRP VLAN group-only control functionality is used. --: No VLAN groups have been assigned.
L3	Layer 3 redundancy switching functionality	Blank: The setting for this item does not exist. Alternatively, no VLAN group is assigned when GSRP VLAN group-only control functionality is used. On: The Layer 3 redundancy switching functionality is being used.
Virtual MAC Address	Virtual MAC address	The virtual MAC address used for the Layer 3 redundancy switching functionality is displayed.
IGMP Snooping	Setting status of IGMP snooping	Blank: No setting On: IGMP snooping is being used.
MLD Snooping	Setting status of MLD snooping	Blank: No setting On: MLD snooping is being used.
Untagged( <i>n</i> )	Untagged port	<i>n</i> : Number of applicable ports Port list
Tagged( <i>n</i> )	Tagged port	<i>n</i> : Number of applicable ports Port list
Tag-Trans( <i>n</i> )	Port for which tag translation is set	<i>n</i> : Number of applicable ports Port list

### Example 3

The following shows an example of displaying VLAN detailed information when a VLAN ID is specified.

*Figure 19-5: Example of displaying VLAN detailed information for a specific VLAN ID*

```
> show vlan 3,1000-1500 detail
Date 20XX/12/10 12:00:00 UTC
VLAN counts:2
VLAN ID:3      Type:Port based      Status:Up
  Learning:On      Tag-Translation:On
  BPDU Forwarding:      EAPOL Forwarding:
  Router Interface Name:VLAN0003
  VRF:3
  IP Address:10.215.196.1/23
                  ee80::220:afff:fed7:8f0a/64
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0003
  Spanning Tree:Single(802.1D)
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:      L3:
  IGMP snooping:      MLD snooping:
  Port Information
    1/0/5      Up      Forwarding      Untagged
    1/0/6      Up      Blocking(STP)      Untagged
    1/0/7      Up      Forwarding      Untagged
    1/0/8      Up      Forwarding      Untagged
    1/0/9      Up      Forwarding      Untagged
    1/0/10     Up      Forwarding      Untagged
    1/0/11     Up      Forwarding      Untagged
    1/0/12     Up      Forwarding      Untagged
    1/0/25(CH:9) Up      Forwarding      Tagged      Tag-Translation:103
    1/0/26(CH:9) Up      Blocking(CH)      Tagged      Tag-Translation:103
VLAN ID:1340 Type:Mac based      Status:Up
  Learning:On      Tag-Translation:On
```

```

BPDU Forwarding:      EAPOL Forwarding:
Router Interface Name:VLAN1340
IP Address:10.215.202.1/24
Source MAC address: 0012.e2de.053c (VLAN)
Description:VLAN1340
Spanning Tree:
AXRP RING ID:         AXRP VLAN group:
GSRP ID:             GSRP VLAN group:   L3:
IGMP snooping:       MLD snooping:
Port Information
1/0/13               Up    Forwarding    Untagged
1/0/14               Up    Forwarding    Untagged
1/0/15               Up    Forwarding    Untagged
1/0/16               Up    Forwarding    Untagged
1/0/17               Up    Forwarding    Untagged
1/0/18               Up    Forwarding    Untagged
1/0/25 (CH:9)        Up    Forwarding    Tagged    Tag-Translation:104
1/0/26 (CH:9)        Up    Blocking (CH) Tagged    Tag-Translation:104
>

```

### Display items in Example 3

Table 19-3: Display items of detailed VLAN information

Item	Meaning	Displayed information
VLAN counts	Number of applicable VLANs	--
VLAN tunneling enabled	VLAN tunneling information	VLAN tunneling is enabled. (This item is displayed only when VLAN tunneling is used.)
VLAN ID	VLAN information	VLAN ID
Type	VLAN type	Port based: Port VLAN Protocol based: Protocol VLAN Mac based: MAC VLAN
Status	VLAN status	Up: Indicates Up status. Down: Indicates Down status. Disabled: The VLAN is disabled.
Protocol VLAN Information	Protocol VLAN information	This item is displayed only for a protocol VLAN.
Name	Name	--
EtherType	EtherType value of Ethernet V2 frames	Displayed as a four-digit hexadecimal number
LLC	LLC value of 802.3 frames	Displayed as a four-digit hexadecimal number
Snap-EtherType	EtherType value of 802.3 SNAP frames	Displayed as a four-digit hexadecimal number
Learning	Status of MAC address learning	On: MAC address learning is enabled. Off: MAC address learning is disabled.
Tag-Translation	Tag translation	Blank: No setting On: Tag translation is being used.
BPDU Forwarding	BPDU forwarding	Blank: No setting On: BPDU forwarding functionality is being used.
EAPOL Forwarding	EAPOL forwarding	Blank: No setting On: EAPOL forwarding functionality is being used.

Item	Meaning	Displayed information
Router Interface Name	Router interface name	Displays the name of the interface assigned to the VLAN.
VRF [OS-L3SA]	VRF ID	This item is displayed only when VRF is assigned to the VLAN interface.
IP Address	IP address (/mask)	Blank: No setting
Source MAC address	Source MAC address used during Layer 3 communication	System: The MAC address for the device is used. VLAN: The MAC address of each VLAN is used.
Description	Description	The character string set for the VLAN name is displayed. <code>VLANxxxx</code> is displayed if this item is not set. (xxxx: VLAN ID)
Spanning Tree	Spanning Tree Protocol being used	Single (802.1D): IEEE 802.1D is used for the entire Switch. Single (802.1w): IEEE 802.1w is used for the entire Switch. PVST+ (802.1D): IEEE 802.1D is used for the VLAN. PVST+ (802.1w): IEEE 802.1w is used for the VLAN. MSTP (802.1s): Multiple Spanning Tree is used.
AXRP RING ID	Ring Protocol ring ID	Blank: No setting (Information about a maximum of 24 IDs is displayed.)
AXRP VLAN group	ID of the VLAN group using the Ring Protocol functionality or the control VLAN	Blank: No setting 1 or 2: ID of the assigned VLAN group Control-VLAN: The control VLAN is assigned.
AXRP Virtual-Link-VLAN	The VLAN is a virtual link VLAN for the Ring Protocol functionality.	This item is displayed when the VLAN is assigned to the virtual link VLAN for the Ring Protocol functionality.
GSRP ID	GSRP ID	Blank: The setting for this item does not exist. Alternatively, no VLAN group is assigned when GSRP VLAN group-only control functionality is used.
GSRP VLAN group	GSRP VLAN group ID	Blank: The setting for this item does not exist. Alternatively, no VLAN group is assigned when GSRP VLAN group-only control functionality is used. --: No VLAN groups have been assigned.
L3	Layer 3 redundancy switching functionality	Blank: The setting for this item does not exist. Alternatively, no VLAN group is assigned when GSRP VLAN group-only control functionality is used. On: The Layer 3 redundancy switching functionality is being used.
Virtual MAC Address	Virtual MAC address	The virtual MAC address used for the Layer 3 redundancy switching functionality is displayed.
IGMP Snooping	Setting status of IGMP snooping	Blank: No setting On: IGMP snooping is being used.
MLD Snooping	Setting status of MLD snooping	Blank: No setting On: MLD snooping is being used.
Port Information	Port information ( <code>&lt;Switch number&gt;/&lt;NIF number&gt;/&lt;Port number&gt;</code> )	No Port information is displayed if there is no port information for the VLAN.
CH	Channel group number	1 to 32 (1 to 52 if a stack configuration is used). This item is not displayed for the ports that do not belong to the channel group.

Item	Meaning	Displayed information
<line-status>	Port state	Up: Indicates that the port status is Up. Down: Indicates that the port status is Down.
<data-forwarding-status>	Data forwarding status	Forwarding: Data is being forwarded. Blocking: Data forwarding is blocked. (VLAN): The VLAN is disabled. (CH): Data forwarding has been stopped by link aggregation. (STP): Data forwarding has been stopped by STP. (GSRP): Data forwarding has been stopped by GSRP. (dot1x): Data forwarding has been stopped by IEEE 802.1X. (CNF): Data forwarding has been stopped because a duplicated protocol value was encountered in the protocol VLAN configuration (data is being forwarded for the protocol values that have successfully been set). (AXRP): Forwarding has been suspended by the Ring Protocol. (ULR): Data transfers have been stopped by ULR. -: Down status
Tag	Tag setting status	Untagged: Untagged port Tagged: Tagged port
Tag-Translation	ID subject to tag translation	1 to 4094

## Example 4

The following shows an example of displaying VLAN information in list format.

*Figure 19-6: Example of displaying VLAN information in list format*

```
> show vlan list
Date 20XX/11/15 17:01:40 UTC
VLAN counts:4
ID   Status   Fwd/Up /Cfg Name           Type   Protocol   Ext.   IP
 1 Up       16/ 18/ 18 VLAN0001      Port   STP PVST+:1D - - - 4
 3 Up       9/ 10/ 10 VLAN0003      Port   STP Single:1D - - T 4/6
120 Up       4/ 5/ 5 VLAN0120        Proto - - - -
1340 Disable 0/ 8/ 8 VLAN1340        Mac - - - -
AXRP (C:Control-VLAN)
GSRP GSRP ID:VLAN Group ID(M:Master/B:Backup)
S:IGMP/MLD snooping T:Tag Translation
4:IPv4 address configured 6:IPv6 address configured
>
```

*Figure 19-7: Example of displaying VLAN information in list format (when GSRP is used)*

```
> show vlan list
Date 20XX/11/15 17:01:40 UTC
VLAN counts:2
ID   Status   Fwd/Up /Cfg Name           Type   Protocol   Ext.   IP
 1 Up       2/ 2/ 2 VLAN0001      Port   GSRP 100: 1(M) - - - 4
 3 Down    0/ 2/ 6 VLAN0003      Port   GSRP 100: 2(B) - - T 4/6
AXRP (C:Control-VLAN)
GSRP GSRP ID:VLAN Group ID(M:Master/B:Backup)
S:IGMP/MLD snooping T:Tag Translation
4:IPv4 address configured 6:IPv6 address configured
>
```

*Figure 19-8: Example of displaying VLAN information in list format (when the Ring Protocol is used)*

```
> show vlan list
Date 20XX/11/15 17:01:40 UTC
```

```

VLAN counts:4
ID   Status  Fwd/Up  /Cfg Name           Type  Protocol      Ext.  IP
   1  Up       1/   2/   2 VLAN0001        Port  AXRP (-)      - - - -
   5  Up       2/   2/   2 VLAN0005        Port  AXRP (C)      - - - -
  10  Up       1/   2/   2 VLAN0010        Port  AXRP (-)      - - - -
  20  Up       3/   4/   4 VLAN0020        Port  AXRP (-)      - - - -
      AXRP (C:Control-VLAN)
      GSRP GSRP ID:VLAN Group ID(M:Master/B:Backup)
      S:IGMP/MLD snooping T:Tag Translation
      4:IPv4 address configured  6:IPv6 address configured
>

```

**Figure 19-9:** Example of displaying VLAN information in list format (when both the Ring Protocol and STP are used)

```

> show vlan list
Date 20XX/11/15 17:01:40 UTC
VLAN counts:4
ID   Status  Fwd/Up  /Cfg Name           Type  Protocol      Ext.  IP
   1  Up       3/   3/   3 VLAN0001        Port  STP Single:1D - - - -
   5  Up       2/   2/   2 VLAN0005        Port  AXRP (C)      - - - -
  10  Up       3/   3/   3 VLAN0010        Port  STP PVST+:1D - - - -
  20  Up       3/   3/   3 VLAN0020        Port  STP Single:1D - - - -
      AXRP (C:Control-VLAN)
      GSRP GSRP ID:VLAN Group ID(M:Master/B:Backup)
      S:IGMP/MLD snooping T:Tag Translation
      4:IPv4 address configured  6:IPv6 address configured
>

```

## Display items in Example 4

**Table 19-4:** Display items for VLAN information in list format

Item	Meaning	Displayed information
VLAN counts	Number of applicable VLANs	--
VLAN tunneling enabled	VLAN tunneling information	VLAN tunneling is enabled. (This item is displayed only when VLAN tunneling is used.)
ID	VLAN ID	VLAN ID
Status	VLAN status	Up: Indicates Up status. Down: Indicates Down status. Disabled: The VLAN is disabled.
Fwd	Number of ports in Forward status	The number of ports belonging to the VLAN that are in Forward status
Up	Number of ports in Up status	The number of ports belonging to the VLAN that are in Up status
Cfg	Number of VLAN ports	The number of ports belonging to the VLAN
Name	VLAN name	The character string set for the VLAN name is displayed. VLANxxxx is displayed if this item is not set. (xxxx: VLAN ID)
Type	VLAN type	Port: Port VLAN Proto: Protocol VLAN Mac: MAC VLAN

Item	Meaning	Displayed information
Protocol	STP information, GSRP information, Ring Protocol information	<p>For STP:  STP &lt;type&gt; : &lt;protocol&gt;  &lt;type&gt;: Single, PVST+, or MSTP  &lt;protocol&gt;: 802.1D, 802.1w, or 802.1s</p> <p>For GSRP:  GSRP &lt;GSRP ID&gt; : &lt;VLAN Group ID&gt; (M/B) (If no VLAN group is assigned when GSRP VLAN group-only control functionality is enabled, a hyphen (-) is displayed, and the subsequent items are not displayed.)  - &lt;GSRP ID&gt;: GSRP group ID  - &lt;VLAN Group ID&gt;: VLAN group ID (If no VLAN group is assigned, a hyphen (-) is displayed.)  - (M) : Master  - (B) : Backup</p> <p>For the Ring Protocol:  AXRP  (C) : Indicates that the control VLAN is assigned. ( (-) is displayed if the control VLAN is not assigned. Note, however, that (-) is not displayed for a VLAN that co-exists with other protocols.)  If nothing is specified, a hyphen (-) is displayed.</p>
Ext.	Extended functionality information	S: Indicates that IGMP snooping or MLD snooping is set. T: Indicates that tag translation is set. -: Indicates that the relevant functionality is not set.
IP	IP address setting information	4: Indicates that an IPv4 address is set. 6: Indicates that an IPv6 address is set. 4/6: Indicates that both an IPv4 address and an IPv6 address are set. -: Indicates that an IP address is not set for the VLAN.

## Example 5

The following shows an example of displaying VLAN information in list format.

*Figure 19-10: Example of displaying information about all ports set for the VLAN*

```
> show vlan configuration
Date 20XX/11/15 14:15:00
VLAN counts: 3
ID   Name                Status  Ports
  1  DefaultVLAN          Up      1/0/1-10,1/0/12,1/0/14,1/0/16,1/0/20-23,1/0/30,
                                     1/0/32,1/0/34,1/0/36,1/0/49-50
 200 Global IP Netw..   Down    1/0/11,1/0/15,1/0/31
4000 VLAN4000          Disable 1/0/2-10,1/0/12,1/0/31
>
```

## Display items in Example 5

*Table 19-5: Display items for the information about all ports set for the VLAN*

Item	Meaning	Displayed information
VLAN counts	Number of applicable VLANs	--
ID	VLAN ID	VLAN ID
Name	VLAN name	VLAN name (a maximum of 14 characters from the beginning)
Status	VLAN status	Up: Indicates Up status. Down: Indicates Down status. Disabled: The VLAN is disabled.

Item	Meaning	Displayed information
Ports	Port information	Switch number/NIF number/port number If no port exists, a hyphen (-) is displayed.

## Impact on communication

None

## Response messages

Table 19-6: List of response messages for the show vlan command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to GSRP.	Communication with the GSRP program failed. Re-execute the command. If the failure occurs frequently, use the <code>restart gsrp</code> command to restart the GSRP program.
Connection failed to L2 Manager.	Communication with the L2Manager program failed. Re-execute the command. If this message is output frequently, execute the <code>restart vlan</code> command to restart the L2Manager program.
Connection failed to Link Aggregation.	Communication with the link aggregation program failed. Re-execute the command. If this message is output frequently, execute the <code>restart link-aggregation</code> command to restart the link aggregation program.
Connection failed to Ring Protocol.	Communication with the Ring Protocol program failed. Re-execute the command. If this message is output frequently, execute the <code>restart axrp</code> command to restart the Ring Protocol program.
Connection failed to Snoospd.	Communication with the IGMP or MLD snooping program failed. Re-execute the command. If this message is output frequently, execute the <code>restart snooping</code> command to restart the IGMP or MLD snooping program.
Connection failed to Spanning Tree.	Communication with the Spanning Tree program failed. Re-execute the command. If this message is output frequently, execute the <code>restart spanning-tree</code> command to restart the Spanning Tree program.
No operational Port.	There are no available ports. Make sure the specified parameter is correct, and then try again.
No operational VLAN.	There are no available VLANs. Make sure the specified parameter is correct, and then try again.

## Notes

1. Be careful if the `switchport mac` configuration command with the `vlan` parameter specified has not been executed for MAC ports that are placed in dynamic VLAN mode for Web authentication or MAC authentication. If this happens, the `show vlan` command displays the VLAN information for the terminals that have been authorized and unauthorized in all MAC VLANs that are set.
2. When a port receives frames from a terminal that has not yet been authorized, the port learns the MAC address of the terminal. However, the port can send frames only to authorized

terminals.

---

## show vlan mac-vlan

---

Displays the MAC addresses registered for MAC VLANs.

### Syntax

```
show vlan mac-vlan [<vlan id list>] [{ static | dynamic }]
show vlan mac-vlan <mac>
```

### Input mode

User mode and administrator mode

### Parameters

<vlan id list>

Displays the MAC VLAN information for the VLAN IDs specified in list format.

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

{ static | dynamic }

static

Displays the MAC address information registered in the configuration.

The MAC address information disabled by hardware conditions is also displayed.

dynamic

Displays the MAC address information registered by Layer 2 authentication. The MAC address information disabled because it is also registered by configuration is also displayed.

<mac>

Displays VLANs for which the specified MAC address is registered.

The MAC address information disabled because it is registered by both configuration and Layer 2 authentication is also displayed.

The MAC address information in the configuration disabled by hardware conditions is also displayed.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following shows an example of displaying information related to MAC VLANs from the information for all configured VLANs.

*Figure 19-11: Example of displaying MAC VLAN information*

```
> show vlan mac-vlan
Date 20XX/09/21 14:15:00 UTC
VLAN counts:2      Total MAC Counts:5
VLAN ID:100      MAC Counts:4
    0012.e200.0001 (static)      0012.e200.0002 (static)
    0012.e200.0003 (static)      0012.e200.0004 (dot1x)
VLAN ID:200      MAC Counts:1
    0012.e200.1111 (dot1x)
>
```

*Figure 19-12:* Example of displaying MAC VLAN information when "dynamic" is specified

```
> show vlan mac-vlan dynamic
Date 20XX/09/21 14:15:00 UTC
VLAN counts:2      Total MAC Counts:3
VLAN ID:100      MAC Counts:2
  * 0012.e200.0003 (dot1x)      0012.e200.0004 (dot1x)
VLAN ID:200      MAC Counts:1
  0012.e200.1111 (dot1x)
>
```

*Figure 19-13:* Example of displaying MAC VLAN information when a MAC address is specified

```
> show vlan mac-vlan 0012.e200.0003
Date 20XX/09/21 14:15:00 UTC
VLAN counts:1      Total MAC Counts:2
VLAN ID:100      MAC Counts:2
  0012.e200.0003 (static)      * 0012.e200.0003 (dot1x)
>
```

## Display items

*Table 19-7:* Display items for MAC VLAN information

Item	Meaning	Displayed information
VLAN Counts	Number of displayed MAC VLANs	--
Total MAC Counts	Number of displayed MAC addresses	Number of displayed MAC addresses. The total number of MAC addresses that include valid entries already assigned to the hardware (an asterisk (*) does not appear next to the displayed MAC address) and invalid entries that have not been assigned to the hardware (an asterisk (*) appears next to the displayed MAC address).
VLAN ID	VLAN information	VLAN ID
MAC Counts	Number of displayed MAC addresses for each VLAN	Number of MAC addresses displayed for the applicable VLAN
<MAC-address> (type)	Registered MAC address	<i>type</i> : Indicates which functionality registered the address. static: Indicates that the address was registered by configuration. dot1x: Indicates that the address was registered by IEEE 802.1X authentication. vaa: Indicates that the address was registered by authentication VLAN. wa: Indicates that the address was registered by Web authentication. macauth: Indicates that the address was registered by MAC-based authentication. *: An asterisk (*) is added in either of the following cases: - Dynamically registered entry that specifies a MAC address that is also specified in an entry registered by configuration - Entry that has not been registered on hardware due to capacity limits

## Impact on communication

None

## Response messages

*Table 19-8:* List of response messages for the show vlan mac-vlan command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Mac Manager.	Communication with the L2 Mac Manager program failed. Re-execute the command. If this message is output frequently, execute the <code>restart vlan</code> command to restart the L2 Mac Manager program.
No MAC address entry.	The relevant MAC address does not exist. Make sure the specified parameter is correct, and then try again.
No operational VLAN.	There are no available VLANs. Make sure the specified parameter is correct, and then try again.

## Notes

None

---

## restart vlan

---

Restarts the VLAN program.

### Syntax

```
restart vlan [mac-manager] [-f] [core-file]
```

### Input mode

User mode and administrator mode

### Parameters

**mac-manager**

Restarts the MAC management program that operates with the VLAN program (operates when MAC VLAN is set).

Operation when this parameter is omitted:

The VLAN program is restarted. If the MAC management program is running, it is also restarted.

**-f**

Restarts VLAN program without outputting any confirmation messages.

Operation when this parameter is omitted:

A confirmation message is displayed.

**core-file**

Outputs the VLAN program's core files when restarting the VLAN program.

Operation when this parameter is omitted:

A core file is not output.

Operation when all parameters are omitted:

After a restart confirmation message is output, the VLAN program is restarted.

### Operation when a stack configuration is used

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

```
remote command <switch no.> restart vlan [mac-manager] [-f] [core-file]
```

### Example

*Figure 19-14: Restarting the VLAN program*

```
> restart vlan
VLAN Program restart OK? (y/n): y
>
```

*Figure 19-15: Restarting the VLAN program (mac-manager parameter specified)*

```
> restart vlan mac-manager
L2 Mac Manager restart OK? (y/n): y
>
```

*Figure 19-16: Restarting the VLAN program (-f parameter specified)*

```
> restart vlan -f
>
```

## Display items

None

## Impact on communication

All Ethernet interfaces are re-initialized, and the ports that make up the LAN temporarily become unable to send or receive data.

In addition, if this command is executed for a member switch where the stack functionality is operating, the member switch restarts. During the restart, communication is temporarily suspended.

## Response messages

*Table 19-9:* List of response messages for the restart vlan command

Message	Description
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 files: `nimd.core` and `L2MacManager.core`  
If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.
- Because all Ethernet interfaces are re-initialized, statistics are cleared.
- If this command is executed immediately after the `restart unicast` command is executed, the IPv4 or IPv6 route table might be unstable for a few minutes. After you execute the `restart unicast` command, wait at least five minutes, and then execute the `restart vlan` command.
- If this command is executed for a member switch where the stack functionality is operating, the member switch restarts.

---

## dump protocols vlan

---

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

### Syntax

```
dump protocols vlan
```

### Input mode

User mode and administrator mode

### Parameters

None

Dumps detailed event trace information and control table information to a file.

### Operation when a stack configuration is used

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

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

### Example

*Figure 19-17: Obtaining a VLAN dump*

```
> dump protocols vlan
>
```

### Display items

None

### Impact on communication

None

### Response messages

None

### Notes

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

Location: `/usr/var/l2/`

File: `L2MacManager_dump.gz`

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

## Chapter

---

# 20. Spanning Tree Protocols

---

```
show spanning-tree
show spanning-tree statistics
clear spanning-tree statistics
clear spanning-tree detected-protocol
show spanning-tree port-count
restart spanning-tree
dump protocols spanning-tree
```

---

## show spanning-tree

---

Displays Spanning Tree information.

### Syntax

```
show spanning-tree [ { vlan [ <vlan id list> ] | single | mst [ instance <mst instance id list> ] } [ port <port list> ] [channel-group-number <channel group list>] [virtual-link <link id>]] [ detail ] [active]
```

### Input mode

User mode and administrator mode

### Parameters

```
{ vlan [ <vlan id list> ] | single | mst [ instance <mst instance id list> ] }
```

vlan

Displays PVST+ Spanning Tree information.

<vlan id list>

Displays PVST+ Spanning Tree information for the VLAN IDs specified in list format.

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

Operation when this parameter is omitted:

Statistics for all VLANs for which PVST+ is running are displayed.

single

Displays information about Single Spanning Tree.

mst

Displays information about Multiple Spanning Tree.

instance <mst instance id list>

Displays information about Multiple Spanning Tree for the MST instance IDs specified in list format. Specifiable values for MST instance ID are in the range from 0 to 4095.

If 0 is specified as the MST instance ID, CIST is subject to display.

Operation when this parameter is omitted:

All MST instances are subject to display.

port <port list>

Displays Spanning Tree information for the specified port number. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Displays Spanning Tree information for the channel groups specified in list format. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

virtual-link <link id>

Displays Spanning Tree information for the specified virtual link ID. Specifiable values for the virtual link ID are in the range from 1 to 250.

Operation when each parameter is omitted:

This command can display only the information relevant to the condition applied by a parameter that has been set. If the parameter has not been set, information is displayed with

no condition applied. If multiple parameters are specified, information conforming to the conditions will be displayed.

detail

Displays detailed information about Spanning Tree Protocols.

Operation when this parameter is omitted:

All MST instances are subject to display.

active

Displays port information for only those ports in the `up` status.

Operation when this parameter is omitted:

Displays information for all ports.

Operation when all parameters are omitted:

Displays Spanning Tree information for Single Spanning Tree, PVST+, and Multiple Spanning Tree.

### Operation when a stack configuration is used

This command is not supported.

### Example 1

*Figure 20-1: Example of displaying PVST+ Spanning Tree information*

```
> show spanning-tree vlan 10-13
Date 20XX/07/14 12:00:00 UTC
VLAN 10  PVST+ Spanning Tree:Enabled  Mode:Rapid PVST+
  Bridge ID      Priority: 32778  MAC Address: 0012.e200.0004
  Bridge Status: Designated
  Root Bridge ID Priority: 32778  MAC Address: 0012.e200.0001
  Root Cost:2000000
  Root Port:0/1
  Port Information
    0/1 Up    Status:Forwarding  Role:Root          LoopGuard
    0/3 Up    Status:Discarding  Role:Backup
    0/4 Up    Status:Forwarding  Role:Designated    PortFast (BPDU Guard)
    0/5 Up    Status:Discarding  Role:Alternate      LoopGuard
    0/8 Up    Status:Forwarding  Role:Designated     RootGuard
    0/9 Down  Status:Disabled    Role:-
    0/10 Up   Status:Forwarding  Role:Designated     PortFast BPDU Filter
VLAN 11  PVST+ Spanning Tree:Disabled  Mode:Rapid PVST+
VLAN 12  PVST+ Spanning Tree:Enabled  Mode:Rapid PVST+
  Bridge ID      Priority: 32780  MAC Address: 0012.e200.0004
  Bridge Status: Designated
  Root Bridge ID Priority: 32780  MAC Address: 0012.e200.0002
  Root Cost:2000000
  Root Port:0/5
  Port Information
    0/5 Up    Status:Forwarding  Role:Root          Compatible
    0/6 Up    Status:Forwarding  Role:Designated     Compatible
    0/7 Up    Status:Forwarding  Role:Designated
    0/9 Down  Status:Disabled    Role:-
VLAN 13 (Disabled) PVST+ Spanning Tree:Enabled  Mode:Rapid PVST+
>
```

## Display items in Example 1

Table 20-1: Display items for the PVST+ Spanning Tree information

Item	Meaning	Displayed information
VLAN	VLAN ID	ID of the VLAN on which PVST+ Spanning Tree Protocol is running. (Disabled) is displayed if the VLAN is not running.
PVST+ Spanning Tree:	Operating status of the PVST+ Spanning Tree Protocol	Enabled: The Spanning Tree Protocol is running. Disabled: The Spanning Tree Protocol is not running.
Mode	Configured protocol type	PVST+: The protocol type is set to PVST+ mode. Rapid PVST+: The protocol type is set to Rapid PVST+ mode.
Bridge ID	Bridge ID on the Switch	--
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address of the Switch
Bridge Status	Status of the Switch	Root: Root bridge Designated: Designated bridge
Root Bridge ID	Bridge ID for the root bridge	--
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address for root bridge
Root Cost	Root path cost	Path cost value from the Switch to the root bridge 0 is displayed if the Switch is the root bridge.
Root Port	Root port	Displays the port number of the root port. If the root port is a link aggregation port, the port list for the channel group and the channel group number (ChGr) are displayed. If a virtual link is used, the port list for the virtual link and the virtual link ID are displayed. A hyphen (-) is displayed if the Switch is the root bridge.
Port Information	Displays information about the ports managed by the PVST+ Spanning Tree Protocol.	
<nif no.>/<port no.>	Port number, channel group number, or virtual link ID	The port number, channel group number, or virtual link ID of the port for which information is displayed
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status. If a virtual link is used, this means that at least one virtual link port is in the Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status. If a virtual link is used, this means that all virtual link ports are in the Down status.

Item	Meaning	Displayed information
Status	Port state	<p>If Mode is PVST+:</p> <p>Blocking: Blocking</p> <p>Listening: Listening</p> <p>Learning: Learning</p> <p>Forwarding: Indicates Forwarding status.</p> <p>Disabled: Disabled</p> <p>If Mode is Rapid PVST+:</p> <p>Discarding: Discarding</p> <p>Learning: Learning</p> <p>Forwarding: Indicates Forwarding status.</p> <p>Disabled: Disabled</p> <p>This parameter becomes Disabled if the port is in the Down status.</p>
Role	The role of the port	<p>Root: Root port</p> <p>Designated: Designated port</p> <p>Alternate: Alternate port</p> <p>Backup: Backup port</p> <p>If the port is in the Down status, a hyphen (-) is displayed, because ports in this status are not included in the topology calculations.</p> <p>These parameters are commonly used when Mode is PVST+ or Rapid PVST+.</p>
PortFast	PortFast	Indicates that the port is a PortFast port.
PortFast(BPDU Guard)	PortFast (BPDU guard functionality is applied)	Indicates that the port is a PortFast port, and that the BPDU guard functionality is applied.
BPDU Filter	BPDU filter	Indicates that the BPDU filter functionality is applied.
LoopGuard	Loop guard	Indicates that the port applies the loop guard functionality.
RootGuard	Root guard	Indicates that the port applies the root guard functionality.
Compatible	Compatible mode	Indicates that the port is operating in compatible mode when Mode for the Spanning Tree Protocol is Rapid PVST+. Ports operating in compatible mode do not perform rapid status transitions.

## Example 2

Figure 20-2: Example of displaying information about Single Spanning Tree

```

> show spanning-tree single
Date 20XX/07/14 12:00:00 UTC
Single Spanning Tree:Enabled   Mode:STP
  Bridge ID      Priority: 32768   MAC Address: 0012.e200.0004
  Bridge Status: Designated
  Root Bridge ID Priority: 32768   MAC Address: 0012.e200.0001
  Root Cost:2000000
  Root Port:0/1-2 (ChGr:32)
Port Information
  0/3      Up    Status:Blocking   Role:Alternate
  0/4      Up    Status:Forwarding Role:Designated   PortFast (BPDU Guard)
  0/5      Up    Status:Blocking   Role:Alternate    LoopGuard
  0/6      Up    Status:Forwarding Role:Designated
  0/7      Up    Status:Forwarding Role:Designated   PortFast
  0/8      Up    Status:Forwarding Role:Designated   RootGuard
  0/9      Down  Status:Disabled   Role:-
  0/10     Up    Status:Forwarding Role:Designated   PortFast BPDU Filter
  ChGr:32  Up    Status:Forwarding Role:Root         LoopGuard
>

```

## Display items in Example 2

Table 20-2: Operating status of Single Spanning Tree

Item	Meaning	Displayed information
Single Spanning Tree:	Operating status of the Spanning Tree Protocol	Enabled: The Spanning Tree Protocol is running. Disabled: The Spanning Tree Protocol is not running.
Mode	Configured protocol type	STP: The protocol type is set to STP mode. Rapid STP: The protocol type is set to Rapid STP mode.
Bridge ID	Bridge ID on the Switch	--
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address of the Switch
Bridge Status	Status of the Switch	Root: Root bridge Designated: Designated bridge
Root Bridge ID	Bridge ID for the root bridge	--
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address for root bridge
Root Cost	Root path cost	Path cost value from the Switch to the root bridge 0 is displayed if the Switch is the root bridge.
Root Port	Root port	Displays the port number of the root port. If the root port is a link aggregation port, the port list for the channel group and the channel group number (ChGr) are displayed. If a virtual link is used, the port list for the virtual link and the virtual link ID are displayed. A hyphen (-) is displayed if the Switch is the root bridge.
Port Information	Displays information about the ports managed by Single Spanning Tree.	
<nif no.>/<port no.>	Port number, channel group number, or virtual link ID	The port number, channel group number, or virtual link ID of the port for which information is displayed
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status. If a virtual link is used, this means that at least one virtual link port is in the Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status. If a virtual link is used, this means that all virtual link ports are in the Down status.

Item	Meaning	Displayed information
Status	Port state	<p>If Mode is STP:</p> <p>Blocking: Blocking</p> <p>Listening: Listening</p> <p>Learning: Learning</p> <p>Forwarding: Indicates Forwarding status.</p> <p>Disabled: Disabled</p> <p>If Mode is Rapid STP:</p> <p>Discarding: Discarding</p> <p>Learning: Learning</p> <p>Forwarding: Indicates Forwarding status.</p> <p>Disabled: Disabled</p> <p>This parameter becomes Disabled if the port is in the Down status.</p>
Role	The role of the port	<p>Root: Root port</p> <p>Designated: Designated port</p> <p>Alternate: Alternate port</p> <p>Backup: Backup port</p> <p>If the port is in the Down status, a hyphen (-) is displayed, because ports in this status are not included in the topology calculations. These parameters are commonly used when Mode is STP or Rapid STP.</p>
PortFast	PortFast	Indicates that the port is a PortFast port.
PortFast(BPDU Guard)	PortFast (BPDU guard functionality is applied)	Indicates that the port is a PortFast port, and that the BPDU guard functionality is applied.
BPDU Filter	BPDU filter	Indicates that the BPDU filter functionality is applied.
LoopGuard	Loop guard	Indicates that the port applies the loop guard functionality.
RootGuard	Root guard	Indicates that the port applies the root guard functionality.
Compatible	Compatible mode	Indicates that the port is operating in compatible mode when Mode for the Spanning Tree Protocol is Rapid STP. Ports operating in compatible mode do not perform rapid status transitions.

### Example 3

*Figure 20-3: Example of displaying information about Multiple Spanning Tree*

```

> show spanning-tree mst instance 0-4095
Date 20XX/04/14 12:00:00 UTC
Multiple Spanning Tree: Enabled
Revision Level: 65535 Configuration Name: MSTP Region Tokyo
CIST Information
VLAN Mapped: 1,3-4093,4095
Unmatch VLAN Mapped: -
CIST Root      Priority: 4096      MAC      : 0012.e200.0001
External Root Cost      : 2000000      Root Port: 0/1-2 (ChGr: 32)
Regional Root Priority: 32768      MAC      : 0012.e200.0003
Internal Root Cost      : 0
Bridge ID      Priority: 32768      MAC      : 0012.e200.0003
Regional Bridge Status : Root
Port Information
0/4      Up      Status:Blocking      Role:Alternate      Boundary Compatible
0/7      Up      Status:Forwarding     Role:Designated
0/8      Up      Status:Forwarding     Role:Designated      RootGuard
0/10     Up      Status:Forwarding     Role:Designated
0/11     Up      Status:Forwarding     Role:Designated      BPDUGuard
0/12     Up      Status:Forwarding     Role:Designated      BPDUFilter
ChGr:32  Up      Status:Forwarding     Role:Root            Boundary

```

```

MST Instance 1
VLAN Mapped: 2,4094
Unmatch VLAN Mapped: -
Regional Root Priority: 4097          MAC      : 0012.e200.0004
Internal Root Cost      : 2000000     Root Port: 0/7
Bridge ID Priority: 32769          MAC      : 0012.e200.0003
Regional Bridge Status : Designated
Port Information
  0/4      Up    Status:Blocking  Role:Alternate  Boundary Compatible
  0/7      Up    Status:Forwarding Role:Root
  0/10     Up    Status:Blocking  Role:Alternate
  0/11     Up    Status:Forwarding Role:Designated BPDUGuard
  ChGr:32  Up    Status:Forwarding Role:Master     Boundary
>

```

### Display items in Example 3

Table 20-3: Display items for information about Multiple Spanning Tree

Item	Meaning	Displayed information
Multiple Spanning Tree	Operating status of Multiple Spanning Tree	Enabled: Running Disabled: Disabled
Revision Level	Revision level	Displays the revision level that is set in the configuration. 0 to 65535
Configuration Name	Region name	Displays the region name that is set in the configuration. 0 to 32 characters
CIST Information	CIST Spanning Tree information	CIST Spanning Tree information
VLAN Mapped	Instance mapping VLAN	Lists the VLANs allocated to MST instance 0 (IST). A hyphen (-) is displayed if no VLANs are allocated. The Switch supports 1 to 4094 VLAN IDs, although according to the standard, 1 to 4095 VLAN IDs are used for region configuration. VLAN IDs from 1 to 4095 are clearly displayed so that you can determine which instance each VLAN ID supported by the standard belongs to.
Unmatch VLAN Mapped	Instance mapping VLAN in Blocking status	If Ring Protocol is also used, this item displays instance mapping VLANs whose Spanning Tree Protocols are blocked because of mismatches with the VLAN mapping of Ring Protocol. A hyphen (-) is displayed if there is no mismatch.
CIST Root	Bridge ID for the CIST root bridge	--
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address for the CIST root bridge
External Root Cost	External root path cost	Path cost value from the Switch's CIST internal bridge to the CIST root bridge. 0 is displayed if the Switch is the CIST root bridge.
Root Port	Root port	Displays the port number of the CIST root port. If the CIST root port is a link aggregation port, the link aggregation port list and the channel group number are displayed. If a virtual link is used, the port list for the virtual link and the virtual link ID are displayed. A hyphen (-) is displayed if the Switch is the CIST root bridge.

Item	Meaning	Displayed information
Regional Root	Bridge ID for the regional root bridge of MST instance 0 (IST)	Displays information about the regional root bridge of MST instance 0 (IST).
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address for the regional root bridge of MST instance 0 (IST)
Internal Root Cost	Internal root path cost for MST instance 0 (IST)	Path cost value from the Switch to the regional root bridge of MST instance 0 (IST). 0 is displayed if the Switch is the regional root bridge of MST instance 0 (IST). A hyphen (-) is displayed if Multiple Spanning Tree is disabled.
Bridge ID	Bridge ID for MST instance 0 (IST) of the Switch	Displays information about the bridge of MST instance 0 (IST) of the Switch.
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address of the Switch
Regional Bridge Status	Status of the bridge for MST instance 0 (IST) of the Switch	Root: Root bridge Designated: Designated bridge
MST Instance	MST instance ID	Displays the MST instance ID and information about the instance.
VLAN Mapped	Instance mapping VLAN	Lists the VLANs allocated to the MST instance. A hyphen (-) is displayed if no VLANs are allocated.
Unmatch VLAN Mapped	Instance mapping VLAN in Blocking status	If Ring Protocol is also used, this item displays instance mapping VLANs whose Spanning Tree Protocols are blocked because of mismatches with the VLAN mapping of Ring Protocol. A hyphen (-) is displayed if there is no mismatch.
Regional Root	ID for the regional root bridge of the MST instance	Displays information about the regional root bridge of the MST instance.
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address for the regional root bridge of the MST instance.
Internal Root Cost	Internal root path cost for the MST instance	Path cost value from the Switch to the regional root bridge of MST instance. 0 is displayed if the Switch is the regional root bridge of the MST instance.
Root Port	Root port of the MST instance	Displays the port number of the root port of the MST instance. If the root port of the MST instance is a link aggregation port, the link aggregation port list and the channel group number are displayed. If a virtual link is used, the port list for the virtual link and the virtual link ID are displayed. A hyphen (-) is displayed if the Switch is the regional root bridge of the MST instance.
Bridge ID	Bridge ID for the MST instance of the Switch	Displays information about the bridge of the MST instance of the Switch.

Item	Meaning	Displayed information
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address of the Switch
Regional Bridge Status	Status of the bridge for the MST instance of the Switch	Root: Root bridge Designated: Designated bridge
Port Information	Information about the ports of the MST instance	Displays information about the ports managed by Multiple Spanning Tree. If no VLANs are allocated to the MST instance, a response message is displayed because there are no ports.
<nif no.>/<port no.>	Port number, channel group number, or virtual link ID	The port numbers, channel group numbers, or virtual link IDs of the ports for which information is displayed
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status. If a virtual link is used, this means that at least one virtual link port is in the Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status. If a virtual link is used, this means that all virtual link ports are in the Down status.
Status	Port state	Discarding: Discarding Learning: Learning Forwarding: Indicates Forwarding status. Disabled: Disabled This parameter becomes Disabled if the port is in the Down status.
Role	The role of the port	Root: Root port Designated: Designated port Alternate: Alternate port Backup: Backup port Master: Master port If the port is in the Down status, a hyphen (-) is displayed, because ports in this status are not included in the topology calculations.
Boundary	Boundary port	Indicates that the port is the boundary port for the region. If the role of the partner device port is alternate port or backup port, the boundary port might never receive BPDUs. In such cases, the port is not displayed as the boundary port.
PortFast	PortFast	Indicates that the port is a PortFast port. (Received): Indicates that the port is subject to the Spanning Tree topology calculations because BPDUs are received while PortFast is being applied.
BPDUGuard	Application of the BPDU guard functionality for PortFast	Indicates that the port is a PortFast port, and that the BPDU guard functionality is applied. (Received): Indicates that the port is down because BPDUs are received while PortFast is being applied.
BPDUFILTER	BPDU filter	Indicates that the BPDU filter functionality is applied.
RootGuard	Root guard	Indicates that the port applies the root guard functionality.

Item	Meaning	Displayed information
Compatible	Compatible mode	Indicates that the port is operating in compatible mode for an MSTP Spanning Tree Protocol. Ports operating in compatible mode do not perform rapid status transitions.

### Example 4

*Figure 20-4: Example of displaying detailed PVST+ Spanning Tree information*

```
> show spanning-tree vlan 10 detail
Date 20XX/07/14 12:00:00 UTC
VLAN 10          PVST+ Spanning Tree:Enabled   Mode:Rapid PVST+
  Bridge ID
    Priority: 32778                      MAC Address: 0012.e200.0004
    Bridge Status: Designated           Path Cost Method:Long
    Max Age:20                          Hello Time:2
    Forward Delay:15
  Root Bridge ID
    Priority: 32778                      MAC Address: 0012.e200.0001
    Root Cost:2000000
    Root Port:0/1
    Max Age:20                          Hello Time:2
    Forward Delay:15
  Port Information
  Port:0/1  Up
    Status:Forwarding                   Role:Root
    Priority:128                        Cost:2000000
    LinkType:point-to-point             Compatible Mode:-
    LoopGuard:ON                       PortFast:OFF
    BpduFilter:OFF                     RootGuard:OFF
  BPDU Parameters(20XX/07/14 12:00:00):
    Designated Root
      Priority:32778                     MAC Address: 0012.e200.0001
    Designated Bridge
      Priority:32778                     MAC Address: 0012.e200.0001
    Root Cost:0
    Port ID
      Priority:128                       Number:16
    Message Age Timer:1(2)/20
  Port:0/3  Up
    Status:Discarding                   Role:Backup
    Priority:128                        Cost:2000000
    LinkType:point-to-point             Compatible Mode:-
    LoopGuard:OFF                      PortFast:OFF
    BpduFilter:OFF                     RootGuard:OFF
  BPDU Parameters(20XX/07/14 12:00:00):
    Designated Root
      Priority:32778                     MAC Address: 0012.e200.0001
    Designated Bridge
      Priority:32778                     MAC Address: 0012.e200.0001
    Root Cost:0
    Port ID Priority:128                 Number:8
    Message Age Timer:5(2)/20
  Port:0/4  Up
    Status:Disabled(unmatched)          Role:-
    Priority:-                           Cost:-
    LinkType:-                           Compatible Mode:-
    LoopGuard:OFF                       PortFast:BPDU Guard(BPDU not received)
    BpduFilter:OFF                      RootGuard:OFF
  Port:0/5  Up
    Status:Discarding                   Role:Alternate
    Priority:128                        Cost:2000000
    LinkType:point-to-point             Compatible Mode:-
    LoopGuard:ON(Blocking)              PortFast:OFF
    BpduFilter:OFF                      RootGuard:OFF
  BPDU Parameters(20XX/07/14 12:00:00):
```

```

    Designated Root
      Priority:32778
    Designated Bridge
      Priority:32778
      Root Cost:200000
      Port ID Priority:128
      Message Age Timer:2(2)/20
Port:0/10 Up
  Status:Forwarding
  Priority:128
  LinkType:point-to-point
  LoopGuard:OFF
  BpduFilter:ON
Port:0/11 Up
  Status:Discarding
  Priority:128
  LinkType:point-to-point
  LoopGuard:OFF
  BpduFilter:OFF
BPDU Parameters(20XX/07/14 12:00:00):
  Designated Root
    Priority:4096
  Designated Bridge
    Priority:32778
    Root Cost:200000
    Port ID Priority:128
    Message Age Timer:2(2)/20
    MAC Address: 0012.e200.0001
    MAC Address: 0012.e200.0002
    Number:16
    Role:Designated
    Cost:2000000
    Compatible Mode:-
    PortFast:ON
    RootGuard:OFF
    Role:Designated
    Cost:2000000
    Compatible Mode:-
    PortFast:OFF
    RootGuard:ON(Blocking)

```

## Display items in Example 4

Table 20-4: Display items for detailed PVST+ Spanning Tree information

Item	Meaning	Displayed information
VLAN	VLAN ID	ID of the VLAN on which PVST+ Spanning Tree Protocol is running. (Disabled) is displayed if the VLAN is not running.
PVST+ Spanning Tree:	Operating status of the PVST+ Spanning Tree Protocol	Enabled: The Spanning Tree Protocol is running. Disabled: The Spanning Tree Protocol is not running.
Mode	Configured protocol type	PVST+: The protocol type is set to PVST+ mode. Rapid PVST+: The protocol type is set to Rapid PVST+ mode.
Bridge ID	Bridge ID on the Switch	--
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address of the Switch
Bridge Status	Status of the Switch	Root: Root bridge Designated: Designated bridge
Path Cost Method	Path cost length mode	Long: 32-bit values are used for the path cost value. Short: 16-bit values are used for the path cost value.
Max Age	Maximum valid time of BPDUs	Maximum valid time of BPDUs sent from the Switch
Hello Time	Interval for sending BPDUs	Interval for sending BPDUs that are regularly sent from the Switch
Forward Delay	Time required for a state transition of the port	Time required for a state transition when the state transition is triggered by the timer

Item	Meaning	Displayed information
Root Bridge ID	Bridge ID for the root bridge	--
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address for root bridge
Root Cost	Root path cost	Path cost value from the Switch to the root bridge 0 is displayed if the Switch is the root bridge.
Root Port	Root port	Displays the port number of the root port. If the root port is a link aggregation port, the port list for the channel group and the channel group number (ChGr) are displayed. If a virtual link is used, the port list for the virtual link and the virtual link ID are displayed. A hyphen (-) is displayed if the Switch is the root bridge.
Max Age	Maximum valid time of BPDUs sent from the root bridge	Maximum valid time of BPDUs sent from the root bridge
Hello Time	Interval for sending BPDUs sent from the root bridge	Interval for sending BPDUs that are regularly sent from the root bridge
Forward Delay	Time required for a state transition of the root bridge port	Time required for a state transition when the state transition in the root bridge is triggered by the timer
Port	Port number, channel group number, or virtual link ID	The port number, channel group number, or virtual link ID of the port for which information is displayed
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status. If a virtual link is used, this means that at least one virtual link port is in the Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status. If a virtual link is used, this means that all virtual link ports are in the Down status.
Status	Port state	If Mode is PVST+: Blocking: Blocking Listening: Listening Learning: Learning Forwarding: Indicates Forwarding status. Disabled: Disabled. This status is displayed when the port is in the Down status. Disabled (unmatched) :Disabled. A configuration mismatch was detected because a BPDU with an IEEE 802.1Q tag was received when the port was disabled. If Mode is Rapid PVST+: Discarding: Discarding Learning: Learning Forwarding: Indicates Forwarding status. Disabled: Disabled. This status is displayed when the port is in the Down status. Disabled (unmatched) :Disabled. A configuration mismatch was detected because a BPDU with an IEEE 802.1Q tag was received when the port was disabled.

Item	Meaning	Displayed information
Role	The role of the port	<p>Root: Root port  Designated: Designated port  Alternate: Alternate port  Backup: Backup port</p> <p>If the port is in the Down status, a hyphen (-) is displayed, because ports in this status are not included in the topology calculations.</p> <p>These parameters are commonly used by STP and Rapid STP.</p>
Priority	Port priority	<p>Value set for the priority of the port on the Switch</p> <p>If the port is in the Down status, a hyphen (-) is displayed.</p>
Cost	Port cost	<p>Value set for the port cost of the Switch.</p> <p>If the port is in the Down status, a hyphen (-) is displayed.</p>
Link Type	Link type of the line	<p>point-to-point: The line is a 1-to-1 connection.</p> <p>shared: The line is a shared connection.</p> <p>A hyphen (-) is displayed when Mode is PVST+ or when the port is in the Down status.</p>
Compatible Mode	Compatible mode	<p>ON: Operation is in progress in compatible mode.</p> <p>A hyphen (-) is displayed when operation is in progress in normal mode (non-compatible mode) or when the port is in the Down status. Ports operating in compatible mode do not perform rapid status transitions.</p>
Loop Guard	Loop guard functionality	<p>ON: The loop guard functionality is being applied.</p> <p>ON (Blocking): The loop guard functionality is running and the port is blocked.</p> <p>OFF: The loop guard functionality is not being used.</p>
PortFast	The PortFast status. The receive status of BPDUs is displayed enclosed in parentheses.	<p>OFF: PortFast is not operating.</p> <p>ON: PortFast is operating.</p> <p>BPDu Guard: The BPDu guard functionality is being applied to PortFast.</p> <p>The receive status of BPDUs is displayed when this item is On or BPDu Guard.</p> <ul style="list-style-type: none"> <li>BPDu received (when PortFast is On: The port is included in the calculations of the Spanning Tree topology, when PortFast is BPDu Guard: The port is down)</li> <li>BPDu not received (the port is not included in the calculations of the Spanning Tree topology)</li> </ul>
BpduFilter	BPDu filter	<p>ON: The BPDu filter functionality is being applied.</p> <p>OFF: The BPDu filter functionality is not being used.</p>
Root Guard	Root guard functionality	<p>ON: The root guard functionality is being applied.</p> <p>ON (Blocking): The root guard functionality is running and the port is blocked.</p> <p>OFF: The root guard functionality is not being used.</p>
BPDu Parameters	Information about received BPDUs on the port. The last time a BPDu was received is displayed enclosed in parentheses.	<p>Displays information about the BPDUs received on the port. This item is not displayed if BPDUs are not received.</p> <p>If the port is blocked by the root guard functionality, this item displays information about the BPDUs that caused the port to be blocked.</p>
Designated Root	Root bridge information stored in the BPDu	--

Item	Meaning	Displayed information
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address for root bridge
Designated Bridge	Bridge information stored in the BPDU	--
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address
Root Cost	Root path cost	Root path cost stored in the BPDU
Port ID	Port information stored in the BPDU	--
Priority	Port priority	0 to 255 The lower the value, the higher the priority.
Number	Port number	0 to 897
Message Age Timer	Valid time of the received BPDUs	Indicates how long received BPDUs are valid. A hyphen (-) is displayed if this period has expired. <current-time>(<time-BPDU-received>)/<maximum-time> <current-time>: The time at which the BPDU is received plus the time that has elapsed <time-BPDU-received>: The time that has elapsed when the BPDU is received (Message Age of the received BPDU) <maximum-time>: Valid time (Max Age of the received BPDU)

### Example 5

*Figure 20-5: Example of displaying detailed information about Single Spanning Tree*

```
> show spanning-tree single detail
Date 20XX/07/14 12:00:00 UTC
Single Spanning Tree:Enabled   Mode:STP
Bridge ID
  Priority: 32768                MAC Address: 0012.e200.0004
  Bridge Status: Designated    Path Cost Method:Long
  Max Age:20                   Hello Time:2
  Forward Delay:15
Root Bridge ID
  Priority: 32768                MAC Address: 0012.e200.0001
  Root Cost:2000000
  Root Port:0/1-2(ChGr:32)
  Max Age:20                   Hello Time:2
  Forward Delay:15
Port Information
Port:0/3 Up
  Status:Blocking              Role:Alternate
  Priority:128                  Cost:2000000
  LinkType:-                    Compatible Mode:-
  LoopGuard:OFF                PortFast:OFF
  BpduFilter:OFF                RootGuard:OFF
BPDU Parameters(20XX/07/14 12:00:00):
  Designated Root
    Priority:32768               MAC Address: 0012.e200.0001
  Designated Bridge
    Priority:32768               MAC Address: 0012.e200.0001
```

```

    Root Cost:0
    Port ID
    Priority:128                               Number:8
    Message Age Timer:5(2)/20
Port:0/4 Up
    Status:Forwarding                         Role:Designated
    Priority:128                             Cost:2000000
    LinkType:-                               Compatible Mode:-
    LoopGuard:OFF                           PortFast:BPDU Guard(BPDU not received)
    BpduFilter:OFF                          RootGuard:OFF
Port:0/5 Up
    Status:Blocking                         Role:Alternate
    Priority:128                             Cost:2000000
    LinkType:-                               Compatible Mode:-
    LoopGuard:ON(Blocking)                  PortFast:OFF
    BpduFilter:OFF                          RootGuard:OFF
Port:0/9 Up
    Status:Disabled(unavailable)            Role:-
    Priority:-                               Cost:-
    LinkType:-                               Compatible Mode:-
    LoopGuard:OFF                           PortFast:OFF
    BpduFilter:OFF                          RootGuard:OFF
Port:0/10 Up
    Status:Forwarding                       Role:Designated
    Priority:128                             Cost:2000000
    LinkType:point-to-point                  Compatible Mode:-
    LoopGuard:OFF                           PortFast:ON
    Bpdu Filter:ON                          RootGuard:OFF
Port:0/11 Up
    Status:Blocking                         Role:Designated
    Priority:128                             Cost:2000000
    LinkType:-                               Compatible Mode:-
    LoopGuard:OFF                           PortFast:OFF
    BpduFilter:OFF                          RootGuard:ON(Blocking)
BPDU Parameters(20XX/07/14 12:00:00):
    Designated Root
    Priority:4096                             MAC Address: 0012.e200.0011
    Designated Bridge
    Priority:32768                             MAC Address: 0012.e200.0022
    Root Cost:0
    Port ID
    Priority:128                               Number:16
    Message Age Timer:1(2)/20
Port:ChGr:32 Up
    Status:Forwarding                       Role:Root
    Priority:128                             Cost:2000000
    LinkType:-                               Compatible Mode:-
    LoopGuard:ON                            PortFast:OFF
    BpduFilter:OFF                          RootGuard:OFF
BPDU Parameters(20XX/07/14 12:00:00):
    Designated Root
    Priority:32768                             MAC Address: 0012.e200.0001
    Designated Bridge
    Priority:32768                             MAC Address: 0012.e200.0001
    Root Cost:0
    Port ID
    Priority:128                               Number:16
    Message Age Timer:1(2)/20

```

&gt;

## Display items in Example 5

Table 20-5: Display items for detailed Single Spanning Tree information

Item	Meaning	Displayed information
Single Spanning Tree:	Operating status of the Spanning Tree Protocol	Enabled: The Spanning Tree Protocol is running. Disabled: The Spanning Tree Protocol is not running.
Mode	Configured protocol type	STP: The protocol type is set to STP mode. Rapid STP: The protocol type is set to Rapid STP mode.
Bridge ID	Bridge ID on the Switch	--
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address of the Switch
Bridge Status	Status of the Switch	Root: Root bridge Designated: Designated bridge
Path Cost Method	Path cost length mode	Long: 32-bit values are used for the path cost value. Short: 16-bit values are used for the path cost value.
Max Age	Maximum valid time of BPDUs	Maximum valid time of BPDUs sent from the Switch
Hello Time	Interval for sending BPDUs	Interval for sending BPDUs that are regularly sent from the Switch
Forward Delay	Time required for a state transition of the port	Time required for a state transition when the state transition is triggered by the timer
Root Bridge ID	Bridge ID for the root bridge	--
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC Address	MAC address	MAC address for root bridge
Root Cost	Root path cost	Path cost value from the Switch to the root bridge 0 is displayed if the Switch is the root bridge.
Root Port	Root port	Displays the port number of the root port. If the root port is a link aggregation port, the port list and the channel group number (ChGr) for the link aggregation are displayed. If a virtual link is used, the port list for the virtual link and the virtual link ID are displayed. A hyphen (-) is displayed if the Switch is the root bridge.
Max Age	Maximum valid time of BPDUs sent from the root bridge	Maximum valid time of BPDUs sent from the root bridge
Hello Time	Interval for sending BPDUs sent from the root bridge	Interval for sending BPDUs that are regularly sent from the root bridge
Forward Delay	Time required for a state transition of the root bridge port	Time required for a state transition when the state transition in the root bridge is triggered by the timer
Port	Port number, channel group number, or virtual link ID	The port number, channel group number, or virtual link ID of the port for which information is displayed

Item	Meaning	Displayed information
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status. If a virtual link is used, this means that at least one virtual link port is in the Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status. If a virtual link is used, this means that all virtual link ports are in the Down status.
Status	Port state	If Mode is STP: Blocking: Blocking Listening: Listening Learning: Learning Forwarding: Indicates Forwarding status. Disabled: Disabled. This status is displayed when the port is in the Down status. Disabled (unavailable): Disabled. Single Spanning Tree cannot be used because PVST+ is enabled for the port. If Mode is Rapid STP: Discarding: Discarding Learning: Learning Forwarding: Indicates Forwarding status. Disabled: Disabled. This status is displayed when the port is in the Down status. Disabled (unavailable): Disabled. Single Spanning Tree cannot be used because PVST+ is enabled for the port.
Role	The role of the port	Root: Root port Designated: Designated port Alternate: Alternate port Backup: Backup port If the port is in the Down status, a hyphen (-) is displayed, because ports in this status are not included in the topology calculations. These parameters are used by both STP and Rapid STP.
Priority	Port priority	Value set for the priority of the port on the Switch If the port is in the Down status, a hyphen (-) is displayed.
Cost	Port cost	Value set for the port cost of the Switch. If the port is in the Down status, a hyphen (-) is displayed.
Link Type	Link type of the line	point-to-point: The line is a 1-to-1 connection. shared: The line is a shared connection. A hyphen (-) is displayed when Mode is PVST+ or when the port is in the Down status.
Compatible Mode	Compatible mode	ON: Operation is in progress in compatible mode. A hyphen (-) is displayed when operation is in progress in normal mode (non-compatible mode) or when the port is in the Down status. Ports operating in compatible mode do not perform rapid status transitions.
Loop Guard	Loop guard functionality	ON: The loop guard functionality is being applied. ON (Blocking): The loop guard functionality is running and the port is blocked. OFF: The loop guard functionality is not being used.

Item	Meaning	Displayed information
PortFast	The PortFast status. The receive status of BPDUs is displayed enclosed in parentheses.	<p>OFF: PortFast is not operating.  ON: PortFast is operating.  BPDU Guard: The BPDU guard functionality is being applied to PortFast.  The receive status of BPDUs is displayed when this item is On or BPDU Guard.</p> <ul style="list-style-type: none"> <li>• BPDU received (when PortFast is On: The port is included in the calculations of the Spanning Tree topology, when PortFast is BPDU Guard: The port is down)</li> <li>• BPDU not received (the port is not included in the calculations of the Spanning Tree topology)</li> </ul>
BpduFilter	BPDU filter	<p>ON: The BPDU filter functionality is being applied.  OFF: The BPDU filter functionality is not being used.</p>
Root Guard	Root guard functionality	<p>ON: The root guard functionality is being applied.  ON (Blocking): The root guard functionality is running and the port is blocked.  OFF: The root guard functionality is not being used.</p>
BPDU Parameters	Information about received BPDUs on the port. The last time a BPDU was received is displayed enclosed in parentheses.	Displays information about the BPDUs received on the port. This item is not displayed if BPDUs are not received. If the port is blocked by the root guard functionality, this item displays information about the BPDUs that caused the port to be blocked.
Designated Root	Root bridge information stored in the BPDU	--
Priority	Bridge priority	<p>0 to 65535  The lower the value, the higher the priority.</p>
MAC Address	MAC address	MAC address for root bridge
Designated Bridge	Bridge information stored in the BPDU	--
Priority	Bridge priority	<p>0 to 65535  The lower the value, the higher the priority.</p>
MAC Address	MAC address	MAC address
Root Cost	Root path cost	Root path cost stored in the BPDU
Port ID	Port information stored in the BPDU	--
Priority	Port priority	<p>0 to 255  The lower the value, the higher the priority.</p>
Number	Port number	0 to 897
Message Age Timer	Valid time of the received BPDUs	<p>Indicates how long received BPDUs are valid.  A hyphen (-) is displayed if this period has expired.  &lt;current-time&gt;(&lt;time-BPDU-received&gt;)/&lt;maximum-time&gt;  &lt;current-time&gt;:  The time at which the BPDU is received plus the time that has elapsed  &lt;time-BPDU-received&gt;:  The time that has elapsed when the BPDU is received (Message Age of the received BPDU)  &lt;maximum-time&gt;:  Valid time (Max Age of the received BPDU)</p>

**Example 6***Figure 20-6: Example of displaying detailed information about Multiple Spanning Tree*

```

> show spanning-tree mst detail
Date 20XX/04/14 12:00:00 UTC
Multiple Spanning Tree: Enabled
Revision Level: 65535 Configuration Name: MSTP Region Tokyo
CIST Information Time Since Topology Change: 2.4:25:50
VLAN Mapped: 1,3-4093,4095
Unmatch VLAN Mapped: -
CIST Root Priority: 4096 MAC : 0012.e200.0001
External Root Cost : 2000000 Root Port : 0/1-2(ChGr: 32)
Max Age : 20
Forward Delay : 15
Regional Root Priority: 32768 MAC : 0012.e200.0003
Internal Root Cost : 0
Remaining Hops : 20
Bridge ID Priority: 32768 MAC : 0012.e200.0003
Regional Bridge Status : Root Path Cost Method: Long
Max Age : 20 Hello Time : 2
Forward Delay : 15 Max Hops : 20
Port Information
Port: 0/4 Up Boundary Compatible
Status : Blocking Role : Alternate
Priority : 128 Cost : 2000000
Link Type : shared PortFast: OFF
BpduFilter:OFF Hello Time: 4
RootGuard :OFF
BPDU Parameters(20XX/07/14 12:00:00):
Protocol Version : STP(IEEE802.1D)
Root Priority: 4096 MAC : 0012.e200.0001
External Root Cost : 2000000
Designated Bridge Priority: 32768 MAC : 0012.e200.0002
Designated Port ID Priority: 128 Number : 1
Message Age Timer : 1(2)/20 Remaining Hops: -
Port:0/7 Up
Status : Forwarding Role : Designated
Priority : 128 Cost : 2000000
Link Type : point-to-point PortFast: OFF
BpduFilter:OFF Hello Time: 2
RootGuard :OFF
BPDU Parameters(20XX/07/14 12:00:00):
Protocol Version : MSTP(IEEE802.1s)
Root Priority: 4096 MAC : 0012.e200.0001
External Root Cost : 2000000
Regional Root Priority: 4096 MAC : 0012.e200.0003
Internal Root Cost : 2000000
Designated Bridge Priority: 32768 MAC : 0012.e200.0004
Designated Port ID Priority: 128 Number : 2
Message Age Timer : 1(2)/20 Remaining Hops: 19
Port:0/10 Up
Status : Forwarding Role : Designated
Priority : 128 Cost : 2000000
LinkType : point-to-point PortFast: OFF
BpduFilter:OFF Hello Time: 2
RootGuard :OFF
BPDU Parameters(20XX/07/14 12:00:00):
Protocol Version : MSTP(IEEE802.1s)
Root Priority: 4096 MAC : 0012.e200.0001
External Root Cost : 2000000
Regional Root Priority: 4096 MAC : 0012.e200.0003
Internal Root Cost : 2000000
Designated Bridge Priority: 32768 MAC : 0012.e200.0005
Designated Port ID Priority: 128 Number : 3
Message Age Timer : 1(2)/20 Remaining Hops: 19
Port:0/11 Up
Status : Forwarding Role : Designated

```

```

Priority : 128          Cost : 2000000
Link Type : point-to-point  PortFast: BPDU Guard(BPDU not received)
BpduFilter:OFF          Hello Time: 2
RootGuard :OFF
Port:0/12 Up
Status :Forwarding      Role : Designated
Priority : 128          Cost : 2000000
Link Type : point-to-point  PortFast: BPDU Filter
BpduFilter:ON          Hello Time: 2
RootGuard :OFF
Port:ChGr:32 Up      Boundary
Status : Forwarding      Role : Root
Priority : 128          Cost : 2000000
Link Type : point-to-point  PortFast: OFF
BpduFilter:OFF          Hello Time: 4
RootGuard :OFF
BPDU Parameters(20XX/07/14 12:00:00):
  Protocol Version : MSTP(IEEE802.1s)
  Root Priority: 4096 MAC : 0012.e200.0001
  External Root Cost : 2000000
  Regional Root Priority: 4096 MAC : 0012.e200.0001
  Internal Root Cost : 2000000
  Designated Bridge Priority: 32768 MAC : 0012.e200.0001
  Designated Port ID Priority: 128 Number : 800
  Message Age Timer : 1(2)/20 Remaining Hops: 19
MST Instance 1 Time Since Topology Change: 2.4:25:30
VLAN Mapped: 2,4094
Unmatch VLAN Mapped: -
Regional Root Priority: 4097 MAC : 0012.e200.0004
Internal Root Cost : 2000000 Root Port : 0/7
Remaining Hops : 20
Bridge ID Priority: 32768 MAC : 0012.e200.0003
Regional Bridge Status : Designated
Max Age : 20 Hello Time : 2
Forward Delay : 15 Max Hops : 20
Port Information
Port: 0/4 Up      Boundary Compatible
Status : Blocking      Role : Alternate
Priority : 128          Cost : 2000000
Link Type : shared      PortFast: OFF
BpduFilter:OFF          Hello Time: 2
RootGuard :OFF
Port:0/7 Up
Status : Forwarding      Role : Root
Priority : 128          Cost : 2000000
Link Type : point-to-point  PortFast: OFF
BpduFilter:OFF          Hello Time: 4
RootGuard :OFF
BPDU Parameters(20XX/07/14 12:00:00):
  Protocol Version : MSTP(IEEE802.1s)
  Regional Root Priority: 4096 MAC : 0012.e200.0004
  Internal Root Cost : 2000000
  Designated Bridge Priority: 32768 MAC : 0012.e200.0004
  Designated Port ID Priority: 128 Number : 2
  Message Age Timer : 1(2)/20 Remaining Hops: 19
Port:0/10 Up
Status : Blocking      Role : Alternate
Priority : 128          Cost : 2000000
Link Type : point-to-point  PortFast: OFF
BpduFilter:OFF          Hello Time: 4
RootGuard :OFF
BPDU Parameters(20XX/07/14 12:00:00):
  Protocol Version : MSTP(IEEE802.1s)
  Regional Root Priority: 4096 MAC : 0012.e200.0004
  Internal Root Cost : 2000000
  Designated Bridge Priority: 32768 MAC : 0012.e200.0002
  Designated Port ID Priority: 128 Number : 3

```

```

    Message Age Timer : 1(2)/20    Remaining Hops: 19
Port:0/11 Up
  Status      : Forwarding          Role      : Designated
  Priority     : 128                  Cost       : 2000000
  Link Type    : point-to-point      PortFast: BPDU Guard(BPDU not received)
  BpduFilter:OFF                     Hello Time: 2
  RootGuard :OFF
Port:ChGr:32 Up      Boundary
  Status      : Forwarding          Role      : Master
  Priority     : 128                  Cost       : 2000000
  Link Type    : point-to-point      PortFast: OFF
  BpduFilter:OFF                     Hello Time: 4
  RootGuard :OFF
BPDU Parameters(20XX/07/14 12:00:00):
  Protocol Version : MSTP(IEEE802.1s)
  Regional Root    Priority: 4096    MAC       : 0012.e200.0004
  Internal Root Cost : 2000000
  Designated Bridge Priority: 32768    MAC       : 0012.e200.0001
  Designated Port ID Priority: 128     Number  : 800
  Message Age Timer : 1(2)/20    Remaining Hops: 19
>

```

## Display items in Example 6

Table 20-6: Display items for detailed Multiple Spanning Tree information

Item	Meaning	Displayed information
Multiple Spanning Tree	Operating status of Multiple Spanning Tree	Enabled: Running Disabled: Disabled
Revision Level	Revision level	Displays the revision level that is set in the configuration. 0 to 65535
Configuration Name	Region name	Displays the region name that is set in the configuration. 0 to 32 characters
CIST Information	CIST Spanning Tree information	CIST Spanning Tree information
Time Since Topology Change	Time since a topology change was detected	hh:mm:ss (when the elapsed time is less than 24 hours) ddd.hh:mm:ss (when the elapsed time exceeds 24 hours) Over 1000 days (when the elapsed time is more than 1000 days)
VLAN Mapped	Instance mapping VLAN	Lists the VLANs allocated to MST instance 0 (IST). A hyphen (-) is displayed if no VLANs are allocated. The Switch supports 1 to 4094 VLAN IDs, although according to the standard, 1 to 4095 VLAN IDs are used for region configuration. VLAN IDs from 1 to 4095 are clearly displayed so that you can determine which instance each VLAN ID supported by the standard belongs to.
Unmatch VLAN Mapped	Instance mapping VLAN in Blocking status	If Ring Protocol is also used, this item displays instance mapping VLANs whose Spanning Tree Protocols are blocked because of mismatches with the VLAN mapping of Ring Protocol. A hyphen (-) is displayed if there is no mismatch.
CIST Root	Bridge ID for the CIST root bridge	--
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.

Item	Meaning	Displayed information
MAC	MAC address	MAC address for the CIST root bridge
External Root Cost	External root path cost	Path cost value from the Switch's CIST internal bridge to the CIST root bridge. 0 is displayed if the Switch is the CIST root bridge.
Root Port	Root port	Displays the port number of the CIST root port. If the CIST root port is a link aggregation port, the link aggregation port list and the channel group number are displayed. If a virtual link is used, the port list for the virtual link and the virtual link ID are displayed. A hyphen (-) is displayed if the Switch is the CIST root bridge.
Max Age	Maximum valid time of BPDUs sent from the CIST root bridge	Displays the maximum valid time of BPDUs sent from the CIST root bridge.
Forward Delay	Time required for a state transition of the CIST root bridge port	Displays the time required for a state transition when the state transition in the CIST root bridge is triggered by the timer
Regional Root	Bridge ID for the regional root bridge of MST instance 0 (IST)	Displays information about the regional root bridge of MST instance 0 (IST).
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address for the regional root bridge of MST instance 0 (IST)
Internal Root Cost	Internal root path cost for MST instance 0 (IST)	Path cost value from the Switch to the regional root bridge of MST instance 0 (IST). 0 is displayed if the Switch is the regional root bridge of MST instance 0 (IST).
Remaining Hops	Number of remaining hops	0 to 40 Displays the remaining number of hops for BPDUs that the regional root bridge of MST instance 0 (IST) sends.
Bridge ID	Bridge ID for MST instance 0 (IST) of the Switch	Displays information about the bridge of MST instance 0 (IST) of the Switch.
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address of the Switch
Regional Bridge Status	Status of the bridge for MST instance 0 (IST) of the Switch	Root: Root bridge Designated: Designated bridge
Path Cost Method	Path cost length mode	Long: 32-bit values are used for the path cost value.
Max Age	Maximum valid time for BPDUs sent from the MST instance 0 (IST) of the Switch	Displays the maximum valid time for BPDUs sent from the MST instance 0 (IST) bridge of the Switch.
Hello Time	Interval for sending the BPDUs of MST instance 0 (IST) of the Switch	Displays the interval for sending BPDUs that are regularly sent from the MST instance 0 (IST) bridge of the Switch.
Forward Delay	Time required for a state transition of the MSI instance 0 (IST) port on the Switch	Displays the time required for a state transition when the state transition in the bridge of MSI instance 0 (IST) on the Switch is triggered by the timer.

Item	Meaning	Displayed information
Max Hops	Maximum number of hops in MST instance 0 (IST) of the Switch	2 to 40 Displays the maximum number of hops for BPDUs sent from the MST instance 0 (IST) bridge of the Switch.
MST Instance	MST instance ID	Displays the MST instance ID and information about the instance.
Time Since Topology Change	Time since a topology change was detected	<i>hh:mm:ss</i> (when the elapsed time is less than 24 hours) <i>ddd.hh:mm:ss</i> (when the elapsed time exceeds 24 hours) Over 1000 days (when the elapsed time is more than 1000 days)
VLAN Mapped	Instance mapping VLAN	Lists the VLANs allocated to the MST instance. A hyphen (-) is displayed if no VLANs are allocated.
Unmatch VLAN Mapped	Instance mapping VLAN in Blocking status	If Ring Protocol is also used, this item displays instance mapping VLANs whose Spanning Tree Protocols are blocked because of mismatches with the VLAN mapping of Ring Protocol. A hyphen (-) is displayed if there is no mismatch.
Regional Root	Bridge ID for the regional root bridge of the MST instance	Displays information about the regional root bridge of the MST instance.
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address for the regional root bridge of the MST instance
Internal Root Cost	Internal root path cost for the MST instance	Path cost value from the Switch to the regional root bridge of MST instance. 0 is displayed if the Switch is the regional root bridge of the MST instance.
Root Port	Root port of the MST instance	Displays the port number of the root port of the MST instance. If the root port of the MST instance is a link aggregation port, the link aggregation port list and the channel group number are displayed. If a virtual link is used, the port list for the virtual link and the virtual link ID are displayed. A hyphen (-) is displayed if the Switch is the regional root bridge of the MST instance.
Remaining Hops	Number of remaining hops	0 to 40 Displays the remaining number of hops for BPDUs that the regional root bridge of the MST instance sends.
Bridge ID	Bridge ID for the MST instance of the Switch	Displays information about the bridge of the MST instance of the Switch.
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address of the Switch
Regional Bridge Status	Status of the bridge for the MST instance of the Switch	Root: Root bridge Designated: Designated bridge
Max Age	Maximum valid time of BPDUs sent from the MST instance of the Switch	Displays the maximum valid time of BPDUs sent from the MST instance bridge of the Switch.

Item	Meaning	Displayed information
Hello Time	Interval for sending BPDUs sent from the MST instance of the Switch	Displays the interval for sending BPDUs that are regularly sent from the MST instance bridge of the Switch.
Forward Delay	Time required for a state transition of the MST instance port on the Switch	Displays the time required for a state transition when the state transition in the bridge of the MST instance on the Switch is triggered by the timer.
Max Hops	Maximum number of hops in the MST instance of the Switch	2 to 40 Displays the maximum number of hops for BPDUs sent from the MST instance bridge of the Switch.
Port Information	Information about the ports of the MST instance	Displays information about the ports managed by Multiple Spanning Tree. If no VLANs are allocated to the MST instance, a response message is displayed because there are no ports.
<nif no.> / <port no.>	Port number, channel group number, or virtual link ID	The port numbers, channel group numbers, or virtual link IDs of the ports for which information is displayed
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status. If a virtual link is used, this means that at least one virtual link port is in the Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status. If a virtual link is used, this means that all virtual link ports are in the Down status.
Boundary	Boundary port	Indicates that the port is the boundary port for the region. If the role of the partner device port is alternate port or backup port, the boundary port might never receive BPDUs. In such cases, the port is not displayed as the boundary port.
Compatible	Compatible mode	Indicates that the port is operating in compatible mode for an MSTP Spanning Tree Protocol. Ports operating in compatible mode do not perform rapid status transitions.
Status	Port state	Discarding: Discarding Learning: Learning Forwarding: Indicates Forwarding status. Disabled: Disabled This parameter becomes Disabled if the port is in the Down status.
Role	The role of the port	Root: Root port Designated: Designated port Alternate: Alternate port Backup: Backup port Master: Master port If the port is in the Down status, a hyphen (-) is displayed, because ports in this status are not included in the topology calculations.
Priority	Port priority	Displays the value of the port priority setting for the MST instance of the Switch. If the port is in the Down status, a hyphen (-) is displayed.
Cost	Port cost	Displays the value of the port cost setting for the MST instance of the Switch. If the port is in the Down status, a hyphen (-) is displayed.

Item	Meaning	Displayed information
Link Type	Link type of the line	point-to-point: The line is a 1-to-1 connection. shared: The line is a shared connection. A hyphen (-) is displayed when Mode is STP or when the port is in the Down status.
PortFast	The PortFast status. The status of receive BPDUs is displayed enclosed in parentheses.	OFF: PortFast is not operating. ON: PortFast is operating. BPDU Guard: The BPDU guard functionality is being applied to PortFast. The receive status of BPDUs is displayed when this item is On or BPDU Guard. <ul style="list-style-type: none"> <li>BPDU received (when PortFast is On: The port is included in the calculations of the Spanning Tree topology, when PortFast is BPDU Guard: The port is down)</li> <li>BPDU not received (the port is not included in the calculations of the Spanning Tree topology)</li> </ul>
BpduFilter	BPDU filter	ON: The BPDU filter functionality is being applied. OFF: The BPDU filter functionality is not being used.
Hello Time	Interval for sending and receiving BPDUs on the port	For the root port, alternate port, and backup port, the value on the partner device is displayed. For the designated port, the value on the Switch is displayed.
Root Guard	Root guard functionality	ON: The root guard functionality is being applied. ON (Blocking): The root guard functionality is running and the port is blocked (all MSTIs for the port are blocked). OFF: The root guard functionality is not being used.
BPDU Parameters	Information about received BPDUs on the port. The last time a BPDU was received is displayed enclosed with parentheses.	Displays information about the BPDUs received at the CIST or MST instance port. This item is not displayed if BPDUs are not received. The BPDU information whose Mode Version is STP or Rapid STP is displayed only by CIST.
Protocol Version	Protocol versions	Displays the protocol version of the received BPDUs. STP (IEEE802.1D): Indicates that BPDUs in which the protocol version is set to STP (IEEE 802.1D) were received from neighboring devices. Rapid STP (IEEE802.1w): Indicates that BPDUs in which the protocol version is set to RSTP (IEEE 802.1W) were received from neighboring devices. MSTP (IEEE802.1s): Indicates that BPDUs in which the protocol version is set to MSTP (IEEE 802.1s) were received from neighboring devices.
Root	Root bridge information stored in the BPDU	If Protocol Version is MSTP, information about the CIST root bridge is displayed. This item is not displayed for MST instance 1 or later instances. If Mode Version is STP or Rapid STP, information about the root bridge is displayed.
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address for the root bridge

Item	Meaning	Displayed information
External Root Cost	External root path cost	If <code>Protocol Version</code> is MSTP, information about the CIST root path cost is displayed. This item is not displayed for MST instance 1 or later instances. If <code>Mode Version</code> is STP or Rapid STP, information about the root path cost is displayed.
Regional Root	Regional root bridge information stored in the BPDU	If <code>Protocol Version</code> is MSTP, information about the CIST and MSTI regional root bridge is displayed. If <code>Mode Version</code> is STP or Rapid STP, this information is not displayed.
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address for the regional root bridge
Internal Root Cost	Internal root path cost	If <code>Protocol Version</code> is MSTP, the internal root path cost is displayed. If <code>Mode Version</code> is STP or Rapid STP, this information is not displayed.
Designated Bridge	Bridge information stored in the BPDU	--
Priority	Bridge priority	0 to 65535 The lower the value, the higher the priority.
MAC	MAC address	MAC address
Port ID	Port information stored in the BPDU	--
Priority	Port priority	0 to 255 The lower the value, the higher the priority.
Number	Port number	0 to 892
Message Age Timer	Valid time of the received BPDUs	Indicates how long received BPDUs are valid. A hyphen (-) is displayed if this period has expired. <current-time>(<time-BPDU-received>)/<maximum-time> <current-time>: The time at which the BPDU is received plus the time that has elapsed <time-BPDU-received>: The time that has already elapsed when the BPDU is received (Message Age of the received BPDU) <maximum-time>: Valid time (Max Age of the received BPDU)
Remaining Hops	Number of remaining hops	0 to 40 Displays the number of remaining hops for the MST bridge stored in the received BPDU. A hyphen (-) is displayed if <code>Mode Version</code> is STP or Rapid STP.

### Impact on communication

None

## Response messages

*Table 20-7:* List of response messages for the show spanning-tree command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Spanning Tree program.	Communication with the Spanning Tree program failed.
No corresponding port information.	No port and channel group information exists as Spanning Tree information.
Spanning Tree is not configured.	The Spanning Tree Protocol has not been configured. Check the configuration.
Specified Spanning Tree is not configured.	The specified Spanning Tree Protocol has not been configured. Check the configuration.

## Notes

None

---

## show spanning-tree statistics

---

Displays statistics about Spanning Tree Protocols.

### Syntax

```
show spanning-tree statistics [ {vlan [ <vlan id list> ] | single | mst [ instance
<mst instance id list> ] } [ port <port list> ] [channel-group-number <channel group
list>] [virtual-link <link id>]]
```

### Input mode

User mode and administrator mode

### Parameters

```
{vlan [ <vlan id list> ] | single | mst [ instance <mst instance id list> ]}
```

vlan

Displays PVST+ statistics.

<vlan id list>

Displays PVST+ Spanning Tree statistics for the VLAN IDs specified in list format.

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

Operation when this parameter is omitted:

Statistics for all VLANs for which PVST+ is running are displayed.

single

Displays statistics about Single Spanning Tree.

mst

Displays statistics about Multiple Spanning Tree.

instance <mst instance id list>

Displays statistics about Multiple Spanning Tree for the MST instance IDs specified in list format. Specifiable values for MST instance ID are in the range from 0 to 4095.

If 0 is specified as the MST instance ID, CIST is subject to display.

Operation when this parameter is omitted:

All MST instances are subject to display.

port <port list>

Displays Spanning Tree statistics for the specified port number. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

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

virtual-link <link id>

Displays Spanning Tree statistics for the specified virtual link ID. Specifiable values for the virtual link ID are in the range from 1 to 250.

Operation when all parameters are omitted:

Displays statistics about Single Spanning Tree, PVST+, and Multiple Spanning Tree.

## Operation when a stack configuration is used

This command is not supported.

### Example 1

*Figure 20-7: Example of displaying PVST+ Spanning Tree statistics*

```
>show spanning-tree statistics vlan 10,12
Date 20XX/07/14 12:00:00 UTC
VLAN 10
Time Since Topology Change:1 day 10 hour 50 minute 20 second
Topology Change Times:130
Port:0/1 Up
  TxBPDUs      :      904567  RxBPDUs      :      130
  Forward Transit Times:      120  RxDiscard BPDUs:      3
  Discard BPDUs by reason
    Timeout      :      3  Invalid      :      0
    Not Support   :      0  Other       :      0
Port:0/2 Up
  TxBPDUs      :      100  RxBPDUs      :      80572
  Forward Transit Times:      10  RxDiscard BPDUs:      0
  Discard BPDUs by reason
    Timeout      :      0  Invalid      :      0
    Not Support   :      0  Other       :      0
Port:0/3 Up
  TxBPDUs      :      129  RxBPDUs      :      79823
  Forward Transit Times:      10  RxDiscard BPDUs:      4
  Discard BPDUs by reason
    Timeout      :      2  Invalid      :      0
    Not Support   :      2  Other       :      0
Port:0/10 Up
  TxBPDUs      :      129  RxBPDUs      :      79823
  Forward Transit Times:      10  RxDiscard BPDUs:      123
  Discard BPDUs by reason
    Timeout      :      0  Invalid      :      0
    Not Support   :      0  Other       :      123
VLAN 12
Time Since Topology Change:1 day 10 hour 50 minute 20 second
Topology Change Times:130
Port:0/1 Up
  TxBPDUs      :      154  RxBPDUs      :      86231
  Forward Transit Times:      24  RxDiscard BPDUs:      2
  Discard BPDUs by reason
    Timeout      :      2  Invalid      :      0
    Not Support   :      0  Other       :      0
Port:0/2 Up
  TxBPDUs      :      100  RxBPDUs      :      80572
  Forward Transit Times:      10  RxDiscard BPDUs:      0
  Discard BPDUs by reason
    Timeout      :      0  Invalid      :      0
    Not Support   :      0  Other       :      0
Port:0/3 Up
  TxBPDUs      :      421  RxBPDUs      :      84956
  Forward Transit Times:      19  RxDiscard BPDUs:      10
  Discard BPDUs by reason
    Timeout      :      10  Invalid      :      0
    Not Support   :      0  Other       :      0
>
```

*Figure 20-8: Example of displaying Single Spanning Tree statistics*

```
>show spanning-tree statistics single
Date 20XX/07/14 12:00:00 UTC
Time Since Topology Change:2 day 4 hour 25 minute 50 second
Topology Change Times:280
Port:0/1 Up
  TxBPDUs      :      1865421  RxBPDUs      :      260
  Forward Transit Times:      250  RxDiscard BPDUs:      10
```

```

Discard BPDUs by reason
  Timeout      :      10 Invalid      :      0
  Not Support   :      0 Other        :      0
Port:0/2 Up
  TxBPDUs      :    1970 RxBPDUs      :   183450
  Forward Transit Times:    120 RxDiscard BPDUs:      5
  Discard BPDUs by reason
    Timeout      :      1 Invalid      :      1
    Not Support   :      3 Other        :      0
Port:0/3 Up
  TxBPDUs      :  1771092 RxBPDUs      :   1745312
  Forward Transit Times:      2 RxDiscard BPDUs:      1
  Discard BPDUs by reason
    Timeout      :      1 Invalid      :      0
    Not Support   :      0 Other        :      0
Port:0/10 Up
  TxBPDUs      :     129 RxBPDUs      :    79823
  Forward Transit Times:     10 RxDiscard BPDUs:     123
  Discard BPDUs by reason
    Timeout      :      0 Invalid      :      0
    Not Support   :      0 Other        :    123
>

```

## Display items in Example 1

Table 20-8: Display items for PVST+ and Single Spanning Tree statistics

Item	Meaning	Displayed information
Time Since Topology Change	Time since a topology change was detected	<i>n</i> day: Days <i>n</i> hour: Hours <i>n</i> minute: Minutes <i>n</i> second: Seconds For Rapid STP or Rapid PVST+, this item shows the time that has elapsed since Spanning Tree Protocol operation started.
Topology ChangeTimes	Number of detecting topology changes	--
Port	Port number	--
ChGr	Channel group number	--
VL	Virtual link ID	--
VLAN ID	VLAN ID subject to PVST+	Displayed only when <code>vlan</code> is specified.
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status. If a virtual link is used, this means that at least one virtual link port is in the Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status. If a virtual link is used, this means that all virtual link ports are in the Down status.
Forward Transit Times	Number of transitions to the forwarding state	--
TxBPDUs	Number of sent BPDUs	--
RxBPDUs	Number of received BPDUs	--

Item	Meaning	Displayed information
RxDiscardsBPDUs	Number of discarded received BPDUs	--
Timeout	Number of BPDUs whose valid time expired	Number of received BPDUs whose valid time (which is set in the BPDUs) expired
Invalid	Number of invalid BPDUs	Number of received BPDUs whose format was invalid
Not Support	Number of unsupported BPDUs	Number of received BPDUs that included unsupported parameters
Other	Number of BPDUs discarded for another reason	Displays the number of discarded received BPDUs when BPDU discard has been configured. - When a BPDU filter has been set - When the root guard functionality is operating - When the port receives BPDUs that were sent from the port

## Example 2

*Figure 20-9: Example of displaying Multiple Spanning Tree statistics*

```
>show spanning-tree statistics mst
Date 20XX/07/14 12:00:00 UTC
MST Instance ID: 0 Topology Change Times:      280
Port:0/1 Up
  TxBPDUs      : 1865421 RxBPDUs      : 260
  Forward Transit Times: 250 RxDiscard BPDUs: 10
  Discard BPDUs by reason
    Timeout      : 10 Invalid      : 0
    Not Support   : 0 Other      : 0
  Ver3Length Invalid : 0 Exceeded Hop : 0
Port:0/2 Up
  TxBPDUs      : 1970 RxBPDUs      : 183450
  Forward Transit Times: 120 RxDiscard BPDUs: 5
  Discard BPDUs by reason
    Timeout      : 1 Invalid      : 1
    Not Support   : 3 Other      : 0
  Ver3Length Invalid : 22 Exceeded Hop : 21
Port:0/3 Up
  TxBPDUs      : 177092 RxBPDUs      : 1742
  Forward Transit Times: 2 RxDiscard BPDUs: 0
  Discard BPDUs by reason
    Timeout      : 0 Invalid      : 0
    Not Support   : 0 Other      : 0
  Ver3Length Invalid : 10 Exceeded Hop : 5
Port:0/4 Up
  TxBPDUs      : 1092 RxBPDUs      : 1312
  Forward Transit Times: 3 RxDiscard BPDUs: 41
  Discard BPDUs by reason
    Timeout      : 0 Invalid      : 2
    Not Support   : 0 Other      : 39
  Ver3Length Invalid : 0 Exceeded Hop : 0
ChGr:32 Up
  TxBPDUs      : 2 RxBPDUs      : 15
  Forward Transit Times: 2 RxDiscard BPDUs: 5
  Discard BPDUs by reason
    Timeout      : 0 Invalid      : 0
    Not Support   : 3 Other      : 2
  Ver3Length Invalid : 0 Exceeded Hop : 0
MST Instance ID: 1 Topology Change Times: 290
Port:0/1 Up
  TxBPDUs      : 1865421 RxBPDUs      : 260
  Forward Transit Times: 250 Discard Message: 0
  Exceeded Hop   : 0
```

```

Port:0/2  Up
  TxBPDUs      :      1970  RxBPDUs      :      183450
  Forward Transit Times:      120  Discard Message:      7
  Exceeded Hop   :      1
Port:0/3  Up
  TxBPDUs      :     177092  RxBPDUs      :      1742
  Forward Transit Times:      2  Discard Message:      0
  Exceeded Hop   :      5
Port:0/4  Up
  TxBPDUs      :      1092  RxBPDUs      :      1312
  Forward Transit Times:      3  Discard Message:      0
  Exceeded Hop   :      0
ChGr:32  Up
  TxBPDUs      :      2  RxBPDUs      :      15
  Forward Transit Times:      2  Discard Message:      0
  Exceeded Hop   :      0
>

```

## Display items in Example 2

Table 20-9: Display items for Multiple Spanning Tree statistics

Item	Meaning	Displayed information
MST Instance ID	Instance ID subject to MST	--
Topology ChangeTimes	Number of detecting topology changes	--
Port	Port number	--
ChGr	Channel group number	--
VL	Virtual link ID	--
Up	The port is in Up status.	Indicates that the port is in Up status. This indicates that the channel group in link aggregation is in the Up status. If a virtual link is used, this means that at least one virtual link port is in the Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. This indicates that the channel group in link aggregation is in the Down status. If a virtual link is used, this means that all virtual link ports are in the Down status.
TxBPDUs	Number of sent BPDUs	--
RxBPDUs	Number of received BPDUs	--
Forward Transit Times	Number of transitions to the forwarding state	--
RxDiscardsFrames	Number of discarded received BPDUs	-- (Displayed only for MST Instance ID:0)
Discard BPDUs by reason	Number of discarded received BPDUs	-- (Displayed only for MST Instance ID:0)
Timeout	Number of BPDUs whose valid time expired	Displays the number of received BPDUs whose valid time (which is set in the BPDUs) expired. (Displayed only for MST Instance ID:0)

Item	Meaning	Displayed information
Invalid	Number of invalid BPDUs	Displays the number of received BPDUs whose format is invalid (Displayed only for MST Instance ID:0). When the length of the configured BPDU is less than 35 octets When the length of the TCN BPDU is less than 4 octets When the length of the RST BPDU is less than 36 octets When the length of the MST BPDU is less than 35 octets When the Version 3 Length value of the MST BPDU is less than 64
Not Support	Number of unsupported BPDUs	Displays the number of received BPDUs that include unsupported parameters (Displayed only for MST Instance ID:0). When the BPDU type value is other than 0x00, 0x02, or 0x80
Other	Number of BPDUs discarded for another reason	Displays the number of discarded received BPDUs when PVST+ BPDUs are received or when BPDU discard has been configured. - When BPDU filtering has been configured - When the root guard functionality is operating (Displayed only for MST Instance ID:0) - When the port receives BPDUs that were sent from the port
Discard Message	MSTI configuration message when the received BPDUs are discarded	Displays the number of MSTI configuration messages when BPDU discard has set by the following functionality: - When the root guard functionality is set (Displayed only for MST instance IDs 1 to 4095.)
Ver3Length Invalid	Number of received BPDUs whose Version 3 Length value is invalid	Displays the number of received BPDUs whose Version 3 Length value is invalid. • When the value is less than 64 • When the value is 1089 or more • When the value is not a multiple of 16 (Displayed only for MST Instance ID:0)
Exceeded Hop	Number of discarded MST configuration messages whose remaining hop value is 0	--

## Impact on communication

None

## Response messages

*Table 20-10:* List of response messages for the show spanning-tree statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Spanning Tree program.	Communication with the Spanning Tree program failed.
No corresponding port information.	No port and channel group information exists as Spanning Tree information.
No corresponding Spanning Tree information.	The relevant Spanning Tree information does not exist.

**Notes**

None

---

## clear spanning-tree statistics

---

Clears statistics about Spanning Tree Protocols.

### Syntax

```
clear spanning-tree statistics [ {vlan [ <vlan id list> ] | single | mst [ instance
<mst instance id list> ] } [ port <port list> ] [channel-group-number <channel group
list>] [virtual-link <link id>]]
```

### Input mode

User mode and administrator mode

### Parameters

```
{vlan [ <vlan id list> ] | single | mst [ instance <mst instance id list> ]}
```

vlan

Clears PVST+ statistics.

<vlan id list>

Specify a list of VLAN IDs for which you want to clear PVST+ Spanning Tree statistics.

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

Operation when this parameter is omitted:

Statistics for all VLANs for which PVST+ is running are cleared.

single

Clears statistics about Spanning Tree Protocols.

mst

Clears statistics about Multiple Spanning Tree.

instance <mst instance id list>

Clears statistics about Multiple Spanning Tree for the MST instance IDs specified in list format. Specifiable values for MST instance ID are in the range from 0 to 4095.

If an MST instance ID of 0 is specified, the CIST statistics are also cleared.

Operation when this parameter is omitted:

All MST instances are subject to clearance.

port <port list>

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

channel-group-number <channel group list>

Clears Spanning Tree statistics for the channel groups specified in list format. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

virtual-link <link id>

Clears statistics about the Spanning Tree Protocols for the specified virtual link ID. Specifiable values for the virtual link ID are in the range from 1 to 250.

Operation when all parameters are omitted:

Statistics about all Spanning Tree Protocols are cleared.

## Operation when a stack configuration is used

This command is not supported.

## Example

*Figure 20-10:* Example of clearing the statistics for all Spanning Tree Protocols

```
> clear spanning-tree statistics
>
```

*Figure 20-11:* Example of clearing Single Spanning Tree statistics

```
> clear spanning-tree statistics single
>
```

*Figure 20-12:* Example of clearing Multiple Spanning Tree statistics

```
>clear spanning-tree statistics mst
>
```

## Display items

None

## Impact on communication

None

## Response messages

*Table 20-11:* List of response messages for the clear spanning-tree statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Spanning Tree program.	Communication with the Spanning Tree program failed.

## Notes

- Even if statistics are cleared, the value for the MIB information obtained by using SNMP is not cleared.  
To clear MIB information, use the `restart spanning-tree` command.
- If the configuration is deleted or added, the target statistics are cleared.

---

## clear spanning-tree detected-protocol

---

Forces recovery of STP compatible mode for Spanning Tree Protocols.

### Syntax

```
clear spanning-tree detected-protocol [ { vlan [ <vlan id list> ] | single | mst }
] [ port <port list> ] [ channel-group-number <channel group list> ]
```

### Input mode

User mode and administrator mode

### Parameters

{ vlan [ <vlan id list> ] | single | mst }

vlan

Forces recovery of STP compatible mode for PVST+.

<vlan id list>

Forces recovery of STP compatible mode for PVST+ for the VLAN IDs specified in list format.

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

Operation when this parameter is omitted:

All VLANs for which PVST+ is running are subject to a forced recovery of STP compatible mode.

single

Forces recovery of STP compatible mode for Single Spanning Tree.

mst

Forces recovery of STP compatible mode for Multiple Spanning Tree.

port <port list>

Forces recovery of STP compatible mode for the specified port number.

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

channel-group-number <channel group list>

Forces recovery of STP compatible mode for the channel groups specified in list format.

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

Operation when all parameters are omitted:

STP compatible mode is forcibly recovered for the ports of all Spanning Tree Protocols.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following shows an example of forcing recovery of STP compatible mode for Spanning Tree Protocols.

*Figure 20-13:* Example of forcibly recovering STP compatible mode for Spanning Tree Protocols

```
> clear spanning-tree detected-protocol
>
```

**Display items**

None

**Impact on communication**

None

**Response messages**

*Table 20-12:* List of response messages for the clear spanning-tree detected-protocol command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Spanning Tree program.	Communication with the Spanning Tree program failed.

**Notes**

This command is valid only for Rapid PVST+, rapid Spanning Tree Protocols, and Multiple Spanning Tree.

---

## show spanning-tree port-count

---

Displays the numbers handled by Spanning Tree Protocols.

### Syntax

```
show spanning-tree port-count [ {vlan | single | mst} ]
```

### Input mode

User mode and administrator mode

### Parameters

{vlan | single | mst}

vlan

Displays the numbers handled by PVST+.

single

Displays the numbers handled by Single Spanning Tree.

mst

Displays the numbers handled by Multiple Spanning Tree.

Operation when this parameter is omitted:

The numbers handled by PVST+, the numbers handled by Single Spanning Tree, and the numbers handled by Multiple Spanning Tree are displayed.

### Operation when a stack configuration is used

This command is not supported.

### Example 1

The following shows an example of displaying the numbers handled by PVST+.

*Figure 20-14:* Example of displaying the numbers handled by PVST+

```
> show spanning-tree port-count vlan
Date 20XX/04/14 12:00:00 UTC
PVST+   VLAN Counts:    5      VLAN Port Counts:    20      Tree Counts:    7
>
```

### Display items in Example 1

*Table 20-13:* Display items for the numbers handled by PVST+

Item	Meaning	Displayed information
PVST+ VLAN Counts	Number of VLANs	Number of VLANs for which PVST+ is running
VLAN Port Counts	Number of VLAN ports	Total number of ports configured for all VLANs subject to PVST+
Tree Counts	Number of PVST+ Spanning Tree Protocols	Number of VLANs subject to PVST+

### Example 2

The following shows an example of displaying the numbers handled by Single Spanning Tree.

*Figure 20-15:* Example of displaying the numbers handled by Single Spanning Tree

```
> show spanning-tree port-count single
Date 20XX/01/26 12:00:00 UTC
```

```
Single VLAN Counts: 16      VLAN Port Counts: 64
>
```

## Display items in Example 2

*Table 20-14:* Display items for the numbers handled by Single Spanning Tree

Item	Meaning	Displayed information
Single VLAN Counts	Number of VLANs	Number of VLANs subject to Single Spanning Tree
VLAN Port Counts	Number of VLAN ports	Total number of ports configured for all VLANs subject to Single Spanning Tree

## Example 3

The following shows an example of displaying the numbers handled by Multiple Spanning Tree.

*Figure 20-16:* Example of displaying the numbers handled by Multiple Spanning Tree

```
> show spanning-tree port-count mst
Date 20XX/01/26 12:00:00 UTC
CIST      VLAN Counts: 4073      VLAN Port Counts: 48
MST 1     VLAN Counts: 4         VLAN Port Counts: 12
MST 128   VLAN Counts: 10        VLAN Port Counts: 80
MST 1024  VLAN Counts: 8         VLAN Port Counts: 32
>
```

## Display items in Example 3

*Table 20-15:* Display items for the numbers handled by Multiple Spanning Tree

Item	Meaning	Displayed information
CIST VLAN Counts	Number of VLANs	Number of CIST instance VLANs
MST VLAN Counts	Number of VLANs	Number of MSTI instance VLANs
VLAN Port Counts	Number of VLAN ports	Total number of ports configured for the applicable instance VLANs among existing VLANs

## Impact on communication

None

## Response messages

*Table 20-16:* List of response messages for the show spanning-tree port-count command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Spanning Tree program.	Communication with the Spanning Tree program failed.
Spanning Tree is not configured.	The Spanning Tree Protocol has not been configured. Check the configuration.
Specified Spanning Tree is not configured.	The specified Spanning Tree Protocol has not been configured. Check the configuration.

## Notes

- The number of PVST+ and Single Spanning Tree VLANs does not include the number of VLANs in the `suspend` status. The total number of PVST+ Spanning Tree Protocol VLANs, including those in the `suspend` status, is displayed under `Tree Counts`.
- The number of VLAN ports for the PVST+, Single Spanning Tree, and Multiple Spanning

Tree does not include the following VLANs or ports:

- VLANs for which the `suspend` parameter is set by the `state` configuration command
- Ports for which VLAN tunneling is set
- Ports for which the BPDU filter functionality is not set when the BPDU guard functionality is used.
- Access ports for which the PortFast functionality and BPDU filter functionality are set

---

## restart spanning-tree

---

Restarts the Spanning Tree program.

### Syntax

```
restart spanning-tree [-f] [core-file]
```

### Input mode

User mode and administrator mode

### Parameters

-f

Restarts the Spanning Tree program without outputting any confirmation messages.

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:

After a restart confirmation message is output, the Spanning Tree program is restarted.

### Operation when a stack configuration is used

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

```
remote command {<switch no.> | all} restart spanning-tree [-f] [core-file]
```

### Example

*Figure 20-17: Example of restarting Spanning Tree Protocols*

```
> restart spanning-tree
Spanning Tree restart OK? (y/n): y
>
```

### Display items

None

### Impact on communication

Communication over the VLANs in which Spanning Tree Protocols are running stops until the calculation of the Spanning Tree topology finishes.

### Response messages

*Table 20-17: List of response messages for the restart spanning-tree command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Spanning Tree program failed to be restarted.	The command could not restart the Spanning Tree program. Re-execute the command.

## Notes

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

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

File name: `stpd.core`

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

- When this command is executed, the uplink redundancy program is also restarted.

---

## dump protocols spanning-tree

---

Outputs to a file detailed event trace information and control table information collected for Spanning Tree programs.

### Syntax

```
dump protocols spanning-tree
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

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

```
remote command {<switch no.> | all} dump protocols spanning-tree
```

### Example

*Figure 20-18:* Example of obtaining a Spanning Tree dump

```
> dump protocols spanning-tree
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 20-18:* List of response messages for the dump protocols spanning-tree command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Spanning Tree program.	Communication with the Spanning Tree program failed.
File open error.	An attempt to open or access a dump file failed.

### Notes

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

Location: `/usr/var/stp/`

Event trace information file: `stpd_trace.gz`

Control table information file: `stpd_dump.gz`

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



## Chapter

---

# 21. Ring Protocol

---

show axrp  
clear axrp  
clear axrp preempt-delay  
restart axrp  
dump protocols axrp

---

## show axrp

---

Displays Ring Protocol information.

### Syntax

```
show axrp [<ring id list>] [detail]
```

### Input mode

User mode and administrator mode

### Parameters

*<ring id list>*

Specify a list of ring IDs for which you want to display information. If you specify multiple ring IDs, you can specify a range.

[Specifying a range by using "-" or ","]

All rings defined by the range are specified. The specifiable values are from 1 to 65535.

*detail*

Displays detailed Ring Protocol information.

Operation when all parameters are omitted:

All summary information about the Ring Protocol is displayed.

### Operation when a stack configuration is used

This command is not supported.

### Example 1

The following shows an example of displaying summary information about the Ring Protocol.

*Figure 21-1: Example of displaying summary information about the Ring Protocol*

```
> show axrp
Date 20XX/01/26 12:00:00 UTC

Total Ring Counts:4

Ring ID:1
Name:RING#1
Oper State:enable           Mode:Master      Attribute:-

VLAN Group ID  Ring Port  Role/State           Ring Port  Role/State
1              0/1       primary/forwarding   0/2       secondary/blocking
2              0/1       secondary/blocking   0/2       primary/forwarding

Ring ID:2
Name:RING#2
Oper State:enable           Mode:Transit     Attribute:-

VLAN Group ID  Ring Port  Role/State           Ring Port  Role/State
1              1 (ChGr)  -/forwarding         2 (ChGr)   -/forwarding
2              1 (ChGr)  -/forwarding         2 (ChGr)   -/forwarding

Ring ID:3
Name:
Oper State:disable          Mode:-           Attribute : -

VLAN Group ID  Ring Port  Role/State           Ring Port  Role/State
1              -         -/-                  -         -/-
2              -         -/-                  -         -/-
```

```

Ring ID:4
Name:RING#4
Oper State:enable           Mode:Transit   Attribute:rft-ring-edge (1)
Shared Edge Port:0/3

VLAN Group ID  Ring Port  Role/State           Ring Port  Role/State
1              0/3       -/-                  0/4       -/forwarding
2              0/3       -/-                  0/4       -/forwarding
>

```

*Figure 21-2: Example of displaying summary information about the Ring Protocol for a specific ring ID*

```

> show axrp 1
Date 20XX/01/26 12:00:00 UTC

Total Ring Counts:1

Ring ID:1
Name:RING#1
Oper State:enable           Mode:Master   Attribute:-

VLAN Group ID  Ring Port  Role/State           Ring Port  Role/State
1              0/1       primary/forwarding    0/2       secondary/blocking
2              0/1       secondary/blocking     0/2       primary/forwarding
>

```

## Display items in Example 1

*Table 21-1: Description of displayed items (summary information about the Ring Protocol)*

Item	Meaning	Displayed information
Total Ring Counts	Number of rings	1 to 24
Ring ID	Ring ID	1 to 65535
Name	Ring identification name	--
Oper State	Whether the ring is enabled or disabled	enable: Enabled disable: Disabled Not Operating: Ring Protocol functionality is not operating for a reason such as invalid configuration (if all necessary configuration entries for using Ring Protocol functionality have not been set, a hyphen (-) is displayed).
Mode	Operating mode	Master: Master node Transit: Transit node
Attribute	In a multi-ring configuration, the attribute of the Switch in a shared-link non-monitoring ring	rft-ring: Master node in a shared-link non-monitoring ring rft-ring-edge (1): Terminal node having an edge node ID of 1 in a shared-link non-monitoring ring (both master and transit nodes can have this attribute) rft-ring-edge (2): Terminal node having an edge node ID of 2 in a shared-link non-monitoring ring (both master and transit nodes can have this attribute) -: Node that is neither a rft-ring node nor a rft-ring-edge node
Shared Edge Port	Port number on the shared-link side of the terminal node in a shared-link non-monitoring ring	Physical port number (NIF number/port number) or channel group number (ChGr) Note: This item is displayed only for the terminal nodes in a shared-link non-monitoring ring. However, if Not Operating or a hyphen (-) is displayed for Oper State, the value that has been set is displayed regardless of the node type.

Item	Meaning	Displayed information
Shared Port	Shared-link port number for the transit node on the shared link	Physical port number (NIF number/port number) or channel group number (ChGr) Note: This item is displayed only for transit nodes on a shared link. However, if <code>Not Operating</code> or a hyphen (-) is displayed for <code>Oper State</code> , the value that has been set is displayed regardless of the node type.
VLAN Group ID	Data transfer VLAN group ID	1 to 2
Ring Port	Ring port number	Physical port number (NIF number/port number) or channel group number (ChGr)
Role	The role of the ring port	primary: Primary port secondary: Secondary port Note: A hyphen (-) is displayed for nodes other than the master node on which Ring Protocol functionality is enabled.
State	Ring port state	Forwarding: Forwarding Blocking: Blocking down: The port or channel group is down. Note: If Ring Protocol functionality is not enabled, or if the port is a shared port in a shared-link non-monitoring ring, a hyphen (-) is displayed.

## Example 2

The following shows an example of displaying detailed Ring Protocol information.

*Figure 21-3: Example of displaying detailed Ring Protocol information*

```
> show axrp detail
Date 20XX/03/10 12:00:00 UTC

Total Ring Counts:4

Ring ID:1
Name:RING#1
Oper State:enable          Mode:Master      Attribute:-
Control VLAN ID:5          Ring State:normal
Health Check Interval      (msec):1000
Health Check Hold Time     (msec):3000
Preempt Delay Time         (sec):-
Flush Request Counts:3
Flush Request Transmit VLAN ID:12

VLAN Group ID:1
VLAN ID:6-10,12
Ring Port:0/1              Role:primary    State:forwarding
Ring Port:0/2              Role:secondary  State:blocking

VLAN Group ID:2
VLAN ID:16-20,22
Ring Port:0/1              Role:secondary  State:blocking
Ring Port:0/2              Role:primary    State:forwarding

Last Transition Time:20XX/10/05 10:00:00
Fault Counts      Recovery Counts      Total Flush Request Counts
1                  1                  12

Multi Fault Detection State:normal
Mode:monitoring   Backup Ring ID:4
Control VLAN ID:100
Multi Fault Detection Interval (msec):1000
Multi Fault Detection Hold Time (msec):3000
```

```

Ring ID:2
Name:RING#2
Oper State:enable           Mode:Transit   Attribute:-
Control VLAN ID:15
Forwarding Shift Time (sec):10
Last Forwarding:flush request receive

VLAN Group ID:1
VLAN ID:26-30,32
Ring Port:1 (ChGr)         Role:-           State:forwarding
Ring Port:2 (ChGr)         Role:-           State:forwarding

VLAN Group ID:2
VLAN ID:36-40,42
Ring Port:1 (ChGr)         Role:-           State:forwarding
Ring Port:2 (ChGr)         Role:-           State:forwarding

Ring ID:3
Name:
Oper State:disable          Mode:-           Attribute : -
Control VLAN ID:-

VLAN Group ID:1
VLAN ID:-
Ring Port:-                Role:-           State:-
Ring Port:-                Role:-           State:-

VLAN Group ID:2
VLAN ID:-
Ring Port:-                Role:-           State:-
Ring Port:-                Role:-           State:-

Ring ID:4
Name:RING#4
Oper State:enable           Mode:Transit   Attribute:rft-ring-edge(1)
Shared Edge Port:0/3
Control VLAN ID:45
Health Check Interval (msec):1000
Forwarding Shift Time (sec):10
Last Forwarding:flush request receive

VLAN Group ID:1
VLAN ID:46-50,52
Ring Port:0/3              Role:-           State:-
Ring Port:0/4              Role:-           State:forwarding

VLAN Group ID:2
VLAN ID:56-60,62
Ring Port:0/3              Role:-           State:-
Ring Port:0/4              Role:-           State:forwarding
>

```

## Display items in Example 2

Table 21-2: Description of displayed items (detailed Ring Protocol information)

Item	Meaning	Displayed information
Total Ring Counts	Number of rings	1 to 24
Ring ID	Ring ID	1 to 65535
Name	Ring identification name	--

Item	Meaning	Displayed information
Oper State	Whether the ring is enabled or disabled	enable: Enabled disable: Disabled Not Operating: Ring Protocol functionality is not operating for a reason such as invalid configuration (if all necessary configuration entries for using Ring Protocol functionality have not been set, a hyphen (-) is displayed).
Mode	Operating mode	Master: Master node Transit: Transit node
Attribute	In a multi-ring configuration, the attribute of the Switch in a shared-link non-monitoring ring	rift-ring: Master node in a shared-link non-monitoring ring rift-ring-edge (1): Terminal node having an edge node ID of 1 in a shared-link non-monitoring ring (both master and transit nodes can have this attribute) rift-ring-edge (2): Terminal node having an edge node ID of 2 in a shared-link non-monitoring ring (both master and transit nodes can have this attribute) -: Node that is neither a rift-ring node nor a rift-ring-edge node
Shared Edge Port	Port number on the shared-link side of the terminal node in a shared-link non-monitoring ring	Physical port number (NIF number/port number) or channel group number (ChGr) Note: This item is displayed only for the terminal nodes in a shared-link non-monitoring ring. However, if Not Operating or a hyphen (-) is displayed for Oper State, the value that has been set is displayed regardless of the node type.
Shared Port	Shared-link port number for the transit node on the shared link	Physical port number (NIF number/port number) or channel group number (ChGr) Note: This item is displayed only for transit nodes on a shared link. However, if Not Operating or a hyphen (-) is displayed for Oper State, the value that has been set is displayed regardless of the node type.
Control VLAN ID	Control VLAN ID	2 to 4094
Forwarding Delay Time	Timer value of the forwarding shift time for the control VLAN	1 to 65535 (seconds) (This item is displayed only for transit nodes.)
Ring State	Status of the ring	normal: Normal fault: A fault has occurred. preempt delay: Path switchbacks are suppressed. monitoring recovery: Recovery is being monitored. Note: This item is displayed only for the master node. However, if Ring Protocol functionality is not enabled, a hyphen (-) is displayed.
Health Check Interval	Value of the health-check frame sending interval timer	200 to 60000 (milliseconds) Note: This item is displayed for the master node and terminal nodes in a shared-link non-monitoring ring.
Health Check Hold Time	Time period during which a health-check frame is not received but the judgment that a failure occurred is suppressed	500 to 300000 (milliseconds) (This item is displayed only for the master node.)
Preempt Delay Time	Time required to complete a switchback operation that has been suppressed	1 to 3600 (seconds), or infinity. If a switchback operation has not been suppressed, a hyphen (-) is displayed. Note: This item is displayed only for the master node. However, this item is not displayed if no value has been set.

Item	Meaning	Displayed information
Flush Request Counts	Number of times a flush control frame was sent	1 to 10 (This item is displayed only for the master node.)
Flush Request Transmit VLAN ID	When a failure occurs in a ring or the failure is corrected, the ID of the VLAN from which neighboring-ring flush control frames are to be sent to the switches in the neighboring ring	1 to 4094 (This item is displayed only for the master node.)
Forwarding Shift Time	Time required to change the status of the data-forwarding VLAN for a ring port to Forwarding	1 to 65535 (seconds), or infinity. (This item is displayed only for transit nodes.)
Last Forwarding	Reason of why the ring port was set for forwarding lately	flush request receive: Flush control frames were received. forwarding shift time out: The forwarding shift time expired. (This item is displayed only for transit nodes.)
VLAN Group ID	Data transfer VLAN group ID	1 to 2
Ring Port	Ring port number	Physical port number (NIF number/port number) or channel group number (ChGr)
VLAN ID	Data transfer VLAN ID	1 to 4094
Role	The role of the ring port	primary: Primary port secondary: Secondary port Note: A hyphen (-) is displayed for nodes other than the master node on which Ring Protocol functionality is enabled.
State	Ring port state	Forwarding: Forwarding Blocking: Blocking down: The port or channel group is down. Note: If Ring Protocol functionality is not enabled, or if the port is a shared port in a shared-link non-monitoring ring, a hyphen (-) is displayed.
Last Transition Time	Time that the failure or recovery monitoring status changed last	yyyy/mm/dd hh:mm:ss UTC: Year, month, day, hour, minute, second, and time zone (This item is displayed only for the master node.)
Fault Counts	Number of times a fault was detected (statistics)	0 to 4294967295 (This item is displayed only for the master node.)
Recovery Counts	Number of times recovery was detected (statistics)	0 to 4294967295 (This item is displayed only for the master node.)
Total Flush Request Counts	Total number of times a flush control frame was sent (statistics)	0 to 4294967295 (This item is displayed only for the master node.)
Multi Fault Detection State	Multi-fault monitoring is enabled	normal: Normal fault: A fault has occurred. (This item is displayed if the multi-fault monitoring functionality is enabled. If a hyphen (-) is displayed, it means that either multi-fault monitoring has not yet started when the monitoring mode is monitoring or that the monitoring mode is transport.)

Item	Meaning	Displayed information
Mode	Multi-fault monitoring mode	monitoring: monitor-enable transport: transport-only (This item is displayed if the multi-fault monitoring functionality is enabled. - is displayed when this item is not set.)
Backup Ring ID	Backup ring ID	1 to 65535 (This item is displayed only when the monitoring mode is monitoring.)
Control VLAN ID	ID of the VLAN used for multi-fault monitoring	2 to 4094 (This item is displayed if the multi-fault monitoring VLAN is set. - is displayed when this item is not set.)
Multi Fault Detection Interval	Value of the multi-fault monitoring frame sending interval timer	500 to 60000 (milliseconds) (This item is displayed only when the monitoring mode is monitoring.)
Multi Fault Detection Hold Time	Time period during which a multi-fault detection frame is not received but the judgment that a multi-failure occurred is suppressed	1000 to 300000 (milliseconds) (This item is displayed only when the monitoring mode is monitoring.)

## Impact on communication

None

## Response messages

Table 21-3: List of response messages for the show axrp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Ring Protocol program.	Communication with the Ring Protocol program failed. Re-execute the command. If this message is output frequently, execute the <code>restart axrp</code> command to restart the Ring Protocol program.
Ring Protocol is initializing.	The Ring Protocol is performing initialization. Processing, such as loading configuration entries, has not been completed. Wait a while, and then re-execute the command.
Ring Protocol is not configured.	The Ring Protocol has not been configured. Check the configuration.
Specified Ring ID is not configured: <ring id>.	The specified ring ID has not been configured. <ring id>: Ring ID

## Notes

The counter values for statistical items do not increment when the upper limit is reached.

---

## clear axrp

---

Clears Ring Protocol statistics.

### Syntax

```
clear axrp [<ring id list>]
```

### Input mode

User mode and administrator mode

### Parameters

<ring id list>

Specify a list of ring IDs for which you want to clear all Ring Protocol statistics. If you specify multiple ring IDs, you can specify a range.

[Specifying a range by using "-" or ", "]

All rings defined by the range are specified. The specifiable values are from 1 to 65535.

Operation when all parameters are omitted:

All Ring Protocol statistics are cleared.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 21-4:* Example of clearing all Ring Protocol statistics

```
> clear axrp
>
```

*Figure 21-5:* Example of clearing all Ring Protocol statistics for a specific ring ID

```
> clear axrp 1
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 21-4:* List of response messages for the clear axrp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Ring Protocol program.	Communication with the Ring Protocol program failed. Re-execute the command. If this message is output frequently, execute the <code>restart axrp</code> command to restart the Ring Protocol program.
Ring Protocol is initializing.	The Ring Protocol is performing initialization. Processing, such as loading configuration entries, has not been completed. Wait a while, and then re-execute the command.

Message	Description
Ring Protocol is not configured.	The Ring Protocol has not been configured. Check the configuration.
Specified Ring ID is not configured:<ring id>.	The specified ring ID has not been configured. <ring id>: Ring ID

## Notes

- Even if statistics are cleared, the value for the MIB information obtained by using SNMP is not cleared.
- If the configuration is deleted or added, the target statistics are cleared.

---

## clear axrp preempt-delay

---

Clears the path switchback suppression status for the master node.

### Syntax

```
clear axrp preempt-delay <ring id> [-f]
```

### Input mode

User mode and administrator mode

### Parameters

<ring id>

Specify the ID of the ring whose path switchback suppression status you want to clear.

The specifiable values are from 1 to 65535.

-f

Clears the path switchback suppression status without outputting any messages.

Operation when this parameter is omitted:

A confirmation message is displayed.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 21-6:* Example of executing the clear axrp preempt-delay command

```
>clear axrp preempt-delay 1
Fault recovery process restore OK? (y/n) :y
>
```

*Figure 21-7:* Example of executing the clear axrp preempt-delay command (with the -f parameter specified)

```
>clear axrp preempt-delay 1 -f
>
```

### Display items

None

### Impact on communication

If this command is executed on a ring for which path switchback suppression is enabled, the suppression is disabled and a path switchback operation is performed. At this time, the VLANs that belong to the VLAN group for the ring become unable to receive frames temporarily.

### Response messages

*Table 21-5:* List of response messages for the clear axrp preempt-delay command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Ring Protocol program.	Communication with the Ring Protocol program failed. Re-execute the command. If this message is output frequently, execute the <code>restart axrp</code> command to restart the Ring Protocol program.

Message	Description
Ring Protocol is not configured.	The Ring Protocol has not been configured. Check the configuration.
Specified Ring ID is not configured:<ring id>.	The specified ring ID has not been configured. <ring id>: Ring ID
Specified Ring ID is not preempt delay state:<ring id>	Path switchback suppression is not enabled for the specified ring. <ring id>: Ring ID

## Notes

None

---

## restart axrp

---

Restarts a Ring Protocol program.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

-f

Restarts the Ring Protocol program without outputting any confirmation messages.

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:

After a restart confirmation message is output, the Ring Protocol program is restarted.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 21-8:* Example of restarting the Ring Protocol program

```
> restart axrp
axrp program restart OK? (y/n):y
>
```

*Figure 21-9:* Example of restarting the Ring Protocol program (when the -f parameter is specified)

```
> restart axrp -f
>
```

### Display items

None

### Impact on communication

The VLANs that belong to the VLAN group for the Ring Protocol become unable to receive frames.

### Response messages

*Table 21-6:* List of response messages for the restart axrp command

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

Message	Description
Ring Protocol doesn't seem to be running.	The Ring Protocol program is not running. Check the configuration.
Ring Protocol program failed to be restarted.	This command could not restart the Ring Protocol program. Re-execute the command.

## Notes

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

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

File name: `axrpd.core`

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

---

## dump protocols axrp

---

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

### Syntax

```
dump protocols axrp
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

This command is not supported.

### Example

The following example outputs a Ring Protocol dump.

*Figure 21-10:* Example of obtaining a Ring Protocol dump

```
> dump protocols axrp
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 21-7:* List of response messages for the dump protocols axrp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Ring Protocol program.	Communication with the Ring Protocol program failed. Re-execute the command. If this message is output frequently, execute the <code>restart axrp</code> command to restart the Ring Protocol program.
File open error.	An attempt to open or access a dump file failed.
Ring Protocol doesn't seem to be running.	The Ring Protocol program is not running. Check the configuration.

### Notes

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

Storage directory: `/usr/var/axrp/`

File name: `axrp_dump.gz`

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



## Chapter

---

# 22. IGMP/MLD Snooping

---

```
show igmp-snooping
clear igmp-snooping
show mld-snooping
clear mld-snooping
restart snooping
dump protocols snooping
```

---

## show igmp-snooping

---

Displays IGMP snooping information. The following information is displayed for each VLAN:

- Whether the querier functionality is set, the IGMP querier address, and multicast router ports
- Subscription multicast group information for each VLAN or port, and learned MAC addresses
- Statistics (number of IGMP packets sent and received)

### Syntax

```
show igmp-snooping [ <vlan id list> ]
show igmp-snooping { group [<ip address>] [<vlan id list>] | port <port list>
                    | channel-group-number <channel group list> }
show igmp-snooping statistics [<vlan id list>]
```

### Input mode

User mode and administrator mode

### Parameters

<vlan id list>

Specify a list of VLAN IDs for which you want to display IGMP snooping information.

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

Operation when this parameter is omitted:

IGMP snooping information for all VLANs is displayed.

{ group [<ip address>] [<vlan id list>] | port <port list> | channel-group-number <channel group list> }

group

Displays the subscription multicast group addresses for the VLANs.

ip address

Specify the multicast group IP address for which you want to display IGMP snooping information.

port <port list>

Displays the subscription multicast group addresses for the specified ports. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Displays the subscription multicast group addresses for the specified channel groups. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

statistics

Displays statistics.

### Operation when a stack configuration is used

This command is not supported.

### Example 1

*Figure 22-1: Example of displaying IGMP snooping information*

```

> show igmp-snooping
Date 20XX/04/10 15:20:00 UTC
VLAN counts: 2
VLAN: 100
  VRF: 2
  IP address: 192.168.11.20      Querier: enable
  IGMP querying system: 192.168.11.20
  Querier version: V3
  IPv4 Multicast routing: On
  Fast-leave: On
  Port(5): 0/1-5
  Mrouter-port: 0/1,0/3
  Group counts: 3
VLAN: 200
  IP address:      Querier: disable
  IGMP querying system:
  Querier version: V2
  IPv4 Multicast routing: Off
  Fast-leave: Off
  Port(4): 0/6-9
  Mrouter-port: 0/6
  Group counts: 0
>

> show igmp-snooping 100
Date 20XX/04/10 15:21:00 UTC
VLAN: 100
  VRF: 2
  IP address:192.168.11.20      Querier: enable
  IGMP querying system: 192.168.11.20
  Querier version: V3
  IPv4 Multicast routing: On
  Fast-leave: Off
  Port(5): 0/1-5
  Mrouter-port: 0/1,0/3
  Group counts: 3
>

```

## Display items in Example 1

Table 22-1: Items displayed for IGMP snooping information

Item	Meaning	Displayed information
VLAN counts	Number of VLANs on which IGMP snooping is enabled	--
VLAN	VLAN information	--
VRF [OS-L3SA]	VRF ID	This item is displayed only when VRF is assigned to the VLAN interface.
IP address	IP address	Blank: No IP address has been set.
Querier	Whether the querier functionality has been set	enable: The functionality has been set. disable: The functionality has not been set.
IGMP querying system	IGMP querier in the VLAN	Blank: There is no IGMP querier.
Querier version	IGMP version of the querier	v2: Version 2 v3: Version 3
IPv4 Multicast routing	Whether IPv4 multicast routing has been set for the VLAN	On: Multicast routing has been set. Off: Multicast routing has not been set.
Fast-leave	Whether IGMP instant leave has been set for the VLAN	On: The functionality has been set. Off: Not set.

Item	Meaning	Displayed information
Port(n)	Number of ports in the VLAN	<i>n</i> : Number of applicable ports
Mrouter-port	Multicast router ports	--
Group counts	Number of multicast groups in the VLAN	--

## Example 2

Figure 22-2: Example of displaying IGMP group information for each VLAN

```
> show igmp-snooping group
Date 20XX/01/15 15:20:00 UTC
Total Groups: 5
VLAN counts: 2
VLAN: 100 Group counts: 3 IPv4 Multicast routing: Off
  Group Address      MAC Address          Version  Mode
  224.10.10.10       0100.5e0a.0a0a       V2      -
    Port-list:0/1-3
  225.10.10.10       0100.5e0a.0a0a       V3      INCLUDE
    Port-list:0/1-2
  239.192.1.1        0100.5e40.0101       V2,V3   EXCLUDE
    Port-list:0/1
VLAN: 300 Group counts: 2 IPv4 Multicast routing: On
  Group Address      MAC Address          Version  Mode
  239.168.10.5       0100.5e28.0a05       -      -
    Port-list:0/4,0/6
  239.192.20.6       0100.5e40.1406       -      -
    Port-list:0/2-4
>
> show igmp-snooping group 100
Date 20XX/01/15 15:20:00 UTC
VLAN counts: 1
VLAN: 100 Group counts: 3 IPv4 Multicast routing: Off
  Group Address      MAC Address          Version  Mode
  224.10.10.10       0100.5e0a.0a0a       V2      -
    Port-list:0/1-3
  225.10.10.10       0100.5e0a.0a0a       V1,V2,V3 EXCLUDE
    Port-list:0/1-2
  239.192.1.1        0100.5e40.0101       V1,V2   -
    Port-list:0/1
>
> show igmp-snooping group 224.10.10.10
Date 20XX/01/15 15:20:00 UTC
Total Groups: 2
VLAN counts: 2
VLAN: 100 Group counts: 1 IPv4 Multicast routing: Off
  Group Address      MAC Address          Version  Mode
  224.10.10.10       0100.5e0a.0a0a       V2      -
    Port-list:0/1-3
VLAN: 300 Group counts: 1 IPv4 Multicast routing: On
  Group Address      MAC Address          Version  Mode
  224.10.10.10       0100.5e0a.0a0a       -      -
    Port-list:0/4,0/6
>
> show igmp-snooping group 224.10.10.10 100
Date 20XX/01/15 15:20:00 UTC
VLAN counts: 1
VLAN: 100 Group counts: 1 IPv4 Multicast routing: Off
  Group Address      MAC Address          Version  Mode
  224.10.10.10       0100.5e0a.0a0a       V2      -
    Port-list:0/1-3
>
```

## Display items in Example 2

Table 22-2: Items displayed for IGMP group information for each VLAN

Item	Meaning	Displayed information
Total Groups	Number of participating groups on the device	--
VLAN counts	Number of VLANs on which IGMP snooping is enabled	--
VLAN	VLAN information	--
Group counts	Number of subscription multicast groups in the VLAN	--
IPv4 Multicast routing	Whether IPv4 multicast routing has been set for the VLAN	On: Multicast routing has been set. Off: Multicast routing has not been set.
Group Address	Subscription group addresses	--
MAC Address	Learned MAC addresses	--
Version	IGMP version information	V1: IGMP version 1 V2: IGMP version 2 V3: IGMP version 3 If IPv4 Multicast routing is On, a hyphen (-) is displayed. In this case, to check the IGMP version information, use the <code>show ip igmp group</code> command. The displayed information is refreshed when an IGMP General Query message is sent or received, and when an IGMP Report message (subscription request) is received.
Mode	Group mode	INCLUDE: INCLUDE mode EXCLUDE: EXCLUDE mode If the IGMP version information does not include V3 or if IPv4 Multicast routing is On, - is displayed. If IPv4 Multicast routing is On, to check the group mode, use the <code>show ip igmp group</code> command. The displayed information is refreshed when an IGMP General Query message is sent or received, and when an IGMP Report message (subscription request) is received.
Port-list	Relay port number (NIF number/port number)	--

## Example 3

Figure 22-3: Example of displaying IGMP group information for each port

```
> show igmp-snooping port 0/1
Date 20XX/05/15 15:20:00 UTC
Port 0/1 VLAN counts: 2
  VLAN: 100 Group counts: 2
    Group Address    Last Reporter    Uptime    Expires
    224.10.10.10     192.168.1.3     00:10     04:10
    239.192.1.1      192.168.1.3     02:10     03:00
  VLAN: 150 Group counts: 1
    Group Address    Last Reporter    Uptime    Expires
    239.10.120.1     192.168.15.10   01:10     02:30
>
```

### Display items in Example 3

Table 22-3: Items displayed for IGMP group information for each port

Item	Meaning	Displayed information
Port	Applicable port in the VLAN	--
VLAN counts	Number of VLANs to which the specified port belongs	--
VLAN	VLAN information	--
Group counts	Number of subscription multicast groups for the specified port	--
Group Address	Subscription multicast group addresses	--
Last Reporter	IP address that last subscribed to the group	--
Uptime	Time elapsed since the group information was generated	xx:yy xx (minutes), yy (seconds) 1hour, 2hours, . . . are displayed if the time is 60 minutes or more. However, 1day, 2days, . . . are displayed if the time is 24 hours or more.
Expires	Group information aging (remaining time)	xx:yy xx (minutes), yy (seconds)

### Example 4

Figure 22-4: Example of displaying IGMP snooping statistics

```
> show igmp-snooping statistics
Date 20XX/01/26 15:20:00 UTC
VLAN: 100
  Port 0/1  Rx:  Query (V2)           14353      Tx:  Query (V2)           0
                Query (V3)             71          Query (V3)           29
                Report (V1)             15
                Report (V2)            271
                Report (V3)             36
                Leave                   137
                Error                    14
  Port 0/2  Rx:  Query (V2)             0      Tx:  Query (V2)           31
                Query (V3)             12          Query (V3)           42
                Report (V1)             0
                Report (V2)            78
                Report (V3)            24
                Leave                   28
                Error                    0
>
```

### Display items in Example 4

Table 22-4: Items displayed for IGMP snooping statistics

Item	Meaning	Displayed information
VLAN	VLAN information	--
Port	Applicable port in the VLAN	--
Rx	Number of received IGMP packets	--
Query(V2)	IGMP Version 2 Query messages	--
Query(V3)	IGMP Version 3 Query messages	--

Item	Meaning	Displayed information
Tx	Number of sent IGMP packets.	--
Report(V1)	IGMP Version 1 Report messages	--
Report(V2)	IGMP Version 2 Report messages	--
Report(V3)	IGMP Version 3 Report messages	--
Leave	Leave messages	--
Error	Error packets	--

## Impact on communication

None

## Response messages

Table 22-5: List of response messages for the show igmp-snooping command

Message	Description
<command name> connection failed to snoopd.	Command execution failed because the IGMP or MLD snooping program had not been started. If this message is output when IGMP snooping is enabled, wait for the IGMP or MLD snooping program to be restarted, and then re-execute the command. <command name>: Name of the entered command
<command name>IGMP snooping not active.	IGMP snooping is not running. <command name>: Name of the entered command
No operational Port.	The ports specified in <port list> did not include active ones.
No operational VLAN.	There are no available VLANs.
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: write: Write error during socket communication read: Read error during socket communication select: Select function error during socket communication

## Notes

None

---

## clear igmp-snooping

---

Clears IGMP snooping information.

### Syntax

```
clear igmp-snooping { all | group [ <vlan id list> ] | statistics
                    [ <vlan id list> ] } [ -f ]
```

### Input mode

User mode and administrator mode

### Parameters

all

Clears all information.

group

Clears the learned MAC address information (group information).

<vlan id list>

Specify a list of VLAN IDs for which you want to clear IGMP snooping information.

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

Operation when this parameter is omitted:

IGMP snooping information for all VLANs is cleared.

statistics

Clears the statistics.

-f

Clears statistics without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

### Operation when a stack configuration is used

This command is not supported.

### Example

None

### Display items

None

### Impact on communication

Note that when the `clear igmp-snooping all` or `clear igmp-snooping group` command is executed, multicast communication temporarily stops.

## Response messages

Table 22-6: List of response messages for the clear igmp-snooping command

Message	Description
<command name> connection failed to snoopd.	Command execution failed because the IGMP or MLD snooping program had not been started. If this message is output when IGMP or MLD snooping is enabled, wait for the IGMP or MLD snooping program to be restarted, and then re-execute the command. <command name>: Name of the entered command
<command name>IGMP snooping not active.	IGMP snooping is not running. <command name>: Name of the entered command
No operational VLAN.	There are no available VLANs.
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: write: Write error during socket communication read: Read error during socket communication select: Select function error during socket communication

## Notes

None

---

## show mld-snooping

---

Displays MLD snooping information. The following information is displayed for each VLAN:

- Whether the querier functionality is set, the MLD querier address, and the multicast router ports
- Subscription multicast group information for each VLAN or port, and learned MAC addresses
- Statistics (number of MLD packets sent and received)

### Syntax

```
show mld-snooping [ <vlan id list> ]
show mld-snooping { group [<ipv6 address>] [<vlan id list>] | port <port list>
                    | channel-group-number <channel group list> }
show mld-snooping statistics [<vlan id list>]
```

### Input mode

User mode and administrator mode

### Parameters

<vlan id list>

Displays information about MLD snooping for the VLAN IDs specified in list format.

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

Operation when this parameter is omitted:

MLD snooping information for all VLANs is displayed.

{ group [<ipv6 address>] [<vlan id list>] | port <port list> | channel-group-number <channel group list> }

group

Displays the subscription multicast group addresses for the VLANs.

ipv6 address

Specify the multicast group IP address for which you want to display MLD snooping information.

port <port list>

Displays the subscription multicast group addresses for the specified ports. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Displays the subscription multicast group addresses for the specified channel groups. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

statistics

Displays statistics.

### Operation when a stack configuration is used

This command is not supported.

## Example 1

Figure 22-5: Example of displaying MLD snooping information

```
> show mld-snooping
Date 20XX/04/10 15:20:00 UTC
VLAN counts: 2
VLAN: 100
  VRF: 2
  IP Address: fe80::b1 Querier: enable
  MLD querying system: fe80::b1
  Querier version: V2
  IPv6 Multicast routing: On
  Port(5): 0/1-5
  Mrouter-port: 0/1,0/3
  Group counts: 3
VLAN: 200
  IP Address: Querier: disable
  MLD querying system:
  Querier version: V1
  IPv6 Multicast routing: Off
  Port(4): 0/6-9
  Mrouter-port: 0/6
  Group counts: 0
>

> show mld-snooping 100
Date 20XX/04/10 15:21:00 UTC
VLAN: 100
  IP Address: fe80::b1 Querier: enable
  MLD querying system: fe80::b1
  Querier version: V2
  IPv6 Multicast routing: On
  Port(5): 0/1-5
  Mrouter-port: 0/1,0/3
  Group counts: 3
>
```

## Display items in Example 1

Table 22-7: Items displayed for MLD snooping information

Item	Meaning	Displayed information
VLAN counts	Number of VLANs on which MLD snooping is enabled	--
VLAN	VLAN information	--
VRF [OS-L3SA]	VRF ID	This item is displayed only when VRF is assigned to the VLAN interface.
IP Address	IP address	Blank: No IP address has been set.
Querier	Whether the querier functionality has been set	enable: The functionality has been set. disable: The functionality has not been set.
MLD querying system	MLD querier in the VLAN	Blank: There is no MLD querier.
Querier version	MLD version of the querier	V1: Version1 V2: Version2
IPv6 Multicast routing	Whether IPv6 multicast routing has been set for the VLAN	On: Multicast routing has been set. Off: Multicast routing has not been set.
Port(n)	Number of ports in the VLAN	n: Number of applicable ports
Mrouter-port	Multicast router ports	--

Item	Meaning	Displayed information
Group counts	Number of subscription multicast groups in the VLAN	--

## Example 2

Figure 22-6: Example of displaying MLD group information for each VLAN

```
> show mld-snooping group
Date 20XX/01/15 15:20:00 UTC
Total Groups: 3
VLAN counts: 2
VLAN: 100 Group counts: 2 IPv6 Multicast routing: Off
  Group Address      MAC Address      Version  Mode
  ff35::1           3333:0000:0001   V1       -
  Port-list:0/1-3
  ff35::2           3333:0000:0002   V2       EXCLUDE
  Port-list:0/1-2
VLAN: 300 Group counts: 1 IPv6 Multicast routing: On
  Group Address      MAC Address      Version  Mode
  ff35::3           3333:0000:0003   -        -
  Port-list:0/4,0/6
>
> show mld-snooping group 100
Date 20XX/01/15 15:20:00 UTC
VLAN counts: 1
VLAN: 100 Group counts: 2 IPv6 Multicast routing: Off
  Group Address      MAC Address      Version  Mode
  ff35::1           3333:0000:0001   V1,V2    EXCLUDE
  Port-list:0/1-3
  ff35::2           3333:0000:0002   V2       EXCLUDE
  Port-list:0/1-2
>
> show mld-snooping group ff35::1
Date 20XX/01/15 15:20:00 UTC
Total Groups: 2
VLAN counts: 2
VLAN: 100 Group counts: 1 IPv6 Multicast routing: Off
  Group Address      MAC Address      Version  Mode
  ff35::1           3333:0000:0001   V1       -
  Port-list:0/1-3
VLAN: 300 Group counts: 1 IPv6 Multicast routing: On
  Group Address      MAC Address      Version  Mode
  ff35::1           3333:0000:0001   -        -
  Port-list:0/4,0/6
>
> show mld-snooping group ff35::1 100
Date 20XX/01/15 15:20:00 UTC
VLAN counts: 1
VLAN: 100 Group counts: 1 IPv6 Multicast routing: Off
  Group Address      MAC Address      Version  Mode
  ff35::1           3333:0000:0001   V1,V2    EXCLUDE
  Port-list:0/1-3
```

## Display items in Example 2

Table 22-8: Items displayed for MLD group information for each VLAN

Item	Meaning	Displayed information
Total Groups	Number of participating groups on the device	--
VLAN counts	Number of VLANs on which MLD snooping is enabled	--
VLAN	VLAN information	--

Item	Meaning	Displayed information
Group counts	Number of subscription multicast groups in the VLAN	--
IPv6 Multicast routing	Whether IPv6 multicast routing has been set for the VLAN	On: Multicast routing has been set. Off: Multicast routing has not been set.
Group Address	Subscription group addresses	--
MAC Address	Learned MAC addresses	--
Version	MLD version information	V1: MLD version 1 V2: MLD version 2 If IPv6 Multicast routing is On, a hyphen (-) is displayed. In this case, to check the MLD version information, use the show ipv6 mld group command. The displayed information is refreshed when an MLD General Query message is sent or received, and when an MLD Report message (subscription request) is received.
Mode	Group mode	INCLUDE: INCLUDE mode EXCLUDE: EXCLUDE mode If the MLD version information is V1 or if IPv6 Multicast routing is On, - is displayed. If IPv6 Multicast routing is On, to check the group mode, use the show ipv6 mld group command. The displayed information is refreshed when an MLD General Query message is sent or received, and when an MLD Report message (subscription request) is received.
Port-list	Relay port number (NIF number/port number)	--

### Example 3

Figure 22-7: Example of displaying MLD group information for each port

```
> show mld-snooping port 0/1
Date 20XX/05/15 15:20:00 UTC
Port 0/1 VLAN counts: 1
VLAN: 100 Group counts: 2
  Group Address      Last Reporter      Uptime      Expires
ff35::2             fe80::b1           00:10       04:10
ff35::3             fe80::b2           02:10       03:00
>
```

### Display items in Example 3

Table 22-9: Items displayed for MLD group information for each port

Item	Meaning	Displayed information
Port	Applicable port in the VLAN	--
VLAN counts	Number of VLANs to which the specified port belongs	--
VLAN	VLAN information	--
Group counts	Number of subscription multicast groups for the specified port	--

Item	Meaning	Displayed information
Group Address	Subscription multicast group addresses	--
Last Reporter	IP address that last subscribed to the group	--
Uptime	Time elapsed since the group information was generated	<i>xx:yy</i> <i>xx</i> (minutes), <i>yy</i> (seconds) 1hour, 2hours, . . . are displayed if the time is 60 minutes or more. However, 1day, 2days, . . . are displayed if the time is 24 hours or more.
Expires	Group information aging (remaining time)	<i>xx:yy</i> <i>xx</i> (minutes), <i>yy</i> (seconds)

## Example 4

Figure 22-8: Example of displaying MLD snooping statistics

```
> show mld-snooping statistics
Date 20XX/05/15 15:20:00 UTC
VLAN: 100
Port 0/1  Rx:  Query (V1)           22      Tx:  Query (V1)       233
              Query (V2)           12      Query (V2)       123
              Report (V1)          32
              Report (V2)          15
              Done                  28
              Error                  0
Port 0/2  Rx:  Query (V1)           32      Tx:  Query (V1)       234
              Query (V2)           19      Query (V2)       115
              Report (V1)          48
              Report (V2)          26
              Done                  45
              Error                  1
```

## Display items in Example 4

Table 22-10: Items displayed for MLD snooping statistics

Item	Meaning	Displayed information
VLAN	VLAN information	--
Port	Applicable port in the VLAN	--
Rx	Number of received MLD packets	--
Tx	Number of sent MLD packets.	--
Query(V1)	MLD Version 1 Query messages	--
Query(V2)	MLD Version 2 Query messages	--
Report(V1)	MLD Version 1 Report messages	--
Report(V2)	MLD Version 2 Report messages	--
Done	Done messages	--
Error	Error packets	--

## Impact on communication

None

## Response messages

Table 22-11: List of response messages for the show mld-snooping command

Message	Description
<command name> connection failed to snoopd.	Command execution failed because the IGMP or MLD snooping program had not been started. If this message is output when MLD snooping is enabled, wait for the IGMP or MLD snooping program to be restarted, and then re-execute the command. <command name>: Name of the entered command
<command name>MLD snooping not active.	MLD snooping is not operating. <command name>: Name of the entered command
No operational Port.	The ports specified in <port list> did not include active ones.
No operational VLAN.	There are no available VLANs.
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: write: Write error during socket communication read: Read error during socket communication select: Select function error during socket communication

## Notes

None

---

## clear mld-snooping

---

Clears MLD snooping information.

### Syntax

```
clear mld-snooping { all | group [ <vlan id list> ] | statistics
                    [ <vlan id list> ] } [ -f ]
```

### Input mode

User mode and administrator mode

### Parameters

all

Clears all information.

group

Clears the learned MAC address information (group information).

<vlan id list>

Specify a list of VLAN IDs for which you want to clear MLD snooping information.

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

Operation when this parameter is omitted:

MLD snooping information for all VLANs is cleared.

statistics

Clears the statistics.

-f

Clears statistics without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

### Operation when a stack configuration is used

This command is not supported.

### Example and display items

None

### Impact on communication

Note that when the `clear mld-snooping all` or `clear mld-snooping group` command is executed, multicast communication temporarily stops.

## Response messages

Table 22-12: List of response messages for the clear mld-snooping command

Message	Description
<command name> connection failed to snoopd.	Command execution failed because the IGMP or MLD snooping program had not been started. If this message is output when IGMP or MLD snooping is enabled, wait for the IGMP or MLD snooping program to be restarted, and then re-execute the command. <command name>: Name of the entered command
<command name>MLD snooping not active.	MLD snooping is not operating. <command name>: Name of the entered command
No operational VLAN.	There are no available VLANs.
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: write: Write error during socket communication read: Read error during socket communication select: Select function error during socket communication

## Notes

None

---

## restart snooping

---

Restarts the IGMP or MLD snooping program.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

-f

Restarts the snooping program without outputting any confirmation messages.

Operation when this parameter is omitted:

A confirmation message is displayed.

core-file

Outputs the snooping program's core file when restarting the program.

Operation when this parameter is omitted:

A core file is not output.

Operation when all parameters are omitted:

After a restart confirmation message is output, the snooping program is restarted.

### Operation when a stack configuration is used

This command is not supported.

### Example

None

### Display items

None

### Impact on communication

After the snooping program has been restarted, multicast communication stops until multicast groups are learned again.

### Response messages

Table 22-13: List of response messages for the restart snooping command

Message	Description
<command name> connection failed to snoopd.	Command execution failed because the IGMP or MLD snooping program had not been started. If this message is output when IGMP or MLD snooping is enabled, wait for the IGMP or MLD snooping program to be restarted, and then re-execute the command. <command name>: Name of the entered command
pid file <file name> mangled!	The PID file for the IGMP or MLD snooping program is corrupted. <file name>: PID file name

Message	Description
pid in file <i>&lt;file name&gt;</i> unreasonably small ( <i>&lt;pid&gt;</i> )	The PID file for the IGMP or MLD snooping program is corrupted. <i>&lt;file name&gt;</i> : PID file name <i>&lt;pid&gt;</i> : Process ID
Program error occurred: <i>&lt;error message&gt;</i>	A program error occurred. Re-execute the command. <i>&lt;error message&gt;</i> : write: Write error during socket communication read: Read error during socket communication select: Select function error during socket communication
snoopd failed to terminate.	The <code>restart snooping</code> command could not restart the IGMP or MLD snooping program. Re-execute the command.
snoopd restarted after termination: old pid <i>&lt;pid&gt;</i> , new pid <i>&lt;pid&gt;</i>	Command execution failed because the PID was changed during execution of the <code>restart snooping</code> command. The IGMP or MLD snooping program might be restarted automatically. If necessary, wait until the program is restarted, and then re-execute the command. <i>&lt;pid&gt;</i> : Process ID
snoopd signaled but still running, waiting 6 seconds more.	The IGMP or MLD snooping program is being restarted by using the <code>restart snooping</code> command. Wait a while.
snoopd still running, sending KILL signal.	The Kill signal is being sent to the IGMP or MLD snooping program so that the program can be restarted by using the <code>restart snooping</code> command. Wait a while.
snoopd terminated.	The IGMP or MLD snooping program was stopped by the <code>restart snooping</code> command. The program will restart automatically. Wait a while.

## Notes

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

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

File name: `snoopd.core`

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

---

## dump protocols snooping

---

Exports the detailed event trace information and control table information for the IGMP or MLD snooping program to a file.

### Syntax

```
dump protocols snooping
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

This command is not supported.

### Example

None

### Impact on communication

None

### Response messages

Table 22-14: List of response messages for the dump protocols snooping command

Message	Description
pid file <file name> mangled!	The PID file for the IGMP or MLD snooping program is corrupted. <file name>: PID file name
pid in file <file name> unreasonably small (<pid>)	The PID file for the IGMP or MLD snooping program is corrupted. <file name>: PID file name <pid>: Process ID
Program error occurred: <error message>	A program error occurred. Re-execute the command. <error message>: write: Write error during socket communication read: Read error during socket communication select: Select function error during socket communication
snoopd doesn't seem to be running.	Command execution failed because the IGMP or MLD snooping program had not been started. If this message is output when IGMP or MLD snooping is enabled, wait for the IGMP or MLD snooping program to be restarted, and then re-execute the command.

### Notes

The following shows the output files for the Switch and the directory to which the files are output.

Directory: /usr/var/mrp/

Dump information file: snoopd\_dump.gz

Trace information file: snoopd\_trace

If the file has already been output, the existing file is unconditionally overwritten. If the existing

file is necessary, back it up before executing the command.



## Chapter

---

# 23. Filters

---

show access-filter  
clear access-filter

---

## show access-filter

---

Displays the filter conditions applied on the Ethernet interface or VLAN interface by the access group commands (`ip access-group`, `ipv6 traffic-filter`, and `mac access-group`), the number of packets that met the filter conditions, and the number of packets discarded because they did not match any filter conditions in the access list.

### Syntax

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

### Input mode

User mode and administrator mode

### Parameters

{ <switch no.> / <nif no.> / <port no.> | interface vlan <vlan id> } [ { <access list number> | <access list name> } ]

<switch no.> / <nif no.> / <port no.>

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

interface vlan <vlan id>

Displays statistics for the specified VLAN interface.

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

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

*access list number*: Access list number

*access list name*: Access list name

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.

Operation when this parameter is omitted:

Displays statistics for all interfaces.

{ in | out }

*in*: Inbound (Specifies the receiving side)

*out*: Outbound (Specifies the sending side)

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

Operation when this parameter is omitted:

Displays statistics for the receiving side and the sending side of the specified interface.

### Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the `remote command` command.

```

remote command { <switch no.> | all } show access-filter
remote command <switch no.> show access-filter <switch no.>/<nif no.>/<port no.> [ {
<access list number> | <access list name> } ] [ { in | out } ]
remote command { <switch no.> | all } show access-filter interface vlan <vlan id>
[ { <access list number> | <access list name> } ] [ { in | out } ]

```

## Example

*Figure 23-1: Result of displaying the extended MAC access list*

```

> show access-filter 1/0/3 only-appletalk
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/3 in
Extended MAC access-list:only-appletalk
    remark "permit only appletalk"
    permit any any appletalk(0x809b)
        matched packets      : 74699826
    permit any any 0x80f3
        matched packets      : 718235
    implicitly denied packets: 2698
>

```

*Figure 23-2: Result of displaying the standard IPv4 access list*

```

> show access-filter 1/0/7 12
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/7 in
Standard IP access-list: 12
    remark "permit only host pc"
    permit host 10.10.10.1
        matched packets      : 74699826
    permit host 10.10.10.254
        matched packets      : 264176
    implicitly denied packets: 2698
>

```

*Figure 23-3: Result of displaying the extended IPv4 access list*

```

> show access-filter 1/0/11 128
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/11 in
Extended IP access-list: 128
    remark "permit only http server"
    permit tcp(6) any host 10.10.10.2 eq http(80)
        matched packets      : 74699826
    implicitly denied packets: 2698
>

```

*Figure 23-4: Result of displaying the IPv6 access list*

```

> show access-filter 1/0/15 telnet-server
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/15 in
IPv6 access-list:telnet-server
    remark "permit only telnet server"
    permit ipv6(41) any host 3ffe:501:811:ff00::1
        matched packets      : 74699826
    implicitly denied packets: 2698
>

```

*Figure 23-5: Result of displaying information when the access list ID is omitted*

```

> show access-filter 1/0/19
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/19 in
Standard IP access-list:pc-a1024
    remark "permit only pc-a1024"
    permit host 192.168.1.254
        matched packets      : 74699826
    implicitly denied packets: 2698

```

```
IPv6 access-list:smtp-server
  remark "permit only smtp server"
  permit ipv6(41) any host 3ffe:501:811:ff00::1
    matched packets      : 74699826
  implicitly denied packets: 2698
>
```

*Figure 23-6: Result of displaying information when In or Out is omitted*

```
> show access-filter interface vlan 1500
Date 20XX/09/01 12:00:00 UTC
Using Interface:vlan 1500 in
Standard IP access-list:pc-a1024
  remark "permit only pc-a1024"
  permit host 192.168.1.254
    matched packets      : 74699826
  implicitly denied packets: 2698
IPv6 access-list:only-smtp
  remark "permit only smtp ipv6"
  permit ipv6(41) any host 3ffe:501:811:ff00::1 eq smtp(25)
    matched packets      : 74699826
  implicitly denied packets: 2698

Using Interface:vlan 1500 out
Extended IP access-list:only-ssh
  remark "permit only ssh"
  permit tcp(6) any any eq ssh(22)
    matched packets      : 74699826
  implicitly denied packets: 2698
>
```

*Figure 23-7: Result of displaying information when all parameters are omitted*

```
> show access-filter
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/7 in
Standard IP access-list: 12
  remark "permit only host pc"
  permit host 10.10.10.1
    matched packets      : 74699826
  permit host 10.10.10.254
    matched packets      : 264176
  implicitly denied packets: 2698

Using Port:1/0/11 in
Extended IP access-list: 128
  remark "permit only http server"
  permit tcp(6) any host 10.10.10.2 eq http(80)
    matched packets      : 74699826
  implicitly denied packets: 2698

Using Port:1/0/15 in
IPv6 access-list:telnet-server
  remark "permit only telnet server"
  permit ipv6(41) any host 3ffe:501:811:ff00::1
    matched packets      : 74699826
  implicitly denied packets: 2698

Using Port:1/0/19 in
Standard IP access-list:pc-a1024
  remark "permit only pc-a1024"
  permit host 192.168.1.254
    matched packets      : 74699826
  implicitly denied packets: 2698
IPv6 access-list:smtp-server
  remark "permit only smtp server"
  permit ipv6(41) any host 3ffe:501:811:ff00::1
    matched packets      : 74699826
  implicitly denied packets: 2698
```

&gt;

## Display items

Display items of statistics for the access list applied to an interface by using an access group command are described below.

```
> show access-filter 1/0/7 12
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/7 in
Standard IP access-list: 12
  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
```

&gt;

Table 23-1: Statistical items for the access list

Item	Displayed information	
	Detailed information	Meaning
Interface information	Using Port:<switch no.>/<nif no.>/<port no.> in	Information about an Ethernet interface to which an access list has been applied on the inbound side
	Using Port:<switch no.>/<nif no.>/<port no.> out	Information about an Ethernet interface to which an access list has been applied on the outbound side
	Using Interface:vlan <vlan id> in	Information about a VLAN interface to which an access list has been applied on the inbound side
	Using Interface:vlan <vlan id> out	Information about a VLAN interface to which an access list has been applied on the outbound side
Access list ID	Extended MAC access-list:<access list name>	Extended MAC access list ID
	Standard IP access-list: { <access list number>   <access list name> }	Standard IPv4 access list ID
	Extended IP access-list: { <access list number>   <access list name> }	Extended IPv4 access list ID
	IPv6 access-list:<access list name>	IPv6 access list ID
Access list information	Displays supplementary information and filter conditions set by access list commands (for details, see 19. Access Lists in the manual <i>Configuration Command Reference Vol. 1 For Version 11.10</i> ).	
Statistics	matched packets:<packets>	Number of packets that meet the filter conditions in the access list
	implicitly denied packets:<packets>	Number of packets that were discarded because they did not meet any of the filter conditions in the access list

## Impact on communication

None

## Response messages

Table 23-2: List of response messages for the show access-filter command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
Illegal Port -- <i>&lt;port no.&gt;</i> .	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <i>&lt;port no.&gt;</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.
No such Switch <i>&lt;switch no.&gt;</i> .	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. <i>&lt;switch no.&gt;</i> : Switch number

## Notes

To check the route information for policy-based routing, execute the `show ip cache policy` command. [OS-L3SA]

---

## 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 <switch no.>/<nif no.>/<port no.>
                    [ { <access list number> | <access list name> } ] [ { in | out } ]
clear access-filter interface vlan <vlan id>
                    [ { <access list number> | <access list name> } ] [ { in | out } ]
```

### Input mode

User mode and administrator mode

### Parameters

{ <switch no.>/<nif no.>/<port no.> | interface vlan <vlan id> } [ { <access list number> | <access list name> } ]

<switch no.>/<nif no.>/<port no.>

Clears statistics for the specified Ethernet interface. For the specifiable range of <switch no.>, <nif no.>, and <port no.> values, see *Specifiable values for parameters*.

interface vlan <vlan id>

Clears statistics for the specified VLAN interface.

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.

Operation when this parameter is omitted:

Clears the statistics for all interfaces to zero.

{ 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.

### Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the `remote command` command.

```
remote command { <switch no.> | all } clear access-filter
```

```
remote command <switch no.> clear access-filter <switch no.>/<nif no.>/<port no.> [
{ <access list number> | <access list name> } ] [ { in | out } ]
remote command { <switch no.> | all } clear access-filter interface vlan <vlan id>
[ { <access list number> | <access list name> } ] [ { in | out } ]
```

## Example

Figure 23-8: Result of resetting the standard IPv4 access list statistics

```
> clear access-filter 1/0/7 12
Date 20XX/07/14 12:00:00 UTC
>
```

## Display items

None

## Impact on communication

None

## Response messages

Table 23-3: List of response messages for the clear access-filter command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Port number
No configuration.	No access group was set for the Ethernet interface or VLAN interface. Make sure the specified parameter or access-group setting is correct, and then try again.
No such access-list.	The access list number or the access group of the access list name you specified has not been set. Make sure the specified parameter is correct, and then try again.
No such interface.	The specified interface has not been configured. Make sure the specified parameter is correct, and then try again.
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. <switch no.>: Switch number

## Notes

None

## Chapter

---

# 24. QoS

---

```
show qos-flow  
clear qos-flow  
show qos queueing  
clear qos queueing
```

---

## show qos-flow

---

Displays the number of packets that meet the flow detection conditions corresponding to the flow detection conditions and specified actions in the QoS flow list applied to the Ethernet interface or VLAN interface by QoS flow group commands (ip qos-flow-group, ipv6 qos-flow-group, and mac qos-flow-group).

### Syntax

```
show qos-flow [ { <switch no.>/<nif no.>/<port no.> | interface vlan <vlan id> }
                [ <qos flow list name> ] ]
```

### Input mode

User mode and administrator mode

### Parameters

```
{ <switch no.>/<nif no.>/<port no.> | interface vlan <vlan id> } [ <qos flow list name> ]
```

<switch no.>/<nif no.>/<port no.>

Displays statistics for the specified Ethernet interface. For the specifiable range of <switch no.>, <nif no.>, and <port no.> values, see *Specifiable values for parameters*.

interface vlan <vlan id>

Displays statistics for the specified VLAN interface.

For <vlan id>, specify the VLAN ID set by the interface vlan command.

<qos flow list name>

<qos flow list name>: Specify the QoS flow list name.

Displays statistics for the specified QoS flow list of the specified interface.

Operation when this parameter is omitted:

Displays statistics for all QoS flow lists applied to the specified interface.

Operation when this parameter is omitted:

Displays statistics for all interfaces.

### Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the remote command command.

```
remote command <switch no.> show qos-flow [ { <switch no.>/<nif no.>/<port no.> |
interface vlan <vlan id> } [ <qos flow list name> ] ]
remote command all show qos-flow [ interface vlan <vlan id> [ <qos flow list name> ] ]
```

### Example

- The following shows an example of displaying QoS flow list information when bandwidth monitoring is not used.

*Figure 24-1: Result of displaying MAC QoS flow list information*

```
> show qos-flow 1/0/3 apple-talk-qos
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/3 in
MAC qos-flow-list:apple-talk-qos
    remark "cos 5 discard-class 2"
    any any appletalk(0x809b) action cos 5 discard-class 2
        matched packets                : 74699826
>
```

*Figure 24-2: Result of displaying IPv4 QoS flow list information*

```
> show qos-flow 1/0/7 http-qos
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/7 in
IP qos-flow-list:http-qos
    remark "cos 4"
    tcp(6) any host 10.10.10.2 eq http(80) action cos 4
    matched packets : 74699826
>
```

*Figure 24-3: Result of displaying IPv6 QoS flow list information*

```
> show qos-flow 1/0/11 telnet-qos
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/11 in
IPv6 qos-flow-list:telnet-qos
    remark "cos 6 discard-class 2"
    ipv6(41) any host 13ffe:501:811:ff00::1 action cos 6 discard-class 2
    matched packets : 74699826
>
```

- The following shows an example of displaying QoS flow list information when bandwidth monitoring is used.

*Figure 24-4: Result of displaying IPv4 QoS flow list information when minimum bandwidth monitoring is used*

```
> show qos-flow 1/0/3 http-qos-min
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/3 in
IP qos-flow-list:http-qos-min
    remark "http access min-rate 256k"
    tcp(6) any any eq http(80) action cos 4 min-rate 256 min-rate-burst 256
    penalty-discard-class 1
    matched packets(min-rate over) : 9826
    matched packets(min-rate under): 74699826
>
```

*Figure 24-5: Result of displaying IPv4 QoS flow list information when maximum bandwidth control is used*

```
> show qos-flow 1/0/7 http-qos-max
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/7 in
IP qos-flow-list:http-qos-max
    remark "http access max-rate 256k"
    tcp(6) any any eq http(80) action cos 4 discard-class 2 max-rate 256
    max-rate-burst 256
    matched packets(max-rate over) : 9826
    matched packets(max-rate under): 74699826
>
```

*Figure 24-6: Result of displaying IPv4 QoS flow list information when minimum bandwidth monitoring and maximum bandwidth control are used*

```
> show qos-flow 1/0/11 http-qos-rate
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/11 in
IP qos-flow-list:http-qos-rate
    remark "http access min-rate 64k and max-rate 256k"
    tcp(6) any any eq http(80) action cos 4 discard-class 2 max-rate 256
    max-rate-burst 256 min-rate 64 min-rate-burst 64 penalty-discard-class 1
    matched packets(max-rate over) : 9826
    matched packets(max-rate under): 74699826
>
```

## Display items

Display items are described below.

```
> show qos-flow 1/0/7 http-qos
Date 20XX/07/14 12:00:00 UTC
Using Port:1/0/7 in
IP qos-flow-list:http-qos
    remark "cos 4"
    tcp any host 10.10.10.2 eq http action cos 4
    matched packets
>
```

<----- Interface information  
 <-----QoS flow list ID  
 <-----QoS flow list information  
 <---QoS flow list information  
 <---Statistics information

Table 24-1: Statistical items for the QoS flow list

Item	Displayed information	
	Detailed information	Meaning
Interface information	Using Port:<switch no.>/<nif no.>/<port no.> in	Information about an Ethernet interface to which a QoS flow list is applied on the inbound side
	Using Interface:vlan <vlan id> in	Information about a VLAN interface to which a QoS flow list is applied on the inbound side
QoS flow list name	MAC qos-flow-list:<qos flow list name>	MAC QoS flow list name
	IP qos-flow-list:<qos flow list name>	IPv4 QoS flow list name
	IPv6 qos-flow-list:<qos flow list name>	IPv6 QoS flow list name
QoS flow list information	Displays supplementary information, flow detection conditions, and operations set by QoS flow list commands (for details, see 20. <i>QoS</i> in the manual <i>Configuration Command Reference Vol. 1 For Version 11.10</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 criteria but violate the maximum bandwidth control criteria of the QoS flow list.
	matched packets(max-rate under):<packets>	Number of packets that match the flow detection criteria and conform to the maximum bandwidth control criteria of the QoS flow list.
	matched packets(min-rate over):<packets>	Number of packets that match the flow detection criteria but violate the minimum bandwidth monitoring criteria of the QoS flow list.
	matched packets(min-rate under):<packets>	Number of packets that match the flow detection criteria and conform to the minimum bandwidth monitoring criteria of the QoS flow list.

## Impact on communication

None

## Response messages

Table 24-2: List of response messages for the show qos-flow command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
Illegal Port -- <i>&lt;port no.&gt;</i> .	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <i>&lt;port no.&gt;</i> : 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 <i>&lt;qos flow list name&gt;</i> was applied to the interface. Make sure the specified parameter is correct, and then try again.
No such Switch <i>&lt;switch no.&gt;</i> .	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. <i>&lt;switch no.&gt;</i> : Switch number.

## Notes

None

---

## clear qos-flow

---

Clears the number of packets (indicated by `matched packets`) that met the flow detection conditions in the QoS flow list, which is displayed by the `show qos-flow` command.

### Syntax

```
clear qos-flow [ { <switch no.>/<nif no.>/<port no.> | interface vlan <vlan id> }
                [ <qos flow list name> ] ]
```

### Input mode

User mode and administrator mode

### Parameters

```
{ <switch no.>/<nif no.>/<port no.> | interface vlan <vlan id> } [ <qos flow list name> ]
```

`<switch no.>/<nif no.>/<port no.>`

Clears statistics for the specified Ethernet interface. For the specifiable range of `<switch no.>`, `<nif no.>`, and `<port no.>` values, see *Specifiable values for parameters*.

`interface vlan <vlan id>`

Clears statistics for the specified VLAN interface.

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.

Operation when this parameter is omitted:

Clears the statistics for all interfaces to zero.

### Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the `remote command` command.

```
remote command <switch no.> clear qos-flow [ { <switch no.>/<nif no.>/<port no.> |
interface vlan <vlan id> } [ <qos flow list name> ] ]
remote command all clear qos-flow [ interface vlan <vlan id> [ <qos flow list name>
] ]
```

### Example

*Figure 24-7: Result of clearing information*

```
> clear qos-flow 1/0/7 http-qos
Date 20XX/07/14 12:00:00 UTC
>
```

### Display items

None

### Impact on communication

None

## Response messages

Table 24-3: List of response messages for the clear qos-flow command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <i>&lt;port no.&gt;</i> .	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <i>&lt;port no.&gt;</i> : 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 <i>&lt;qos flow list name&gt;</i> was applied to the interface. Make sure the specified parameter is correct, and then try again.
No such Switch <i>&lt;switch no.&gt;</i> .	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. <i>&lt;switch no.&gt;</i> : Switch number.

## Notes

None

---

## show qos queueing

---

Displays information about the send queue of the port.

The send queue length, the maximum queue length, and the number of packets discarded without being accumulated in the send queue are displayed to enable monitoring of the traffic status.

### Syntax

```
show qos queueing [<switch no.>/<nif no.>/<port no.> ]
```

### Input mode

User mode and administrator mode

### Parameters

<switch no.>/<nif no.>/<port no.>

Displays information about the send queue of the specified port. For the specifiable range of <switch no.>, <nif no.>, and <port no.> values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

Displays information about the send queues of all ports implemented on the device, and about the send queues for traffic from the ports to the CPU.

### Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the `remote command` command.

```
remote command { <switch no.> | all } show qos queueing
```

```
remote command <switch no.> show qos queueing <switch no.>/<nif no.>/<port no.>
```

### Example

Figure 24-8: Result of displaying information about all send queues [AX3800S]

```
> show qos queueing
Date 20XX/01/01 12:00:00 UTC
Switch1 To-CPU (outbound)
Max_Queue=8
Queue 1: Qlen=    0, Limit_Qlen=   48, HOL1=        0
Queue 2: Qlen=    0, Limit_Qlen=   48, HOL1=        0
Queue 3: Qlen=    0, Limit_Qlen= 1024, HOL1=        0
Queue 4: Qlen=    0, Limit_Qlen= 1024, HOL1=        0
Queue 5: Qlen=    0, Limit_Qlen= 1024, HOL1=        0
Queue 6: Qlen=    0, Limit_Qlen= 1024, HOL1=        0
Queue 7: Qlen=    0, Limit_Qlen= 1024, HOL1=        0
Queue 8: Qlen=    0, Limit_Qlen= 2048, HOL1=       64
Tail_drop=      2339
Switch1/NIF0/Port1 (outbound)
Max_Queue=12, Rate_limit=64kbit/s, Burst_size=4kbyte, Qmode=pq/tail_drop
Queue 1: Qlen=    0, Limit_Qlen= 2880, HOL1=        0
Queue 2: Qlen=    0, Limit_Qlen= 2880, HOL1=        0
Queue 3: Qlen=    0, Limit_Qlen= 2880, HOL1=        0
Queue 4: Qlen=    0, Limit_Qlen= 2880, HOL1=        0
Queue 5: Qlen=    0, Limit_Qlen= 2880, HOL1=        0
Queue 6: Qlen=    0, Limit_Qlen= 2880, HOL1=        0
Queue 7: Qlen=    0, Limit_Qlen= 2880, HOL1=        0
Queue 8: Qlen=    0, Limit_Qlen= 2880, HOL1=        0
Queue 9: Qlen=    0, Limit_Qlen= 2880, HOL1=        0
Queue 10: Qlen=   0, Limit_Qlen= 2880, HOL1=        0
Queue 11: Qlen=    0, Limit_Qlen= 2880, HOL1=        0
Queue 12: Qlen=    0, Limit_Qlen= 2880, HOL1=       655
Tail_drop=      1532
.
```

```

.
.
Switch1/NIF0/Port48 (outbound)
Max_Queue=12, Rate_limit=64kbit/s, Burst_size=4kbyte, Qmode=pq/tail_drop
Queue 1: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 2: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 3: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 4: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 5: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 6: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 7: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 8: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 9: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 10: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 11: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 12: Qlen= 0, Limit_Qlen= 2880, HOL1= 54
Tail_drop= 1532
>

```

*Figure 24-9: Result of displaying information about all the send queues (when stack is enabled and a stack port is set) [AX3800S]*

```

> show qos queueing
Date 20XX/01/01 12:00:00 UTC
Switch1 To-CPU (outbound)
Max_Queue=11
Queue 1: Qlen= 0, Limit_Qlen= 48, HOL1= 0
Queue 2: Qlen= 0, Limit_Qlen= 48, HOL1= 0
Queue 3: Qlen= 0, Limit_Qlen= 1024, HOL1= 0
Queue 4: Qlen= 0, Limit_Qlen= 1024, HOL1= 0
Queue 5: Qlen= 0, Limit_Qlen= 1024, HOL1= 0
Queue 6: Qlen= 0, Limit_Qlen= 1024, HOL1= 0
SQueue 1: Qlen= 0, Limit_Qlen= 1024, HOL1= 0
SQueue 2: Qlen= 0, Limit_Qlen= 1024, HOL1= 0
Queue 7: Qlen= 3, Limit_Qlen= 1024, HOL1= 0
Queue 8: Qlen= 7, Limit_Qlen= 2048, HOL1= 25
SQueue 3: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Tail_drop= 2339
Switch1/NIF0/Port1 (outbound)
Max_Queue=12, Rate_limit=64kbit/s, Burst_size=4kbyte, Qmode=pq/tail_drop
Queue 1: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 2: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 3: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 4: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 5: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 6: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 7: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 8: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 9: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 10: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 11: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 12: Qlen= 0, Limit_Qlen= 2880, HOL1= 655
Tail_drop= 1532
.
.
Switch1/NIF0/Port49 (outbound)
Max_Queue=14, Rate_limit=40Gbit/s, Burst_size=-, Qmode=pq/tail_drop
Queue 1: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 2: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 3: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 4: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 5: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 6: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 7: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 8: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 9: Qlen= 0, Limit_Qlen= 2880, HOL1= 0
Queue 10: Qlen= 0, Limit_Qlen= 2880, HOL1= 0

```

```

Queue 11: Qlen=    0, Limit_Qlen= 2880, HOL1=    0
Queue 12: Qlen=    0, Limit_Qlen= 2880, HOL1=   35
SQueue 1: Qlen=    1, Limit_Qlen=  360, HOL1=    0
SQueue 2: Qlen=    1, Limit_Qlen=  360, HOL1=    0
Tail_drop=   1532
.
.
Switch1/NIF0/Port52 (outbound)
Max_Queue=12, Rate_limit=40Gbit/s, Burst_size=-, Qmode=pq/tail_drop
Queue 1: Qlen=    0, Limit_Qlen= 2880, HOL1=    0
Queue 2: Qlen=    0, Limit_Qlen= 2880, HOL1=    0
Queue 3: Qlen=    0, Limit_Qlen= 2880, HOL1=    0
Queue 4: Qlen=    0, Limit_Qlen= 2880, HOL1=    0
Queue 5: Qlen=    0, Limit_Qlen= 2880, HOL1=    0
Queue 6: Qlen=    0, Limit_Qlen= 2880, HOL1=    0
Queue 7: Qlen=    0, Limit_Qlen= 2880, HOL1=    0
Queue 8: Qlen=    0, Limit_Qlen= 2880, HOL1=    0
Queue 9: Qlen=    0, Limit_Qlen= 2880, HOL1=    0
Queue 10: Qlen=    0, Limit_Qlen= 2880, HOL1=    0
Queue 11: Qlen=    0, Limit_Qlen= 2880, HOL1=    0
Queue 12: Qlen=    0, Limit_Qlen= 2880, HOL1=   54
Tail_drop=   2561
>

```

*Figure 24-10: Result of displaying information about all send queues [AX3650S]*

```

> show qos queueing
Date 20XX/09/01 12:00:00 UTC
Switch1 To-CPU (outbound)
Max_Queue=8
Queue1: Qlen=  0, Limit_Qlen=  6, HOL1=    0
Queue2: Qlen=  0, Limit_Qlen=  6, HOL1=    0
Queue3: Qlen=  0, Limit_Qlen=128, HOL1=    0
Queue4: Qlen=  0, Limit_Qlen=128, HOL1=    0
Queue5: Qlen=  0, Limit_Qlen=128, HOL1=    0
Queue6: Qlen=  1, Limit_Qlen=128, HOL1=    0
Queue7: Qlen=  3, Limit_Qlen=128, HOL1=    0
Queue8: Qlen=  7, Limit_Qlen=256, HOL1=   25
Tail_drop=   8839
Switch1/NIF0/Port1 (outbound)
Max_Queue=8, Rate_limit=64kbit/s, Burst_size=4kbyte, Qmode=pq/tail_drop
Queue1: Qlen=  1, Limit_Qlen=  64, HOL1=    0
Queue2: Qlen=  0, Limit_Qlen=  64, HOL1=    0
Queue3: Qlen=  0, Limit_Qlen=  64, HOL1=    0
Queue4: Qlen=  2, Limit_Qlen=  64, HOL1=    0
Queue5: Qlen=  3, Limit_Qlen=  64, HOL1=    0
Queue6: Qlen=  5, Limit_Qlen=  64, HOL1=    0
Queue7: Qlen=  8, Limit_Qlen=  64, HOL1=    0
Queue8: Qlen= 11, Limit_Qlen=  64, HOL1=  123
Tail_drop=   1532
.
.
Switch1/NIF0/Port52 (outbound)
Max_Queue=8, Rate_limit=100Mbit/s, Burst_size=32kbyte, Qmode=pq/tail_drop
Queue1: Qlen=  0, Limit_Qlen=  64, HOL1=    0
Queue2: Qlen=  0, Limit_Qlen=  64, HOL1=    0
Queue3: Qlen=  0, Limit_Qlen=  64, HOL1=    0
Queue4: Qlen=  0, Limit_Qlen=  64, HOL1=    0
Queue5: Qlen=  0, Limit_Qlen=  64, HOL1=    0
Queue6: Qlen=  0, Limit_Qlen=  64, HOL1=    0
Queue7: Qlen=  0, Limit_Qlen=  64, HOL1=    0
Queue8: Qlen= 13, Limit_Qlen=  64, HOL1=   82
Tail_drop=   1532
>

```

*Figure 24-11:* Result of displaying information about all the send queues (when a stack is enabled and a stack port is set) [AX3650S]

```
> show qos queueing
Date 20XX/09/01 12:00:00 UTC
Switch1 To-CPU (outbound)
Max_Queue=11
Queue1: Qlen= 0, Limit_Qlen= 6, HOL1= 0
Queue2: Qlen= 0, Limit_Qlen= 6, HOL1= 0
Queue3: Qlen= 0, Limit_Qlen=128, HOL1= 0
Queue4: Qlen= 0, Limit_Qlen=128, HOL1= 0
Queue5: Qlen= 0, Limit_Qlen=128, HOL1= 0
Queue6: Qlen= 1, Limit_Qlen=128, HOL1= 0
SQueue1:Qlen= 0, Limit_Qlen=128, HOL1= 0
SQueue2:Qlen= 0, Limit_Qlen=128, HOL1= 0
Queue7: Qlen= 3, Limit_Qlen=128, HOL1= 0
Queue8: Qlen= 7, Limit_Qlen=256, HOL1= 25
SQueue3:Qlen= 0, Limit_Qlen= 8, HOL1= 0
Tail_drop= 8839
Switch1/NIF0/Port1 (outbound)
Max_Queue=8, Rate_limit=64kbit/s, Burst_size=4kbyte, Qmode=pq/tail_drop
Queue1: Qlen= 1, Limit_Qlen= 64, HOL1= 0
Queue2: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue3: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue4: Qlen= 2, Limit_Qlen= 64, HOL1= 0
Queue5: Qlen= 3, Limit_Qlen= 64, HOL1= 0
Queue6: Qlen= 5, Limit_Qlen= 64, HOL1= 0
Queue7: Qlen= 8, Limit_Qlen= 64, HOL1= 0
Queue8: Qlen= 11, Limit_Qlen= 64, HOL1= 123
Tail_drop= 1532
.
.
Switch1/NIF0/Port49 (outbound)
Max_Queue=9, Rate_limit=10Gbit/s, Burst_size--, Qmode=pq/tail_drop
Queue1: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue2: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue3: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue4: Qlen= 8, Limit_Qlen= 64, HOL1= 0
Queue5: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue6: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue7: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue8: Qlen= 64, Limit_Qlen= 64, HOL1= 82
SQueue1:Qlen= 1, Limit_Qlen= 8, HOL1= 0
Tail_drop= 2561
.
.
Switch1/NIF0/Port52 (outbound)
Max_Queue=8, Rate_limit=100Mbit/s, Burst_size=32kbyte, Qmode=pq/tail_drop
Queue1: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue2: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue3: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue4: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue5: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue6: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue7: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue8: Qlen= 13, Limit_Qlen= 64, HOL1= 82
Tail_drop= 1532
>
```

## Display items

Table 24-4: Display items of statistics

Item	Displayed information	
	Detailed information	Meaning
Interface information	Switch<switch no.>/NIF<nif no.>/Port<port no.> (outbound)	Port send queues
	Switch<switch no.> To-CPU (outbound)	Send queues for traffic from the ports to the CPU
QoS information	Max_Queue=<number of queue>	Number of send queues
	Rate_limit=<rate>	Bandwidth set for the port <ul style="list-style-type: none"> <li>When auto-negotiation is unresolved (including when processing is in progress): - - is displayed.</li> <li>When auto-negotiation has been resolved or the port bandwidth control is specified for the specified speed: The specified bandwidth is displayed.</li> <li>When auto-negotiation has been resolved or the port bandwidth control is not specified for the specified speed: The line speed is displayed.</li> </ul>
	Burst_size=<byte>	Burst size for port bandwidth control. <ul style="list-style-type: none"> <li>If port bandwidth control is enabled, the specified burst size is displayed.</li> <li>If port bandwidth control is disabled, a hyphen (-) is displayed.</li> </ul> For details about the port bandwidth control settings, see the description of the <code>traffic-shape rate</code> configuration command ( <i>traffic-shape rate</i> in the manual <i>Configuration Command Reference Vol. 1 For Version 11.10</i> ).
	Qmode=<schedule name>/<drop name>	Scheduling (For AX3830S: pq, 4pq+8rr, 4pq+8wfq, 4pq+8err, 4pq+8wrr; For AX3650S: pq, wrr, wfq, 2pq+6drr, 2pq+6wrr)/drop control mode ( <code>tail_drop</code> ) For details about scheduling, see the description of the <code>qos-queue-list</code> configuration command ( <i>qos-queue-list</i> in the manual <i>Configuration Command Reference Vol. 1 For Version 11.10</i> ).
Queue information	Queue<queue no.>:	Send queue number <sup>#1</sup>
	SQueue<queue no.>:	System queue number <sup>#2</sup>
	Qlen=<queue length>	Number of buffers used by send queue
	Limit_Qlen=<queue length>	Maximum number of send queues

Item	Displayed information	
	Detailed information	Meaning
Queue statistics	HOL1=<packets> HOL: Stands for head of line blocking.	When the destination port for received packets is determined, the number of packets discarded for the following reasons regardless of the queuing priority is displayed <sup>#3, #4, #5</sup> 1. Regardless of the remaining free space of the packet buffer, no more packets can be put in the send queue of the send port (the number of packets discarded by the tail drop functionality <sup>#6</sup> of drop control because the drop threshold value for queuing priority is exceeded). <sup>#7</sup> 2. There is free space in the send queue, but the packet buffer has no free space. <sup>#8</sup>
Port statistics	Tail_drop=<packets>	The number of packets discarded because the drop threshold for queuing priority 1 or 2 is exceeded <sup>#4, #5</sup>

#1

For AX3830S, sending queues on ports exist in UC (unicast frames) and MC (frames other than unicast frames, such as unlearned unicast frames and multicast frames, or mirrored frames) independently. The following table shows the CoS values corresponding to the sending queues.

Table 24-5: CoS values corresponding to sending queues (for 12 queues) [AX3800S]

Queue number	CoS value	
	UC	MC
1	0	--
2	1	--
3	--	0 to 3
4	2	--
5	3	--
6	4	--
7	--	4, 5
8	5	--
9	--	6
10	6	--
11	--	7
12	7	--

Table 24-6: CoS values corresponding to sending queues (for 4 queues) [AX3800S]

Queue number	CoS value	
	UC	MC
1	--	0 to 6
2	0 to 6	--

Queue number	CoS value	
	UC	MC
3	--	7
4	7	--

Table 24-7: CoS values corresponding to sending queues (for 8 queues) [AX3650S]

Queue number	CoS value
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	7

Table 24-8: CoS values corresponding to sending queues (for 2 queues) [AX3650S]

Queue number	CoS value
1	0 to 6
2	7

#2

The system queue is used by the stack functionality for communication and exists only when the stack functionality is enabled. The system queue is displayed in a sending queue from a port to the CPU and in a sending queue on a stack port.

#3

If the displayed port is a mirror port, HOL1 might be counted depending on the status of the sending queue on the monitor port. [AX3800S]

#4

Some control packets are handled with a queuing priority other than 3.

#5

If the queuing priority is not 3, the HOL1 and Tail\_drop values are incremented.

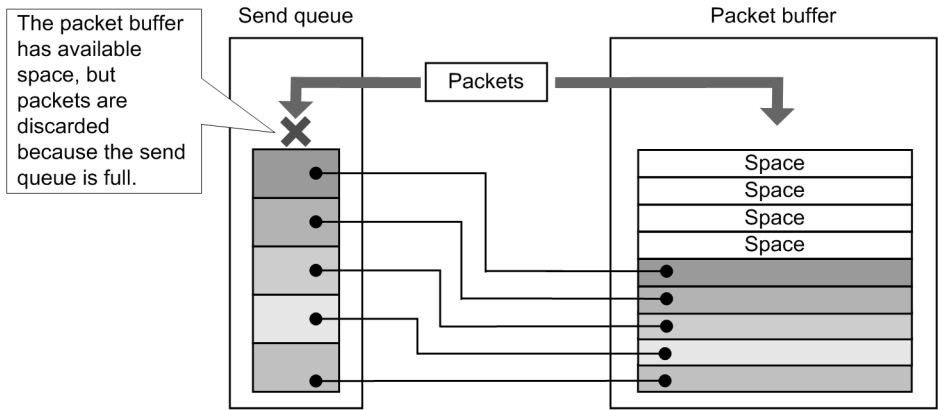
#6

For details about the tail drop functionality of drop control, see 4.4.1(1) *Tail drop* in the manual *Configuration Guide Vol. 2 For Version 11.10*.

#7

The following figure shows an overview of processing that discards packets because the send queue is full.

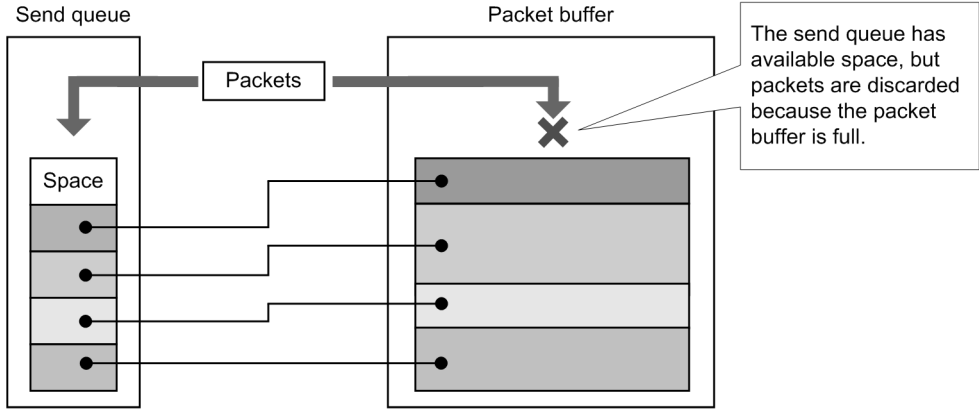
Figure 24-12: Overview of processing that discards packets because the send queue is full



#8

The following figure shows an overview of processing that discards packets because the packet buffer is full.

Figure 24-13: Overview of processing that discards packets because the packet buffer is full



Impact on communication

None

Response messages

Table 24-9: List of response messages for the show qos queuing command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Port number
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. <switch no.>: Switch number.

Notes

None

---

## clear qos queueing

---

For the information displayed by the `show qos queueing` command, this command clears to 0 the number of packets (HOL1 and Tail\_drop) that were not placed in the send queue and were discarded.

### Syntax

```
clear qos queueing [<switch no.>/<nif no.>/<port no.> ]
```

### Input mode

User mode and administrator mode

### Parameters

<switch no.>/<nif no.>/<port no.>

The number of packets discarded without being put into the send queue of the specified port is reset to 0. For the specifiable range of <switch no.>, <nif no.>, and <port no.> values, see *Specifiable values for parameters*.

Operation when this parameter is omitted:

The number of packets discarded is reset to 0 for the following queues: the send queues of all ports on the switch and the queue for sending packets from ports to the CPU.

### Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the `remote command` command.

```
remote command { <switch no.> | all } clear qos queueing
```

```
remote command <switch no.> clear qos queueing <switch no.>/<nif no.>/<port no.>
```

### Example

*Figure 24-14: Result of clearing statistics for a port*

```
> clear qos queueing 1/0/3
Date 20XX/07/14 12:00:00 UTC
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 24-10: List of response messages for the clear qos queueing command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Illegal Port -- <port no.>.	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <port no.>: Port number
No such Switch <switch no.>.	The specified switch number does not exist. Make sure the specified parameter is correct, and then try again. <switch no.>: Switch number.

**Notes**

None



## Chapter

---

# 25. IEEE 802.1X

---

```
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.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 25-1: Displaying the statistics for each port that uses IEEE 802.1X port-based authentication*

```
> show dot1x statistics port 0/10
Date 20XX/01/23 12:32:00 UTC
[EAPOL frames]
Port 0/10 TxTotal      :      30 TxReq/Id   :      10 TxReq      :      10
          TxSuccess    :      10 TxFailure  :      0 TxNotify   :      0
          RxTotal      :      20 RxStart    :      0 RxLogoff   :      0
          RxResp/Id    :      10 RxResp     :      10 RxNotify   :      0
          RxInvalid    :      0 RxLenErr   :      0

[EAPoverRADIUS frames]
Port 0/10 TxTotal      :      10 TxNakResp  :      0 TxNoNakRsp:      10
          RxTotal      :      30 RxAccAcpt  :      10 RxAccRejct:      10
          RxAccChllg    :      10 RxInvalid  :      0
>
```

**Figure 25-2:** Displaying statistics for each channel group that uses IEEE 802.1X port-based authentication

```
> show dot1x statistics channel-group-number 11
Date 20XX/01/23 12:32:00 UTC
[EAPOL frames]
ChGr 11 TxTotal : 30 TxReq/Id : 10 TxReq : 10
      TxSuccess : 10 TxFailure : 0 TxNotify : 0
      RxTotal : 20 RxStart : 0 RxLogoff : 0
      RxResp/Id : 10 RxResp : 10 RxNotify : 0
      RxInvalid : 0 RxLenErr : 0

[EAPoverRADIUS frames]
ChGr 11 TxTotal : 10 TxNakResp : 0 TxNoNakRsp: 10
      RxTotal : 30 RxAccAcpt: 10 RxAccRejct: 10
      RxAccChllg: 10 RxInvalid : 0
>
```

**Figure 25-3:** Displaying statistics about each VLAN for IEEE 802.1X VLAN-based authentication (static)

```
> show dot1x statistics vlan 20
Date 20XX/01/23 12:32:00 UTC
[EAPOL frames]
VLAN 20 TxTotal : 30 TxReq/Id : 10 TxReq : 10
      TxSuccess : 10 TxFailure : 0 TxNotify : 0
      RxTotal : 20 RxStart : 0 RxLogoff : 0
      RxResp/Id : 10 RxResp : 10 RxNotify : 0
      RxInvalid : 0 RxLenErr : 0

[EAPoverRADIUS frames]
VLAN 20 TxTotal : 10 TxNakResp : 0 TxNoNakRsp: 10
      RxTotal : 30 RxAccAcpt: 10 RxAccRejct: 10
      RxAccChllg: 10 RxInvalid : 0
>
```

**Figure 25-4:** Displaying statistics for IEEE 802.1X VLAN-based authentication (dynamic)

```
> show dot1x statistics vlan dynamic
Date 20XX/01/23 12:32:00 UTC
[EAPOL frames]
VLAN TxTotal : 30 TxReq/Id : 10 TxReq : 10
(Dynamic) TxSuccess : 10 TxFailure : 0 TxNotify : 0
      RxTotal : 20 RxStart : 0 RxLogoff : 0
      RxResp/Id : 10 RxResp : 10 RxNotify : 0
      RxInvalid : 0 RxLenErr : 0

[EAPoverRADIUS frames]
VLAN TxTotal : 10 TxNakResp : 0 TxNoNakRsp: 10
(Dynamic) RxTotal : 30 RxAccAcpt: 10 RxAccRejct: 10
      RxAccChllg: 10 RxInvalid : 0
>
```

**Figure 25-5:** Displaying statistics for all types of IEEE 802.1X authentication (port-based authentication and VLAN-based authentication)

```
> show dot1x statistics
Date 20XX/01/23 12:32:00 UTC
[EAPOL frames]
Port 0/10 TxTotal : 30 TxReq/Id : 10 TxReq : 10
      TxSuccess : 10 TxFailure : 0 TxNotify : 0
      RxTotal : 20 RxStart : 0 RxLogoff : 0
      RxResp/Id : 10 RxResp : 10 RxNotify : 0
      RxInvalid : 0 RxLenErr : 0
ChGr 11 TxTotal : 30 TxReq/Id : 10 TxReq : 10
      TxSuccess : 10 TxFailure : 0 TxNotify : 0
      RxTotal : 20 RxStart : 0 RxLogoff : 0
      RxResp/Id : 10 RxResp : 10 RxNotify : 0
      RxInvalid : 0 RxLenErr : 0
```

```

VLAN 20    TxTotal    :      30 TxReq/Id    :      10 TxReq      :      10
           TxSuccess  :      10 TxFailure  :      0 TxNotify  :      0
           RxTotal    :      20 RxStart    :      0 RxLogoff  :      0
           RxResp/Id  :      10 RxResp     :      10 RxNotify  :      0
           RxInvalid  :      0 RxLenErr   :      0
VLAN
(Dynamic)  TxTotal    :      30 TxReq/Id    :      10 TxReq      :      10
           TxSuccess  :      10 TxFailure  :      0 TxNotify  :      0
           RxTotal    :      20 RxStart    :      0 RxLogoff  :      0
           RxResp/Id  :      10 RxResp     :      10 RxNotify  :      0
           RxInvalid  :      0 RxLenErr   :      0

[EAPoverRADIUS frames]
Port 0/10 TxTotal    :      10 TxNakResp :      0 TxNoNakRsp:      10
           RxTotal    :      30 RxAccAccpt:      10 RxAccRejct:      10
           RxAccChllg:      10 RxInvalid  :      0
ChGr 11   TxTotal    :      10 TxNakResp :      0 TxNoNakRsp:      10
           RxTotal    :      30 RxAccAccpt:      10 RxAccRejct:      10
           RxAccChllg:      10 RxInvalid  :      0
VLAN 20   TxTotal    :      10 TxNakResp :      0 TxNoNakRsp:      10
           RxTotal    :      30 RxAccAccpt:      10 RxAccRejct:      10
           RxAccChllg:      10 RxInvalid  :      0
VLAN
(Dynamic) TxTotal    :      10 TxNakResp :      0 TxNoNakRsp:      10
           RxTotal    :      30 RxAccAccpt:      10 RxAccRejct:      10
           RxAccChllg:      10 RxInvalid  :      0
>

```

## Display items

Table 25-1: Display items for statistics concerning 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	

Item	Meaning	Displayed information
RxInvalid	The number of invalid EAPOL frames that have been received (the number of discarded frames)	
RxLenErr	The number of invalid-length EAPOL frames that have been received (the number of discarded frames)	
[EAPoverRADIUS frames]	Statistics for EAPoverRADIUS frames. For details about the items, see the following.	
TxTotal	The total number of EAPoverRADIUS frames that have been sent	
TxNakResp	The number of AccessRequest/EAP Response/NAK frames that have been sent	
TxNoNakRsp	The number of AccessRequest/EAP Response frames (excluding NAK frames) that have been sent	
RxTotal	The total number of EAPoverRADIUS frames that have been received	
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 25-2: List of response messages for the show dot1x statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <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.

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.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 25-6:* Displaying the status information for the IEEE 802.1X switch

```
> show dot1x
Date 20XX/01/23 12:32:00 UTC
System 802.1X : Enable
```

```

AAA Authentication Dot1x : Enable
  Authorization Network  : Enable
  Accounting Dot1x       : Enable

Port/ChGr/VLAN  AccessControl  PortControl  Status      Supplicants
Port  0/1       ---           Auto         Authorized  1
Port  0/10      Multiple-Auth  Auto         ---         1
ChGr  11        Multiple-Auth  Auto         ---         1
VLAN  20        Multiple-Auth  Auto         ---         1
VLAN(Dynamic)  Multiple-Auth  Auto         ---         1
>

```

*Figure 25-7:* Displaying the status information for each port that uses IEEE 802.1X port-based authentication (no display type is specified)

```

> show dot1x port 0/1
Date 20XX/01/23 12:32:00 UTC
Port 0/1
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 25-8:* Displaying the status information for each port that uses IEEE 802.1X port-based authentication (detail display)

```

> show dot1x port 0/1 detail
Date 20XX/01/23 17:57:03 UTC
Port 0/1
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
0012.e200.0021      Authorized  Authenticated  Idle          0
177                  20XX/01/23 17:55:00
>

```

*Figure 25-9:* 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 20XX/01/23 12:32:00 UTC
ChGr 11
AccessControl : Multiple-Auth
Status        : ---
Supplicants   : 2 / 2 / 64
TxTimer(s)    : 15 / 30
ReAuthSuccess : 4
SuppDetection : Shortcut
PortControl   : Auto
Last EAPOL    : 0012.e200.0011
ReAuthMode    : Enable
ReAuthTimer(s): 123 / 300
ReAuthFail    : 0
>

```

*Figure 25-10:* 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 20XX/01/23 17:57:03 UTC
ChGr 11
AccessControl : Multiple-Auth
Status        : ---
Supplicants   : 2 / 2 / 64
TxTimer(s)    : 15 / 30
PortControl   : Auto
Last EAPOL    : 0012.e200.0011
ReAuthMode    : Enable
ReAuthTimer(s): 123 / 300
>

```

```

ReAuthSuccess : 4
SuppDetection : Shortcut
ReAuthFail    : 0

Supplicants MAC      Status      AuthState      BackEndState  ReAuthSuccess
                   SessionTime(s) Date/Time
0012.e200.0011      Authorized  Authenticated  Idle          0
                   177          20XX/01/23 17:55:00
0012.e200.0012      Authorized  Authenticated  Idle          0
                   5           20XX/01/23 17:56:58
>

```

**Figure 25-11:** 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 20XX/10/17 12:32:00 UTC
VLAN 20
AccessControl : Multiple-Auth
Status        : ---
Supplicants   : 2 / 2 / 256
TxTimer(s)    : --- / 30
ReAuthSuccess : 4
SuppDetection : Disable
Port(s): 0/1-10, ChGr 1-5
Force-Authorized Port(s): 0/4,8-10, ChGr 1-5
>

```

**Figure 25-12:** Displaying status information about VLAN for IEEE 802.1X VLAN-based authentication (static) (details display)

```

> show dot1x vlan 20 detail
Date 20XX/10/17 17:57:03 UTC
VLAN 20
AccessControl : Multiple-Auth
Status        : ---
Supplicants   : 2 / 2 / 256
TxTimer(s)    : --- / 30
ReAuthSuccess : 4
SuppDetection : Disable
Port(s): 0/1-10, ChGr 1-5
Force-Authorized Port(s): 0/4,8-10, ChGr 1-5

Supplicants MAC      Status      AuthState      BackEndState  ReAuthSuccess
                   SessionTime(s) Date/Time
[Port 0/1]
0012.e200.0003      Authorized  Authenticated  Idle          0
                   177          20XX/10/17 17:55:00
0012.e200.0004      Authorized  Authenticated  Idle          0
                   5           20XX/10/17 17:56:58
>

```

**Figure 25-13:** Displaying status information about IEEE 802.1X VLAN-based authentication (dynamic) (no display type is specified)

```

> show dot1x vlan dynamic
Date 20XX/10/17 12:32:00 UTC
VLAN(Dynamic)
AccessControl : Multiple-Auth
Status        : ---
Supplicants   : 2 / 2 / 256
TxTimer(s)    : --- / 30
ReAuthSuccess : 4
SuppDetection : Disable
VLAN(s): 2-5

VLAN(Dynamic) Supplicants
VLAN 2      2      VLAN 3      0      VLAN 4      0      VLAN 5      0
>

```

**Figure 25-14:** Displaying status information about IEEE 802.1X VLAN-based authentication (dynamic) (detail display)

```
> show dot1x vlan dynamic detail
Date 20XX/10/17 17:57:03 UTC
VLAN(Dynamic)
AccessControl : Multiple-Auth          PortControl : Auto
Status        : ---                    Last EAPOL   : 0012.e200.0005
Supplicants   : 2 / 2 / 256            ReAuthMode   : Enable
TxTimer(s)    : --- / 30               ReAuthTimer(s): 123 / 300
ReAuthSuccess : 4                      ReAuthFail   : 0
SuppDetection : Disable
VLAN(s): 2-5

Supplicants MAC      Status      AuthState      BackEndState  ReAuthSuccess
SessionTime(s) Date/Time
[VLAN 2]
0012.e200.0005      Authorized  Authenticated  Idle          0
177                 20XX/10/17 17:55:00
0012.e200.0006      Authorized  Authenticated  Idle          0
5                   20XX/10/17 17:56:58
```

**Figure 25-15:** 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 20XX/10/17 12:32:00 UTC
VLAN(Dynamic)
AccessControl : Multiple-Auth          PortControl : Auto
Status        : ---                    Last EAPOL   : 0012.e200.0005
Supplicants   : 2 / 2 / 256            ReAuthMode   : Enable
TxTimer(s)    : --- / 30               ReAuthTimer(s): 123 / 300
ReAuthSuccess : 4                      ReAuthFail   : 0
SuppDetection : Disable
VLAN(s): 2-5

VLAN(Dynamic) Supplicants
VLAN 2        2
```

**Figure 25-16:** Displaying status information about each VLAN for IEEE 802.1X VLAN-based authentication (dynamic) (detail display)

```
> show dot1x vlan dynamic 2 detail
Date 20XX/10/17 17:57:03 UTC
VLAN(Dynamic)
AccessControl : Multiple-Auth          PortControl : Auto
Status        : ---                    Last EAPOL   : 0012.e200.0005
Supplicants   : 2 / 2 / 256            ReAuthMode   : Enable
TxTimer(s)    : --- / 30               ReAuthTimer(s): 123 / 300
ReAuthSuccess : 4                      ReAuthFail   : 0
SuppDetection : Disable
VLAN(s): 2-5

Supplicants MAC      Status      AuthState      BackEndState  ReAuthSuccess
SessionTime(s) Date/Time
[VLAN 2]
0012.e200.0005      Authorized  Authenticated  Idle          0
177                 20XX/10/17 17:55:00
0012.e200.0006      Authorized  Authenticated  Idle          0
5                   20XX/10/17 17:56:58
```

**Figure 25-17:** Displaying the status information for all types of IEEE 802.1X authentication

```
> show dot1x detail
Date 20XX/04/08 17:57:03 UTC
System 802.1X : Enable
```

AAA Authentication Dot1x : Enable  
 Authorization Network : Enable  
 Accounting Dot1x : Enable

Port 0/1  
 AccessControl : --- PortControl : Auto  
 Status : Authorized Last EAPOL : 0012.e200.0021  
 Supplicants : 1 / 1 ReAuthMode : Enable  
 TxTimer(s) : --- / 30 ReAuthTimer(s) : 123 / 300  
 ReAuthSuccess : 4 ReAuthFail : 0  
 KeepUnauth(s) : --- / 3600

Supplicants MAC	Status	AuthState	BackEndState	ReAuthSuccess
	SessionTime(s)	Date/Time		
0012.e200.0021	Authorized	Authenticated	Idle	0
	177	20XX/04/08 17:55:00		

Port 0/20  
 AccessControl : Multiple-Auth PortControl : Auto  
 Status : --- Last EAPOL : 0012.e200.0001  
 Supplicants : 2 / 2 / 64 ReAuthMode : Enable  
 TxTimer(s) : 15 / 30 ReAuthTimer(s) : 123 / 300  
 ReAuthSuccess : 4 ReAuthFail : 0  
 SuppDetection : Shortcut

Supplicants MAC	Status	AuthState	BackEndState	ReAuthSuccess
	SessionTime(s)	Date/Time		
0012.e200.0001	Authorized	Authenticated	Idle	0
	177	20XX/04/08 17:55:00		
0012.e200.0002	Authorized	Authenticated	Idle	0
	5	20XX/04/08 17:56:58		

ChGr 11  
 AccessControl : Multiple-Auth PortControl : Auto  
 Status : --- Last EAPOL : 0012.e200.0011  
 Supplicants : 2 / 2 / 64 ReAuthMode : Enable  
 TxTimer(s) : 15 / 30 ReAuthTimer(s) : 123 / 300  
 ReAuthSuccess : 4 ReAuthFail : 0  
 SuppDetection : Shortcut

Supplicants MAC	Status	AuthState	BackEndState	ReAuthSuccess
	SessionTime(s)	Date/Time		
0012.e200.0011	Authorized	Authenticated	Idle	0
	177	20XX/04/08 17:55:00		
0012.e200.0012	Authorized	Authenticated	Idle	0
	5	20XX/04/08 17:56:58		

VLAN 20  
 AccessControl : Multiple-Auth PortControl : Auto  
 Status : --- Last EAPOL : 0012.e200.0003  
 Supplicants : 2 / 2 / 256 ReAuthMode : Enable  
 TxTimer(s) : --- / 30 ReAuthTimer(s) : 123 / 300  
 ReAuthSuccess : 4 ReAuthFail : 0  
 SuppDetection : Disable  
 Port(s) : 0/1-15, ChGr 1-5  
 Force-Authorized Port(s) : 0/4,8-15, ChGr 1-5

Supplicants MAC	Status	AuthState	BackEndState	ReAuthSuccess
	SessionTime(s)	Date/Time		
[Port 0/1]				
0012.e200.0003	Authorized	Authenticated	Idle	0
	177	20XX/04/08 17:55:00		
*0012.e200.0004	Authorized	Authenticated	Idle	0
	5	20XX/04/08 17:56:58		

VLAN(Dynamic)  
 AccessControl : Multiple-Auth PortControl : Auto

```

Status          : ---
Supplicants     : 2 / 2 / 256
TxTimer(s)      : --- / 30
ReAuthSuccess   : 4
SuppDetection   : Disable
VLAN(s) : 2-5
Last EAPOL      : 0012.e200.0005
ReAuthMode      : Enable
ReAuthTimer(s)  : 123 / 300
ReAuthFail      : 0

```

Supplicants MAC	Status	AuthState	BackEndState	ReAuthSuccess
[VLAN 2]	SessionTime(s)	Date/Time		
0012.e200.0005	VLAN(Dynamic)	Supplicants : 2		
	Authorized	Authenticated	Idle	0
	177	20XX/04/08 17:55:00		
0012.e200.0006	Authorized	Authenticated	Idle	0
	5	20XX/04/08 17:56:58		

&gt;

## Display items

Table 25-3: 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"> <li>1. Enable (IEEE 802.1X authentication is operating.)</li> <li>2. Disable (IEEE 802.1X authentication stops.)</li> </ol>
AAA	Authentication Dot1x	Displays the operating status of authentication requests to RADIUS.	<ol style="list-style-type: none"> <li>1. Enable (Authentication request to RADIUS is enabled.)</li> <li>2. Disable (Authentication request to RADIUS is disabled.)</li> </ol>
	Authorization Network	Displays the operating status of VLAN allocation from RADIUS when VLAN-based authentication (dynamic) is used.	<ol style="list-style-type: none"> <li>1. Enable (VLAN allocation from RADIUS is enabled.)</li> <li>2. Disable (VLAN allocation from RADIUS is disabled.)</li> </ol>
	Accounting Dot1x	Displays the operating status of the accounting functionality.	<ol style="list-style-type: none"> <li>1. Enable (The accounting functionality is enabled.)</li> <li>2. Disable (The accounting functionality is disabled.)</li> </ol>
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"> <li>1. ---</li> <li>2. Multiple-Hosts</li> <li>3. Multiple-Auth</li> </ol>

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: <number of authenticated supplicants> / <number of supplicants to be authenticated> For terminal authentication mode: <number of authenticated supplicants> / <number of supplicants to be authenticated> / <maximum number of supplicants within an authentication type>	
ReAuthMode	Displays the status of the self-issuance of EAPOL Request/ID re-authentication requests.	1. Enabled 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. - New terminal detection mode was Auto. - The following authentication types are disabled: Port-based authentication: For port or a channel group to be authenticated VLAN-based authentication (static or dynamic): For VLAN to be authenticated <current timer value> / <tx_period seconds>	
ReAuthTimer(s)	Displays the timer for sending EAPOL Request/ID re-authentication requests after a successful authentication. ---: The timer is disabled because authentication has not been successful. <current timer value> / <reauth_period seconds>	
ReAuthSuccess	The number of times that re-authentication has been successful	
ReAuthFail	The number of times that re-authentication has failed	

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>&lt;current timer value&gt; / &lt;keepunauth_period seconds&gt;</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>Full: Complete search mode</p> <p>Shortcut: Omission mode</p> <p>Auto: Automatic detection mode</p>	<ol style="list-style-type: none"> <li>1. Disable</li> <li>2. Full</li> <li>3. Shortcut</li> <li>4. Auto</li> </ol>
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 authentication-exempted ports.	
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	<p>The supplicant's MAC address.</p> <p>Supplicants with an asterisk (*) on the left are being quarantined.</p>	
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"> <li>1. Authorized</li> <li>2. Unauthorized</li> </ol>
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"> <li>1. Connecting</li> <li>2. Authenticating</li> <li>3. Authenticated</li> <li>4. Aborting</li> <li>5. Held</li> </ol>

Item	Meaning	Displayed information
BackEndState	Displays the status of authentication processing for the supplicant by the RADIUS server. Idle: The supplicant is waiting for processing. Response: The supplicant is responding to the server. Request: A request is being sent to the supplicant. Success: Authentication processing has finished successfully. Fail: The authentication processing failed. Timeout: A timeout occurred during an attempt to connect to the server.	1. Idle 2. Response 3. Request 4. Success 5. Fail 6. Timeout
ReAuthSuccess	Displays the number of times re-authentication was successful.	
SessionTime	Displays the time (in seconds for each supplicant) required to establish a session after a successful authentication.	
Date/Time	Displays the time that authentication of the supplicant was successful.	

## Impact on communication

None

## Response messages

Table 25-4: List of response messages for the show dot1x command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <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.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 25-18: Clearing IEEE 802.1X authentication statistics*

```
> clear dot1x statistics
>
```

### Display items

None

### Impact on communication

None

## Response messages

*Table 25-5:* List of response messages for the clear dot1x statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <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.

## Operation when a stack configuration is used

This command is not supported.

## Example

*Figure 25-19: 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 25-6: List of response messages for the clear dot1x auth-state command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <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.

## Operation when a stack configuration is used

This command is not supported.

## Example

*Figure 25-20:* 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 25-7:* List of response messages for the reauthenticate dot1x command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <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.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 25-21: Restarting the IEEE 802.1X program*

```
> restart dot1x
802.1X restart OK? (y/n) : y
>
```

*Figure 25-22: 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 25-8: 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.

Message	Description
Now another user is using dot1x command, please try again.	Another user is using the dot1x command. Wait a while, and then retry the operation.

## Notes

The storage directory and the name of the 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

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 25-23: Acquiring IEEE 802.1X program online dump*

```
> dump protocols dot1x
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 25-9: List of response messages for the dump protocols dot1x command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <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.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 25-24: Displaying IEEE 802.1X operation log messages*

```
> show dot1x logging
Date 20XX/01/23 13:32:00 UTC
No=1:Jan 23 13:31:43:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=0/1 VLAN=10 Login
succeeded. ; New Supplicant Auth Success.
No=16:Jan 23 13:16:55:NORMAL:LOGOUT: MAC=0012.e200.0001 PORT=0/1 VLAN=10 Force
Logout. ; Port link down.
No=2:Jan 23 13:16:10:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=0/1 VLAN=10 Login
succeeded. ; Supplicant Re-Auth Success.
No=1:Jan 23 13:15:10:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=0/1 VLAN=10 Login
succeeded. ; New Supplicant Auth Success.
No=30:Jan 23 13:10:34:NOTICE:LOGIN: MAC=0012.e200.0001 PORT=0/1 VLAN=10 Login
failed. ; RADIUS authentication failed.
```

### Display items

The following table shows the items displayed when an IEEE 802.1X operation log message is displayed.

*Table 25-10: 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=0/1 VLAN=3 Logout succeeded.  
 (1) (2) (3) (4) (5) (6) (7)

- (1) Message number: Indicates the number assigned to each message shown in *Table 25-13: 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 25-11: Log ID and type in operation log messages*.
- Log type: See *Table 25-11: Log ID and type in operation log messages*.
- Additional information: See *Table 25-12: Additional information*
- List of messages: See *Table 25-13: List of operation log messages*

*Table 25-11: 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 system alert.
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 25-12: 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 25-13: 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
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
3	NORMAL	LOGIN	Login succeeded. ; Limited by ACL.	[Meaning] A supplicant was authenticated, but a pre-authentication filter is enabled. [Action] Clear the quarantine conditions.	MAC address port number or channel group number VLAN ID
10	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 the MAC address was configured for the MAC address table. [Action] None	MAC address port number or channel group number VLAN ID
14	NORMAL	LOGOUT	Force logout. ; The status of port was changed to Unauthorized, because another supplicant was 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

#	Log ID	Log type	Message text	Meaning and action	Additional information
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
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

#	Log ID	Log type	Message text	Meaning and action	Additional information
32	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: "aaa authorization network default" is not configured.)	[Meaning] VLAN dynamic assignment failed because the aaa authorization network default configuration command was not configured. [Action] Set the aaa authorization network default configuration command.	MAC address port number, or channel group number
33	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: No Tunnel-Type Attribute.)	[Meaning] VLAN dynamic assignment failed because there was no Tunnel-Type attribute. [Action] Set the Tunnel-Type attribute in the Accept packet to be sent by the RADIUS server.	MAC address port number, or channel group number
34	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Tunnel-Type Attribute is not VLAN(13).)	[Meaning] VLAN dynamic assignment failed because the value of the Tunnel-Type attribute was not VLAN(13). [Action] Set the Tunnel-Type attribute in the Accept packet to be sent by the RADIUS server to VLAN(13).	MAC address port number, or channel group number
35	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: No Tunnel-Medium-Type Attribute.)	[Meaning] VLAN dynamic assignment failed because there was no Tunnel-Medium-Type attribute. [Action] Set the Tunnel-Medium-Type attribute in the Accept packet to be sent by the RADIUS server.	MAC address port number, or channel group number
36	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Tunnel-Medium-Type Attribute is not IEEE802(6).)	[Meaning] VLAN dynamic assignment failed because the value of the Tunnel-Medium-Type attribute was not IEEE 802(6). [Action] Set the Tunnel-Medium-Type attribute in the Accept packet to be sent by the RADIUS server to IEEE 802(6).	MAC address port number, or channel group number
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

#	Log ID	Log type	Message text	Meaning and action	Additional information
38	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Invalid Tunnel-Private-Group-ID Attribute.)	<p>[Meaning] VLAN dynamic assignment failed because an invalid value was set for the Tunnel-Private-Group-ID attribute.</p> <p>[Action] Check the setting of the Tunnel-Private-Group-ID attribute in the Accept packet to be sent by the RADIUS server.</p>	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.)	<p>[Meaning] VLAN dynamic assignment failed because the VLAN ID was not in the normal range.</p> <p>[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.</p>	MAC address port number or channel group number VLAN ID
40	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The Port doesn't belong to VLAN.)	<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

#	Log ID	Log type	Message text	Meaning and action	Additional information
43	NOTICE	LOGIN	Login failed. ; The number of supplicants on the switch is full.	[Meaning] Authentication was not available because there were too many supplicants for the Switch. [Action] Attempt authentication again when the total number of authenticated supplicants falls below the capacity limit.	MAC address port number or channel group number VLAN ID
44	NOTICE	LOGIN	Login failed. ; The number of supplicants on the interface is full.	[Meaning] Authentication was not available because there were too many supplicants on the interface. [Action] Attempt authentication again when the number of authenticated supplicants on the interface falls below the capacity limit.	MAC address port number or channel group number VLAN ID
45	NOTICE	LOGIN	Login failed. ; Failed to authenticate the supplicant because it could not be registered to mac-address-table.(code=x)	[Meaning] Authentication failed because the registration of a supplicant in the MAC address table failed. [Action] If the total number of supplicants to be authenticated including other types of authentication exceeds the capacity limit of a Switch or the set maximum number of authentication terminals, perform authentication again when the number of authenticated supplicants goes below the capacity limit.	MAC address port number or channel group number VLAN ID
46	NOTICE	LOGIN	Login failed. ; Failed to authenticate the supplicant because it could not be registered to MAC VLAN.(code=x)	[Meaning] Authentication failed because the registration of a supplicant in the MAC VLAN failed. [Action] If the total number of supplicants to be authenticated including other types of authentication exceeds the capacity limit of a Switch or the set maximum number of authentication terminals, perform authentication again when the number of authenticated supplicants goes below the capacity limit. In addition, make sure that the supplicants have not been authenticated by any other methods.	MAC address port number or channel group number VLAN ID

#	Log ID	Log type	Message text	Meaning and action	Additional information
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"> <li>• Communication between the Switch and the RADIUS server is available.</li> <li>• The RADIUS server functionality is enabled.</li> </ul>	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"> <li>• The contents of EAPOL frames sent by the supplicant</li> <li>• Transmission line quality</li> </ul>	n/a
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"> <li>• The contents of packets sent by the RADIUS server</li> <li>• Transmission line quality</li> </ul>	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"> <li>• Communication between the Switch and the RADIUS server is available.</li> <li>• The RADIUS server functionality is enabled.</li> </ul>	Server IP address

#	Log ID	Log type	Message text	Meaning and action	Additional information
83	WARNIN G	SYSTEM	Failed to connect to RADIUS server.	[Meaning] An attempt to connect to the RADIUS server failed. [Action] Check the following: <ul style="list-style-type: none"> <li>Communication between the Switch and the RADIUS server is available.</li> <li>The RADIUS server functionality is enabled.</li> </ul>	Server IPv6 address
84	WARNIN G	SYSTEM	Failed to connect to Accounting server.	[Meaning] An attempt to connect to the accounting server failed. [Action] Check the following: <ul style="list-style-type: none"> <li>Communication between the Switch and the accounting server is available.</li> <li>The accounting server functionality is enabled.</li> </ul>	Server IP address
85	WARNIN G	SYSTEM	Failed to connect to Accounting server.	[Meaning] An attempt to connect to the accounting server failed. [Action] Check the following: <ul style="list-style-type: none"> <li>Communication between the Switch and the accounting server is available.</li> <li>The accounting server functionality is enabled.</li> </ul>	Server IPv6 address
86	WARNIN G	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 25-14:* List of response messages for the show dot1x logging command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <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

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 25-25: Clearing IEEE 802.1X operation log messages*

```
> clear dot1x logging
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 25-15: List of response messages for the clear dot1x logging command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to 802.1X program.(Reason:Connection Error)	An attempt to connect to the IEEE 802.1X program failed. Re-execute the command. If the failure occurs frequently, use the <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

---

# 26. 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
clear web-authentication dead-interval-timer
```

---

## 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.

### Operation when a stack configuration is used

This command is not supported.

### Example

When USER01 is added as the user name, user0101 as the password, and 10 as the VLAN ID:

```
# set web-authentication user USER01 user0101 10
```

### Display items

None

### Impact on communication

None

### Response messages

Table 26-1: 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.

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Now another user is using WA command, please try again.	Another user is using a command for the Web authentication 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.

### Operation when a stack configuration is used

This command is not supported.

### Example

Changing the password for user USER01:

```
# set web-authentication passwd USER01 user0101 user1111
```

### Display items

None

### Impact on communication

None

### Response messages

Table 26-2: List of response messages for the set web-authentication passwd command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Now another user is using WA command, please try again.	Another user is using a command for the Web authentication 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.

### Operation when a stack configuration is used

This command is not supported.

### 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 26-3: List of response messages for the set web-authentication vlan command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Now another user is using WA command, please try again.	Another user is using a command for the Web authentication 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 the user without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

### Operation when a stack configuration is used

This command is not supported.

### 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 26-4: List of response messages for the remove web-authentication user command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Now another user is using WA command, please try again.	Another user is using a command for the Web authentication functionality. Wait a while, and then retry the operation.

Message	Description
Unknown user '<user name>'.	The specified user has not been registered.
WA is not configured.	The Web authentication 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
- set authentication passwd
- set authentication vlan
- remove web-authentication user

User information is displayed in ascending order of user name.

### Syntax

```
show web-authentication user {edit | commit}
```

### Input mode

Administrator mode

### Parameters

{edit | commit}

edit

Displays user information being edited.

commit

Displays operating user information.

### Operation when a stack configuration is used

This command is not supported.

### Example

- When displaying the user information being edited:

```
# show web-authentication user edit
Date 20XX/10/14 10:52:49 UTC
Total user counts:2
username          VLAN
0123456789012345  3
USER01            4094
```

- When displaying information of the user who is performing operation:

```
# show web-authentication user commit
Date 20XX/10/14 10:52:49 UTC
Total user counts:3
username          VLAN
0123456789012345  4
USER02            4094
USER03            2
```

### Display items

*Table 26-5: Display items of users registered for Web authentication*

Item	Meaning	Displayed information
Total user counts	Total number of registered users	The number of registered users

Item	Meaning	Displayed information
username	User name	A registered user name
VLAN	VLAN	The VLAN set for the registered user

## Impact on communication

None

## Response messages

*Table 26-6:* List of response messages for the show web-authentication user command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Now another user is using WA command, please try again.	Another user is using a command for the Web authentication 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

### Operation when a stack configuration is used

This command is not supported.

### Example

The following shows an example of displaying authenticated users:

- When the authentication mode is legacy mode:

```
# show web-authentication login
Date 20XX/10/15 10:52:49 UTC
Total user counts:2
Username
VLAN    MAC address      Login time                Limit time
01234567890123456789012345678901
   3    0012.e2e3.9166  20XX/11/15 09:58:04 UTC  00:10:20
USER01
4094    0012.e268.7527   20XX/11/15 10:10:23 UTC  00:20:35
```

- When the authentication mode is dynamic VLAN mode:

```
# show web-authentication login
Date 20XX/10/15 10:52:49 UTC
Total user counts:2
F Username
VLAN    MAC address      Login time                Limit time
* 01234567890123456789012345678901
   3    0012.e2e3.9166  20XX/10/15 09:58:04 UTC  00:10:20
* USER01
4094    0012.e268.7527   20XX/10/15 10:10:23 UTC  00:20:35
```

- When the authentication mode is fixed VLAN mode:

```
# show web-authentication login
Date 20XX/10/15 10:52:49 UTC
Total user counts:2
F Username
VLAN    MAC address      Port  IP address
Login time                Limit time
* 01234567890123456789012345678901
   3    0012.e2e3.9166   0/5   192.168.0.1
20XX/10/15 09:58:04 UTC  00:10:20
* USER01
4094    0012.e268.7527   0/6   192.168.1.10
20XX/10/15 10:10:23 UTC  00:20:35
```

## Display items

Table 26-7: Items displayed for authenticated users

Item	Meaning	Displayed information
Total user counts	Total number of users	The number of the authenticated, currently login users
F	Forced authentication indication	Forcibly authenticated terminals *: Indicates that the terminal was forcibly authenticated.
Username	User name	The name of the authenticated, currently login user.
VLAN	VLAN	The VLAN set for the authenticated, currently login users
MAC address	MAC address	The MAC address of the authenticated, currently login user
Port	Port number	The number of the physical port accommodating the authenticated, currently login users (displayed for fixed VLAN mode)
IP address	IP address	The IP address of the authenticated, currently login users (displayed for fixed VLAN mode)
Login time	Login date and time	The time when the authenticated, currently login user logged in
Limit time	Remaining login time	The remaining login time of the authenticated, currently login user. 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. When the maximum connection time is 10 to 1440 minutes: <code>hh:mm:ss</code> hour:minute:second When the maximum connection time is set to unlimited: infinity

## Impact on communication

None

## Response messages

Table 26-8: List of response messages for the show web-authentication login command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <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.

### Operation when a stack configuration is used

This command is not supported.

### Example

#### ■ When the parameter is omitted:

```
# show web-authentication logging
Date 20XX/11/15 10:52:49 UTC
No=1:Nov 15 00:09:50:NORMAL:LOGIN:MAC=0012.e200.0001 USER=testdata1 Login
succeeded.
No=2:Nov 15 00:10:10:NORMAL:LOGOUT: MAC=0012.e200.0001 USER=testdata1
Logout succeeded.
No=90:Nov 15 00:09:55:NORMAL:SYSTEM: connection failed ; L2MacManager.
```

#### ■ When user is specified for the parameter:

```
# show web-authentication logging user
Date 20XX/11/15 11:13:15 UTC
No=1:Nov 15 00:09:50:NORMAL:LOGIN: MAC=0012.e200.0001 USER=testdata1 Login
succeeded.
No=2:Nov 15 00:10:10:NORMAL:LOGOUT: MAC=0012.e200.0001 USER=testdata1
Logout succeeded.
```

### Display items

Table 26-9: Items 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 26-12: 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 26-10: Log ID and type in operation log messages*.
- Log type: See *Table 26-10: Log ID and type in operation log messages*.
- Additional information: See *Table 26-11: Additional information*.
- List of messages: See *Table 26-12: List of operation log messages*.

*Table 26-10: 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 26-11: 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 26-12: 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 <sup>#1</sup> VLAN ID <sup>#1</sup> Port number <sup>#1</sup>

#	Log ID	Log type	Message text	Meaning and action	Additional information
2	NORMAL	LOGOUT	Logout succeeded.	[Meaning] Client successfully canceled authentication. [Action] None	MAC address User name IP address <sup>#1</sup> VLAN ID <sup>#1</sup> Port number <sup>#1</sup>
3	NORMAL	LOGIN	Login update succeeded.	[Meaning] The user's login time was successfully updated. [Action] None	MAC address User name IP address <sup>#1</sup> VLAN ID <sup>#1</sup> Port number <sup>#1</sup>
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 <sup>#1</sup> VLAN ID <sup>#1</sup> Port number <sup>#1</sup>
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 <sup>#1</sup> VLAN ID <sup>#1</sup> Port number <sup>#1</sup>
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 <sup>#1</sup> VLAN ID <sup>#1</sup> Port number <sup>#1</sup>
7	NORMAL	LOGOUT	Force logout ; VLAN deleted.	[Meaning] Authentication was canceled because a VLAN for Web authentication was deleted. Alternatively, authentication was canceled because dynamically registered VLANs were deleted by executing the <code>switchport mac configuration</code> command with the <code>vlan</code> parameter specified for the authentication port. [Action] Check the VLAN configuration settings.	MAC address User name VLAN ID

#	Log ID	Log type	Message text	Meaning and action	Additional information
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 <sup>#1</sup> VLAN ID Port number <sup>#1</sup>
10	NOTICE	LOGIN	Login failed ; User name not found to web authentication DB.	[Meaning] Authentication failed because the specified user ID was not registered in the internal DB, or the number of characters for the user ID was out of range. [Action] Use the correct user ID to log in.	User name
11	NOTICE	LOGIN	Login failed ; Password not found to web authentication DB. [Password=[password]]	[Meaning] Authentication failed because a password was not entered or the entered password was incorrect. [Action] Use the correct password to log in.	User name Password
12	NOTICE	LOGIN	Login failed ; ARP resolution.	[Meaning] Authentication failed because ARP resolution of the client PC's IP address failed. [Action] Log in again.	User name IP address
13	NOTICE	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 <sup>#1</sup> IP address

#	Log ID	Log type	Message text	Meaning and action	Additional information
14	NOTICE	LOGIN	Login failed ; Double login.	<p>[Meaning] Authentication failed because duplicated login operation was performed. The cause is either of the following:</p> <ul style="list-style-type: none"> <li>• The user has already logged in the same client PC using a different user ID.</li> <li>• In dynamic VLAN mode, the user has already logged in the same client PC in a different VLAN</li> </ul> <p>[Action] Log in from another PC. Alternatively, log out from the same client PC, and then log in again.</p>	MAC address User name
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"> <li>• The capacity limit for Web authentication has already been exceeded.</li> <li>• The total number of IEEE 802.1X authentications, Web authentications, and MAC-based authentications exceeded the capacity limit.</li> </ul> <p>[Action] Log in again when the number of authenticated users drops low enough.</p>	MAC address User name
16	NOTICE	LOGIN	Login failed ; The login failed because of hardware restriction.	<p>[Meaning] Authentication cannot be performed because the MAC address could not be registered due to hardware limitations.</p> <p>[Action] Log in from another PC.</p>	MAC address User name

#	Log ID	Log type	Message text	Meaning and action	Additional information
17	NOTICE	LOGIN	Login failed ; VLAN not specified.	[Meaning] Authentication could not be performed because the VLAN ID did not match the VLAN ID set for Web authentication. [Action] Set the correct VLAN ID in the configuration.	MAC address User name VLAN ID
18	NOTICE	LOGIN	Login failed ; MAC address could not register.	[Meaning] Authentication could not be performed because registration of the MAC address failed. [Action] Log in again.	MAC address User name
19	NOTICE	LOGOUT	Logout failed ; MAC address could not delete.	[Meaning] Authentication could not be performed because deletion of the MAC address failed. [Action] Log out again.	MAC address <sup>#2</sup> User name <sup>#1, #2</sup> VLAN ID <sup>#1, #2</sup> Port number <sup>#1, #2</sup>
20	NOTICE	LOGIN	Login failed ; RADIUS authentication failed.	[Meaning] Authentication could not be performed because RADIUS authentication failed. [Action] Use the correct user ID to log in.	MAC address User name IP address <sup>#1</sup> VLAN ID <sup>#1</sup> Port number <sup>#1</sup>
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 User name IP address <sup>#1</sup> VLAN ID <sup>#1</sup> Port number <sup>#1</sup>
22	NOTICE	LOGIN	Login failed ; Connection failed L2MacManager.	[Meaning] Authentication failed because an attempt to communicate with the VLAN program failed. [Action] Log in again. If this message appears frequently, specify the <code>mac-manager</code> parameter for the <code>restart vlan</code> command and execute it.	MAC address User name

#	Log ID	Log type	Message text	Meaning and action	Additional information
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
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"> <li>• IEEE 802.1X authentication performed on the same PC after Web authentication.</li> <li>• After Web authentication, the same MAC address as the authenticated terminal is registered by using the <code>mac-address</code> configuration command.</li> </ul> <p>[Action] Analyze the cause and log in again.</p>	MAC address

#	Log ID	Log type	Message text	Meaning and action	Additional information
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 performed. The cause is either of the following:</p> <ul style="list-style-type: none"> <li>The terminal for which Web authentication was performed had already been authenticated by IEEE 802.1X or MAC authentication.</li> <li>The MAC address for the terminal to be authenticated had already been registered by the <code>mac-address</code> configuration command.</li> </ul> <p>[Action] Use another terminal to log in.</p>	MAC address User name VLAN ID
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. [Action] Configure the VLAN (MAC VLAN) again.</p>	[Legacy mode] MAC address User name VLAN ID
				<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. [Action] Configure the VLAN again.</p>	[Fixed VLAN mode or Dynamic VLAN mode] MAC address User name IP address VLAN ID Port number
27	NOTICE	LOGIN	Login failed ; VLAN not specified.	<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. [Action] Correctly configure the VLAN again.</p>	MAC address User name VLAN ID

#	Log ID	Log type	Message text	Meaning and action	Additional information
28	NORMAL	LOGOUT	Force logout ; Polling time out.	[Meaning] Authentication was canceled because disconnection of an authenticated terminal was detected. [Action] None	MAC address User name IP address VLAN ID Port number
29	NORMAL	LOGOUT	Force logout ; Client moved.	[Meaning] Authentication was canceled because it was detected that the port of an authenticated terminal was moved. [Action] Log in again.	MAC address User name IP address VLAN ID Port number
31	NORMAL	LOGOUT	Force logout ; Port not specified.	[Meaning] Authentication has been canceled because the setting for the authentication port was deleted. [Action] Check the configuration.	MAC address User name IP address VLAN ID Port number
32	NOTICE	LOGIN	Login update failed.	[Meaning] The login time could not be updated because re-authentication of the user failed. [Action] Log in again using the correct user ID and password.	MAC address User name IP address
33	NORMAL	LOGOUT	Force logout ; Port link down.	[Meaning] Authentication of all users logged in for the port was canceled because the link for the applicable port was down. [Action] After confirming that the port status is link-up, log in again.	MAC address User name IP address VLAN ID Port number
34	NOTICE	LOGIN	Login failed ; Port not specified.	[Meaning] Authentication cannot be performed because the request was not issued from the port set for fixed VLAN mode or dynamic VLAN mode. [Action] Connect the terminal to the port to be authenticated, and then log in again.	MAC address User name Port number

#	Log ID	Log type	Message text	Meaning and action	Additional information
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
41	NORMAL	LOGOUT	Force logout ; Other authentication program.	<p>[Meaning] Authentication was canceled because it was overwritten by another authentication operation.</p> <p>[Action] Make sure other authentication methods are not used for login from the same terminal.</p>	MAC address User name IP address VLAN ID Port number
48	NORMAL	LOGOUT	Force logout ; Program stopped.	<p>[Meaning] Authentication of all users was canceled because the Web authentication program has stopped.</p> <p>[Action] To use Web authentication uninterruptedly for authentication, set the configuration.</p>	MAC address User name IP address VLAN ID Port number
49	NORMAL	LOGOUT	Force logout ; Authentic mode had changed (dynamic vlan -> static vlan).	<p>[Meaning] Authentication of all users was canceled because the authentication method was switched from legacy mode or dynamic VLAN mode to fixed VLAN mode.</p> <p>[Action] None</p>	MAC address User name IP address <sup>#1</sup> VLAN ID Port number <sup>#1</sup>
50	NORMAL	LOGOUT	Force logout ; Authentic mode had changed (static vlan -> dynamic vlan).	<p>[Meaning] Authentication of all users was canceled because the authentication method was switched from fixed VLAN mode to legacy mode or dynamic VLAN mode.</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
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
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
54	NORMAL	LOGIN	Force login succeeded.	[Meaning] Forced authentication succeeded. [Action] None	MAC address User name IP address VLAN ID Port number
55	NORMAL	LOGIN	Force login update succeeded.	[Meaning] Updating of the user's login time by forced authentication was successful. [Action] None	MAC address User name IP address VLAN ID Port number
56	NOTICE	LOGIN	Login failed ; Number of login was beyond limit of port.	[Meaning] Authentication cannot be performed because the maximum login limit for a port was exceeded. [Action] Reduce the number of terminals to be authenticated.	MAC address User name IP address VLAN ID Port number

#	Log ID	Log type	Message text	Meaning and action	Additional information
57	NORMAL	LOGOUT	Force logout ; Number of login was beyond limit of port.	[Meaning] Authentication was canceled because the number of ports after moving terminals exceeded the maximum allowable number. [Action] Reduce the number of terminals to be authenticated.	MAC address User name IP address VLAN ID Port number
82	NORMAL	SYSTEM	Accepted clear auth-state command.	[Meaning] A request issued by the <code>clear web-authentication auth-state command</code> to cancel authentication was received. [Action] None	n/a
83	NORMAL	SYSTEM	Accepted clear statistics command.	[Meaning] A request issued by the <code>clear web-authentication statistics command</code> to clear statistics was received. [Action] None	n/a
84	NORMAL	SYSTEM	Accepted commit command.	[Meaning] A commit notification issued by the <code>commit web-authentication command</code> for the internal DB was received. [Action] None	n/a
85	NORMAL	SYSTEM	Accepted dump command.	[Meaning] A dump output request issued by the <code>dump protocols web-authentication command</code> 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.[ <i>error code</i> ]	<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=[ <i>error-code</i> ]	<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. <i>[error code]</i>	[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

#	Log ID	Log type	Message text	Meaning and action	Additional information
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 <sup>#1</sup> VLAN ID Port number <sup>#1</sup>
110	NORMAL	SYSTEM	Accepted clear dead-interval-timer command.	[Meaning] A request issued by the <code>clear web-authentication dead-interval-timer</code> command for recovering the dead interval functionality was received. [Action] None	n/a

#	Log ID	Log type	Message text	Meaning and action	Additional information
255	ERROR	SYSTEM	The other error. [ <i>error-code</i> ]	<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 26-13: List of response messages for the show web-authentication logging command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <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.

---

## show web-authentication

---

Displays the configuration for Web authentication.

### Syntax

```
show web-authentication
```

### Input mode

Administrator mode

### Parameters

None

### Operation when a stack configuration is used

This command is not supported.

### Example

- When the authentication mode is legacy mode and the authentication method is local authentication with no registered VLANs:

```
# show web-authentication
Date 20XX/10/15 10:52:49 UTC
web-authentication Information:
  Authentic-mode   : Legacy
  Authentic-method : Local           Accounting-state : disable
    Max-timer     : 60               Max-user       : 256
    VLAN Count    : 0               Auto-logout    : enable
  Syslog-send      : enable
  Jump-URL          : http://www.example.com/
  Web-port          : http   : 80           https   : 443
```

- When the authentication mode is legacy mode and the authentication method is local authentication with registered VLANs:

```
# show web-authentication
Date 20XX/10/15 10:52:49 UTC
web-authentication Information:
  Authentic-mode   : Legacy
  Authentic-method : Local           Accounting-state : disable
    Max-timer     : 60               Max-user       : 256
    VLAN Count    : 16               Auto-logout    : disable
  Syslog-send      : enable
  Jump-URL          : http://www.example.com/
  Web-port          : http   : 80           https   : 443
```

```
VLAN Information:
  VLAN ID :      5,10,15,20,25,30,35,40,1000-1007
```

- When the authentication mode is fixed VLAN mode and the authentication method is RADIUS authentication with registered VLANs:

```
# show web-authentication
Date 20XX/10/15 10:52:49 UTC
web-authentication Information:
  Authentic-mode   : Static-VLAN
  Authentic-method : RADIUS           Accounting-state : disable
  Dead-interval    : 10
    Max-timer     : 60               Max-user       : 256
    VLAN Count    : -               Auto-logout    : -
  Syslog-send      : enable
  Alive-detection  : enable
    timer         : 60   interval-timer : 3   count      : 3
```

```

URL-redirect      : enable      Protocol : http
Jump-URL          : http://www.example.com/
Web-IP-address    : 192.168.1.1
FQDN              : aaa.example.com
Web-port          : http : 80, 8080      https : 443, 8443
ARP-relay Port    : 0/1-2
Force-Authorized  : disable
Auth-max-user     : 1024

```

```

Port      : 0/1
VLAN ID   : 5,10,15
Access-list-No: 100
Max-user  : 64

```

```

Port      : 0/2
VLAN ID   : 15-16
Access-list-No: 100
Max-user  : 64

```

- When the authentication mode is dynamic VLAN mode and the authentication method is local authentication:

```

# show web-authentication
Date 20XX/10/15 10:52:49 UTC
web-authentication Information:
Authentic-mode      : Dynamic-VLAN
Authentic-method    : Local          Accounting-state : disable
Dead-interval       : 10
Max-timer            : 60              Max-user       : 256
VLAN Count          : -               Auto-logout    : disable
Syslog-send         : enable
URL-redirect        : enable      Protocol : http
Jump-URL            : http://www.example.com/
Web-IP-address      : 192.168.1.1
FQDN                : aaa.example.com
Web-port            : http : 80, 8080      https : 443, 8443
ARP-relay Port      : 0/10,12
Force-Authorized    : enable
Auth-max-user       : 1024

```

```

Port      : 0/10
VLAN ID   : 1000,1500
Native VLAN : 10
Forceauth VLAN: 1000
Access-list-No: 100
Max-user  : 64

```

```

Port      : 0/12
VLAN ID   : 1000,1500
Native VLAN : 10
Forceauth VLAN: -
Access-list-No: 100
Max-user  : 64

```

- When the authentication mode is dynamic VLAN mode and the authentication method is RADIUS authentication:

```

# show web-authentication
Date 20XX/10/15 10:52:49 UTC
web-authentication Information:
Authentic-mode      : Dynamic-VLAN
Authentic-method    : RADIUS          Accounting-state : enable
Dead-interval       : 10
Max-timer            : 60              Max-user       : 256
VLAN Count          : -               Auto-logout    : disable
Syslog-send         : enable
URL-redirect        : enable      Protocol : http

```

```

Jump-URL           : http://www.example.com/
Web-IP-address     : 192.168.1.1
FQDN               : aaa.example.com
Web-port           : http : 80, 8080      https : 443, 8443
ARP-relay Port     : 0/10,12
Force-Authorized   : enable
Auth-max-user      : 1024

```

```

Port               : 0/10
VLAN ID            : 1000,1500
Native VLAN        : 10
Forceauth VLAN:    : 1000
Access-list-No:    : 100
Max-user           : 256

```

```

Port               : 0/12
VLAN ID            : 1000,1500
Native VLAN        : 10
Forceauth VLAN:    : -
Access-list-No:    : 100
Max-user           : 256

```

## Display items

Table 26-14: 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.
Dead-interval	RADIUS connection retry interval	The interval time (in minutes) at which a RADIUS connection attempt is retried if a RADIUS connection fails
Max-timer	Maximum connection time	Maximum connection time (in minutes) for a login user
Max-user	Maximum number of authenticated users	The maximum number of authenticated users who can log in to the Web authentication 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 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

Item	Meaning	Displayed information
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	Sending interval of monitoring packet 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	Usage state of URL redirection in Web authentication enable: Used disable: Not used
Protocol	http/https type	Login page type to be displayed on a terminal. http: Login page is displayed 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
ARP-relay port	ARP relay	The number of the port that is used as a relay port if arp-relay is specified. - is displayed if arp-relay is not configured.
Force-Authorized	Status of forced authentication	Status of forced authentication. enable: Forced authentication is enabled. disable: Forced authentication is disabled.
Auth-max-user	Maximum number of authenticated users allowed on the switch	Maximum number of authenticated users allowed on the switch
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

Item	Meaning	Displayed information
Forceauth VLAN	VLAN setting for forced authentication	The VLAN ID switched to when forced authentication is performed in dynamic VLAN mode. If this information is not set by using a configuration command, a hyphen (-) is displayed. This item is not displayed in fixed VLAN mode.
Access-list No.	Access Lists	Access list number or access list name. - is displayed if neither is set.
Max-user	Maximum number of authenticated users allowed on each port	Maximum number of authenticated users allowed on each port. If this information is not set by using a configuration command, a hyphen (-) is displayed.

## Impact on communication

None

## Response messages

*Table 26-15: List of response messages for the show web-authentication command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <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

### Operation when a stack configuration is used

This command is not supported.

### Example

- Below is an example of executing the command when the authentication mode is fixed or dynamic VLAN mode, the authentication method is local or forced authentication, there is no RADIUS definition, and no user information is registered in the internal Web authentication database.

```
# show web-authentication statistics
Date 20XX/10/15 11:10:49 UTC
web-authentication Information:
  Authentication Request Total :      100
  Authentication Current Count :       10
  Authentication Error Total   :       30
  Force Authorized Count       :       10
Port Information:
  Port      User-count
  0/10      5/ 256
  0/12      5/1024
```

- When the authentication mode is fixed VLAN mode or dynamic VLAN mode, and the authentication method is RADIUS authentication:

```
# show web-authentication statistics
Date 20XX/10/15 11:10:49 UTC
web-authentication Information:
  Authentication Request Total :      100
  Authentication Current Count :       10
  Authentication Error Total   :       30
  Force Authorized Count       :       10
RADIUS web-authentication Information:
[RADIUS frames]
  TxTotal   :      10  TxAccReq  :      10  TxError   :       0
  RxTotal   :      30  RxAccAccpt:      10  RxAccRejct:      10
                        RxAccChllg:      10  RxInvalid  :       0
Account web-authentication Information:
[Account frames]
  TxTotal   :      10  TxAccReq  :      10  TxError   :       0
  RxTotal   :      20  RxAccResp :      10  RxInvalid  :       0
Port Information:
  Port      User-count
  0/10      5/ 256
  0/12      5/1024
```

- When the authentication mode is legacy mode and the authentication method is local authentication:

```
# show web-authentication statistics
```

```

Date 20XX/10/12 11:10:49 UTC
web-authentication Information:
  Authentication Request Total :      100
  Authentication Current Count :      10
  Authentication Error Total   :      30

```

- When the authentication mode is legacy mode and the authentication method is RADIUS authentication:

```

# show web-authentication statistics
Date 20XX/10/12 11:10:49 UTC
web-authentication Information:
  Authentication Request Total :      100
  Authentication Current Count :      10
  Authentication Error Total   :      30
RADIUS web-authentication Information:
[RADIUS frames]
  TxTotal   :      10  TxAccReq   :      10  TxError    :      0
  RxTotal   :      30  RxAccAccpt:      10  RxAccRejct:     10
                        RxAccChllg:      10  RxInvalid  :      0
Account web-authentication Information:
[Account frames]
  TxTotal   :      10  TxAccReq   :      10  TxError    :      0
  RxTotal   :      20  RxAccResp  :      10  RxInvalid  :      0

```

## Display items

Table 26-16: Items displayed for statistics related to Web authentication

Item	Meaning
Authentication Request Total	The total number of authentication requests
Authentication Current Count	The number of users currently authenticated
Authentication Error Total	The total number of authentication request errors
Force Authorized Count	The number of users forcibly authenticated at this time. Note that this item is not displayed in legacy mode.
RADIUS frames	RADIUS information
TxTotal	The total number of packets 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
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

Item	Meaning
RxAccResp	The total number of Accounting-Response packets received from the accounting server
RxInvalid	The total number of invalid frames received from the accounting server
Port Information	Port information. Note that this item is not displayed in legacy mode.
Port	Port number
User-count	The number of authenticated users for each port and the maximum number of users that can be authenticated for each port. This information is displayed in $m/n$ format where $m$ is the number of authenticated users, and $n$ is the maximum number of users that can be authenticated.

### Impact on communication

None

### Response messages

*Table 26-17:* List of response messages for the show web-authentication statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <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 logging

---

Clears log information for Web authentication.

### Syntax

```
clear web-authentication logging
```

### Input mode

Administrator mode

### Parameters

None

### Operation when a stack configuration is used

This command is not supported.

### Example

The following shows an example of clearing log information for Web authentication.

```
# clear web-authentication logging
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 26-18:* List of response messages for the clear web-authentication logging command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <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

### Operation when a stack configuration is used

This command is not supported.

### 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 26-19:* List of response messages for the clear web-authentication statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <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.

### Operation when a stack configuration is used

This command is not supported.

### 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 26-20: 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.	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.

### Operation when a stack configuration is used

This command is not supported.

### Example

When the authdata backup file for Web authentication user information is created:

```
# store web-authentication authdata
Backup web-authentication user data. Are you sure? (y/n): y
Backup complete.
```

### Display items

None

### Impact on communication

None

### Response messages

Table 26-21: List of response messages for the store web-authentication command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Now another user is using WA command, please try again.	Another user is using a command for the Web authentication 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 20XX/04/01 19:46:29 JST
Flash :
      user area   config area   dump area   area total
used   37,063kB      65kB         16kB      37,144kB
free    616kB       7,199kB       8,152kB     15,967kB
total  37,679kB      7,265kB       8,168kB     53,112kB
```

Note: The underlined part (the value for free indicating the free capacity of the user area) must be at least 20 kB.

If the free capacity in flash memory is insufficient, use the `rm` command to delete unnecessary files before creating the backup files.

---

## load web-authentication

---

Restores Web authentication user information from a backup file for Web authentication user information. Note that information registered or changed by using the following commands will be replaced by the information that is being restored:

- set web-authentication user
- set web-authentication passwd
- set web-authentication vlan
- remove web-authentication user
- commit web-authentication

### Syntax

```
load web-authentication <file name> [-f]
```

### Input mode

Administrator mode

### Parameters

<file name>

Specify the name of the backup file from which Web authentication user information is restored.

-f

Restores Web authentication user information without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

### Operation when a stack configuration is used

This command is not supported.

### 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 26-22: 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.

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.
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 login 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 login 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 login users.

mac-address <mac>

<mac>

Forces user logout by specifying the MAC address that is used by the authenticated, currently login 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.

### Operation when a stack configuration is used

This command is not supported.

### Example

- When forcing logout of authenticated, currently login 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 login 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 26-23:* List of response messages for the clear web-authentication auth-state command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <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 login 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 the Web authentication program and the Web server 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.

### Operation when a stack configuration is used

This command is not supported.

### 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 26-24:* 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"> <li>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.</li> </ul>

## 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

### Operation when a stack configuration is used

This command is not supported.

### 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 26-25:* 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

Reply-Message page: loginProcess.html

Login success page: loginOK.html

Login failed page: loginNG.html

Logout page: logout.html

Logout success page: logoutOK.html

Logout failed page: logoutNG.html

Authentication error messages: webauth.msg

Icons to be displayed 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.

## Operation when a stack configuration is used

This command is not supported.

## 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 1263 Dec 6 09:59 loginProcess.html
-rwxr-xr-x operator users 1302 Dec 6 09:59 loginNG.html
-rwxr-xr-x operator users 1300 Dec 6 09:59 loginOK.html
-rwxr-xr-x operator users 843 Dec 6 09:59 logout.html
-rwxr-xr-x operator users 869 Dec 6 09:59 logoutNG.html
-rwxr-xr-x operator users 992 Dec 6 09:59 logoutOK.html
-rwxr-xr-x operator users 109 Dec 6 09:59 webauth.msg
-rwxr-xr-x operator users 199 Dec 6 09:59 favicon.ico
-rwxr-xr-x operator users 20045 Dec 6 09:59 aaa.gif

# set web-authentication html-files k-html
Would you wish to install new html-files ? (y/n):y
Executing...
Install complete.
```

## Display items

None

## Impact on communication

None

## Response messages

*Table 26-26: 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 put a sub directory in the directory.	The specified directory contains a subdirectory.
Can't specify "/config/wa/htdocs" in this command.	The /config/wa/htdocs directory cannot be specified.
Directory size over.	The capacity of the specified directory exceeds the limit (1024KB).
Install operation failed.	An attempt to register the file failed.
No login.html file in the directory.	There is no login.html file in the specified directory.
No such directory.	The specified directory does not exist.
Too many files.	The number of files exceeds the limit of 100.

## Notes

- This command does not check the contents of the HTML files. If the contents of the specified file are incorrect, login and logout operations for Web authentication might not be possible.
- This command can be executed regardless of whether or not the configuration command for Web authentication has been set.
- Page images, messages, and icons registered by using this command are retained when Web authentication is performed, the Web server is restarted, and a switch is restarted.
- The total capacity of a file that can be registered is 1024 KB. If the capacity exceeds 1024 KB,

the file cannot be registered.

- A maximum of 100 files can be registered. If there are too many files, command execution might take time.
- If this command is interrupted while it is being executed, the registered page is not displayed, but the default page is displayed. In addition, the result might not be displayed correctly by using the `show web-authentication html-files` command. If this happens, re-execute this command to register page images and messages.
- In the dynamic VLAN mode or the legacy mode, if you associate the `loginOK.html` file with another file, the login success page might not be displayed correctly.

---

## clear web-authentication html-files

---

Deletes the Web authentication pages, messages, and icons registered by the `set web-authentication html-files` command, and reverts to the default settings.

### Syntax

```
clear web-authentication html-files [-f]
```

### Input mode

Administrator mode

### Parameters

`-f`

Deletes the pages, messages, and icons without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following 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 26-27:* 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.
Clear operation failed.	An attempt to delete the file failed.

### Notes

This command can be executed regardless of whether or not the configuration command for Web authentication has been set.

---

## show web-authentication html-files

---

Displays the size of the file (in bytes) registered by the `set web-authentication html-files` command and the date and time registered. If no file has been registered, that the default setting is being used is displayed.

### Syntax

```
show web-authentication html-files [detail]
```

### Input mode

Administrator mode

### Parameters

detail

Specify this parameter if you want to display information about individual files that are not the HTML file, msg (message) file, and ico (icon) file (such as GIF files).

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.

### Operation when a stack configuration is used

This command is not supported.

### 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 20XX/04/15 10:07:04 UTC
TOTAL SIZE      :      62777
-----
                SIZE      DATE
login.html      :      2049  20XX/04/10 14:05
loginProcess.html :      2002  20XX/04/10 14:05
loginOK.html     :      1046  20XX/04/10 14:05
loginNG.html     :       985  20XX/04/10 14:05
logout.html      :       843  20XX/04/10 14:05
logoutOK.html    :       856  20XX/04/10 14:05
logoutNG.html    :       892  20XX/04/10 14:05
webauth.msg      :       104  20XX/04/10 14:05
favicon.ico      :         0  default now
the other files  :     54000  20XX/04/10 14:05
```

#### ■ When the file is not registered (the default information is displayed):

```
# show web-authentication html-files
Date 20XX/04/15 10:07:04 UTC
TOTAL SIZE      :      6993
-----
                SIZE      DATE
login.html      :      1108  default now
loginProcess.html :      1263  default now
loginOK.html     :      1046  default now
loginNG.html     :       985  default now
logout.html      :       843  default now
logoutOK.html    :       856  default now
logoutNG.html    :       892  default now
webauth.msg      :         0  default now
```

```

favicon.ico      :          0      default now
the other files :          0      default now

```

- When 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 20XX/04/15 10:07:04 UTC
```

```
TOTAL SIZE      :      62777
```

```

-----
              SIZE      DATE
login.html    :      2049  20XX/04/10 14:05
loginProcess.html  2002  20XX/04/10 14:05
loginOK.html   :      1046  20XX/04/10 14:05
loginNG.html   :        985  20XX/04/10 14:05
logout.html    :        843  20XX/04/10 14:05
logoutOK.html  :        856  20XX/04/10 14:05
logoutNG.html  :        892  20XX/04/10 14:05
webauth.msg    :        104  20XX/04/10 14:05
favicon.ico    :          0  default now
aaa.gif        :     20000  20XX/04/10 14:05
bbb.gif        :     15000  20XX/04/10 14:05
ccc.gif        :     10000  20XX/04/10 14:05
ddd.gif        :        9000  20XX/04/10 14:05

```

## Display items

None

## Impact on communication

None

## Response messages

*Table 26-28:* 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.

## Notes

This command can be executed regardless of whether or not the configuration command for Web authentication has been set.

---

## clear web-authentication dead-interval-timer

---

If the first RADIUS server becomes unresponsive and the dead interval functionality causes the switch to start using the second or later RADIUS server, the `clear web-authentication dead-interval-timer` command resumes access to the first RADIUS server before the time specified by the `authentication radius-server dead-interval` configuration command has elapsed.

### Syntax

```
clear web-authentication dead-interval-timer
```

### Input mode

Administrator mode

### Parameters

None

### Operation when a stack configuration is used

This command is not supported.

### Example

The command in the following example disables the dead interval functionality so that access to the second or later RADIUS server is canceled:

```
# clear web-authentication dead-interval-timer
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 26-29:* List of response messages for the `clear web-authentication dead-interval-timer` command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to WA program.	Communication with the Web authentication program failed. Re-execute the command. If communication fails frequently, use the <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



## Chapter

---

# 27. 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
clear mac-authentication dead-interval-timer
```

---

## show mac-authentication login

---

Displays the authenticated, currently login terminals in ascending order by login date and time.

### Syntax

```
show mac-authentication login
```

### Input mode

Administrator mode

### Parameters

None

### Operation when a stack configuration is used

This command is not supported.

### Example

The following shows an example of displaying authenticated MAC addresses:

```
# show mac-authentication login
Date 20XX/10/15 10:52:49 UTC
Total client counts:2
F MAC address      Port   VLAN   Login time                Limit time  Mode
* 0012.e200.0001   0/1    3      20XX/10/15 09:58:04 UTC   00:10:20   Static
* 0012.e200.0002   0/10   4094   20XX/10/15 10:10:23 UTC   00:20:35   Dynamic
```

### Display items

The following table describes the items displayed for authenticated MAC addresses.

*Table 27-1: Items displayed for authenticated MAC addresses*

Item	Meaning	Displayed information
Total client counts	Total number of terminals	The number of authenticated, currently login terminals
F	Forced authentication indication	Forcibly authenticated terminals *: Indicates that the terminal was forcibly authenticated.
MAC address	MAC address	The MAC addresses of authenticated, currently login terminals
Port	Port number	The physical port numbers of the ports where the authenticated, currently login terminal is located
VLAN	VLAN	VLANs set for the authenticated, currently login terminals. VLANs that were switched after authentication in dynamic VLAN mode.
Login time	Login date and time	Login times of the authenticated, currently login terminals

Item	Meaning	Displayed information
Limit time	Remaining login time	Remaining login time of the authenticated, currently login terminals. 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. When the maximum connection time is from 10 to 1440 (minutes): <code>hh:mm:ss</code> hour:minute:second When the maximum connection time is set to unlimited: infinity
Mode	Operating mode	Authenticated mode. <code>Static</code> : Authenticated in fixed VLAN mode <code>Dynamic</code> : Authenticated in dynamic VLAN mode

### Impact on communication

None

### Response messages

Table 27-2: List of response messages for the show mac-authentication login command

Message	Description
Can't execute.	The command could not be executed.
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <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.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following examples show operation log messages displayed for MAC-based authentication.

■ When the parameter is omitted:

```
# show mac-authentication logging
Date 20XX/12/01 10:52:49 UTC
No=1:Dec 1 10:09:50:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=0/1 VLAN=3 Login
succeeded.
No=2:Dec 1 10:10:10:NORMAL:LOGOUT: MAC=0012.e212.0001 PORT=0/1 VLAN=3
Logout succeeded.
No=3:Dec 1 10:10:55:NORMAL:SYSTEM: accepted clear auth-state command.
```

■ When client is specified for the parameter:

```
# show mac-authentication logging client
Date 20XX/12/01 11:13:15 UTC
No=1:Dec 1 10:09:50:NORMAL:LOGIN: MAC=0012.e200.0001 PORT=0/1 VLAN=3 Login
succeeded.
No=2:Dec 1 10:10:10:NORMAL:LOGOUT: MAC=0012.e212.0001 PORT=0/1 VLAN=3
Logout succeeded.
```

### Display items

The following table describes the items displayed for MAC-based authentication operation log messages.

*Table 27-3: 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=0/1 VLAN=3 Login succeeded.  
 (1) (2) (3) (4) (5) (6) (7)

- (1) Message number: Indicates the number assigned to each message shown in *Table 27-6: 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 27-4: Log ID and type in operation log messages*.
- Log type: See *Table 27-4: Log ID and type in operation log messages*.
- Additional information: See *Table 27-5: Additional information*.
- List of messages: See *Table 27-6: List of operation log messages*.

*Table 27-4: 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 27-5: Additional information*

Display format	Meaning
MAC=xxxx.xxxx.xxxx	Indicates the MAC address.
VLAN=xxxx	Indicates the VLAN ID. Note, however, that this is not displayed if VLAN ID information could not be acquired.
PORT=xx/xx	Indicates the port number.

*Table 27-6: 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

#	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. Alternatively, authentication was canceled because dynamically registered VLANs were deleted by executing the <code>switchport mac</code> configuration command with the <code>vlan</code> parameter specified for the authentication port.</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"> <li>• The capacity limit for MAC-based authentication has already been exceeded.</li> <li>• The total number of IEEE 802.1X authentications, Web authentications, and MAC-based authentications exceeded the capacity limit.</li> </ul> <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. <i>[error-code]</i>	[Meaning] Authentication could not be performed because registration of the MAC address failed. [Action] Attempt authentication again. If <i>error-code</i> is <code>HARDWARE_RESTRICTION</code> , log in from another PC.	MAC address Error code
19	NOTICE	LOGOUT	Logout failed ; MAC address could not delete. <i>[error-code]</i>	[Meaning] An attempt to delete MAC address failed. [Action] Attempt de-authentication again.	MAC address <sup>#1</sup> VLAN ID <sup>#1</sup> Port number <sup>#1</sup> 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
33	NORMAL	LOGIN	Force login succeeded.	[Meaning] Forced authentication for the terminal was successful. [Action] None	MAC address VLAN ID Port number
34	NORMAL	LOGIN	Un-authorized Port Accepted.	[Meaning] Communication with an authentication-exempted terminal was detected. [Action] None	MAC address VLAN ID Port number
35	NORMAL	LOGOUT	Force logout ; Interface mode had changed.	[Meaning] Authentication was canceled because the interface mode of the MAC port for which <code>dot1q</code> is set was changed. [Action] None	MAC address VLAN ID Port number
36	NOTICE	LOGIN	Login failed ; Number of login was beyond limit of port.	[Meaning] Authentication cannot be performed because the maximum login limit for a port was exceeded. [Action] Reduce the number of terminals to be authenticated.	MAC address VLAN ID Port number
37	NORMAL	LOGOUT	Force logout ; Number of login was beyond limit of port.	[Meaning] Authentication was canceled because the number of ports after moving terminals exceeded the maximum allowable number. [Action] Reduce the number of terminals to be authenticated.	MAC address VLAN ID Port number
82	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

#	Log ID	Log type	Message text	Meaning and action	Additional information
84	NORMAL	SYSTEM	Accepted commit command.	[Meaning] A notification issued by the commit mac-authentication 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 dump protocols mac-authentication 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
88	ERROR	SYSTEM	Macauthd could not initialize.[error-code]	[Meaning] Initializing the MAC-based authentication program failed. [Action] Check the configurations of MAC-based authentication. If this message appears frequently, use the restart mac-authentication command to restart the MAC-based authentication program.	Error code
89	ERROR	SYSTEM	Connection failed ; Operation command. error=[error-code]	[Meaning] Outputting the response message for the command failed. [Action] Wait a while, and then re-execute the command.	Error code

#	Log ID	Log type	Message text	Meaning and action	Additional information
90	ERROR	SYSTEM	Connection failed ; L2MacManager.	[Meaning] An attempt to communicate with the VLAN program was made, but failed. [Action] If this message appears frequently, specify the <code>mac-manager</code> parameter for the <code>restart vlan</code> command and execute it.	n/a
92	ERROR	SYSTEM	Disconnection failed ; L2MacManager.	[Meaning] Communication with the VLAN program was interrupted. [Action] If this message appears frequently, specify the <code>mac-manager</code> parameter for the <code>restart vlan</code> command and execute it.	n/a
93	ERROR	SYSTEM	Program failed ; Configuration command. [error-code]	[Meaning] An attempt to read the configuration failed. [Action] Use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.	Error code
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

#	Log ID	Log type	Message text	Meaning and action	Additional information
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 clear mac-authentication logging command was received. [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

#	Log ID	Log type	Message text	Meaning and action	Additional information
107	NOTICE	LOGIN	Login failed ; MAC address not found to MAC authentication DB.	<p>[Meaning] Authentication failed because the MAC address to be authenticated was not registered in the internal MAC-based authentication DB.</p> <p>[Action] Make sure the MAC address registered in the internal MAC-based authentication DB is correct.</p>	MAC address VLAN ID <sup>#2</sup>
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
110	NORMAL	SYSTEM	Accepted clear dead-interval-timer command.	<p>[Meaning] A request issued by the <code>clear mac-authentication dead-interval-timer</code> command for recovering the dead interval functionality was received.</p> <p>[Action] None</p>	n/a
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 27-7:* List of response messages for the show mac-authentication logging command

Message	Description
Can't execute.	The command could not be executed.
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <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.

---

## show mac-authentication

---

Displays the configuration for MAC-based authentication.

### Syntax

```
show mac-authentication
```

### Input mode

Administrator mode

### Parameters

None

### Operation when a stack configuration is used

This command is not supported.

### Example

The following examples show configuration information displayed for MAC-based authentication.

- When a port for MAC-based authentication is not registered:

```
# show mac-authentication
Date 20XX/10/15 10:52:49 UTC
mac-authentication Information:
  Authentic-method : RADIUS           Accounting-state : disable
  Dead-interval   : 10
  Syslog-send     : enable
  Force-Authorized : disable
  Auth-max-user   : 1024

  Authentic-mode   : Static-VLAN
    Max-timer      : 60                      Max-terminal : 256
    Port Count     : 0                      Auto-logout  : enable
  VLAN-check      : enable
  Vid-key         : %VLAN

  Authentic-mode   : Dynamic-VLAN
    Max-timer      : 60                      Max-terminal : 256
    Port Count     : 0                      Auto-logout  : enable
```

- When a port for MAC-based authentication is registered:

```
# show mac-authentication
Date 20XX/10/15 10:52:49 UTC
mac-authentication Information:
  Authentic-method : RADIUS           Accounting-state : disable
  Dead-interval   : 10
  Syslog-send     : enable
  Force-Authorized : enable
  Auth-max-user   : 1024

  Authentic-mode   : Static-VLAN
    Max-timer      : 60                      Max-terminal : 256
    Port Count     : 2                      Auto-logout  : enable
  VLAN-check      : enable
  Vid-key         : %VLAN

  Authentic-mode   : Dynamic-VLAN
    Max-timer      : 60                      Max-terminal : 256
    Port Count     : 2                      Auto-logout  : enable

Port Information:
  Port              : 0/1
```

```

Static-VLAN      :
  VLAN ID       : 5,10,15
  Auth type     : force-authorized
Dynamic-VLAN     :
  VLAN ID       : 1200,1500
  Native VLAN   : 10
  Forceauth VLAN: 1500
Access-list-No   : 100
Max-user        : 64

Port            : 0/2
Dynamic-VLAN    :
  VLAN ID       : 1300-1310
  Native VLAN   : 20
  Forceauth VLAN: 1300
Access-list-No  : 100
Max-user        : 64

Port            : 0/10
Static-VLAN     :
  VLAN ID       : 300,305
Access-list-No  : 100
Max-user        : 64

```

## Display items

Table 27-8: 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.
Dead-interval	RADIUS connection retry interval	The interval time (in minutes) at which a RADIUS connection attempt is retried if a RADIUS connection fails
Syslog-send	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
Force-Authorized	Status of forced authentication	Status of forced authentication. enable: Forced authentication is enabled. disable: Forced authentication is disabled.
Auth-max-user	Maximum number of authenticated users allowed on the switch	Maximum number of authenticated users allowed on the switch
Authentic-mode	Authentication mode	Authentication mode for MAC-based authentication. 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

Item	Meaning	Displayed information
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 when authentication is performed by MAC-based authentication in fixed VLAN mode. enable: The VLAN ID is checked. disable: The VLAN ID is not checked.
Vid-key	Character string to be added to the account name when RADIUS authentication is performed.	Character strings to be added to the account name when authentication request is sent to the RADIUS server.
Port	Port information	The number of the port registered for MAC-based authentication
VLAN ID	VLAN information	The ID of the VLAN to which a port, which is registered for MAC-based authentication, belongs. In dynamic VLAN mode, the VLAN ID specified for the MAC VLAN is displayed.
Auth type	Setting that determines whether authentication is required for tagged frames	Whether to permit communication without authentication for terminals that use tagged frames to communicate over a MAC port. force-authorized: Permit communication without authentication. mac auth: Authentication is required.
Native VLAN	VLAN ID of a native VLAN	The VLAN ID of the native VLAN set for the port for dynamic VLAN mode
Forceauth VLAN	VLAN setting for forced authentication	The VLAN ID switched to when forced authentication is performed in dynamic VLAN mode. If this information is not set by using a configuration command, a hyphen (-) is displayed. This item is not displayed in fixed VLAN mode.
Access-list No.	Access Lists	Access list number or access list name. - is displayed if neither is specified.
Max-user	Maximum number of authenticated users allowed on each port	Maximum number of authenticated users allowed on each port. If this information is not set by using a configuration command, a hyphen (-) is displayed.

### Impact on communication

None

## Response messages

*Table 27-9:* List of response messages for the show 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

None

## show mac-authentication statistics

Displays MAC-based authentication statistics.

### Syntax

```
show mac-authentication statistics
```

### Input mode

Administrator mode

### Parameters

None

### Operation when a stack configuration is used

This command is not supported.

### Example

The following shows an example of displaying MAC-based authentication statistics:

```
# show mac-authentication statistics
Date 20XX/10/15 11:10:49 UTC
mac-authentication Information:
  Authentication Request Total :      100
  Authentication Current Count :       10
  Authentication Error Total   :       30
  Force Authorized Count       :       10
Unauthorized Information:
  Unauthorized Client Count    :         5
RADIUS mac-authentication Information:
[RADIUS frames]
      TxTotal   :      10  TxAccReq  :      10  TxError   :         0
      RxTotal   :      30  RxAccAccpt:      10  RxAccRejct:      10
                        RxAccChllg:      10  RxInvalid  :         0
Account mac-authentication Information:
[Account frames]
      TxTotal   :      10  TxAccReq  :      10  TxError   :         0
      RxTotal   :      20  RxAccResp :      10  RxInvalid  :         0
Port Information:
  Port      User-count
  0/10      5/ 256
  0/12      5/1024
```

### Display items

Table 27-10: 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
Force Authorized Count	Number of users forcibly authenticated at this time
Unauthorized Information	Information about authentication-exempted terminals
Unauthorized Client Count	Number of current authentication-exempted terminals
RADIUS frames	RADIUS information
TxTotal	The total number of packets transmitted to the RADIUS server

Item	Meaning
TxAccReq	The total number of Access-Request packets sent to the RADIUS server
TxError	The number of errors occurring during transmission to the RADIUS server
RxTotal	The total number of received packets from the RADIUS server
RxAccAccept	The total number of Access-Accept packets received from the RADIUS server
RxAccReject	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
Port Information	Port information
Port	Port number
User-count	Total number of authenticated terminals and authentication-exempted terminals for the port / maximum number of terminals that can be authenticated set for the port. This information is displayed in $m/n$ format where $m$ is the number of authenticated users, and $n$ is the maximum number of users that can be authenticated.

## Impact on communication

None

## Response messages

*Table 27-11:* List of response messages for the show mac-authentication statistics command

Message	Description
Can't execute.	The command could not be executed.
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <code>restart mac-authentication</code> command to restart the MAC-based authentication program.

Message	Description
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 login 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 login terminals.

-f

Forcibly logs out terminals without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following 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 27-12:* List of response messages for the clear mac-authentication auth-state command

Message	Description
Can't execute.	The command could not be executed.
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <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

### Operation when a stack configuration is used

This command is not supported.

### 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 27-13:* List of response messages for the clear mac-authentication logging command

Message	Description
Can't execute.	The command could not be executed.
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <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

### Operation when a stack configuration is used

This command is not supported.

### 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 27-14:* List of response messages for the clear mac-authentication statistics command

Message	Description
Can't execute.	The command could not be executed.
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <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:

In fixed VLAN mode, the VLAN ID is not checked at authentication time.

In dynamic VLAN mode, an authentication error occurs during authentication for the specified MAC address.

### Operation when a stack configuration is used

This command is not supported.

### Example

To add 0012.e200.1234 as the MAC address and 10 as the VLAN ID:  

```
# set mac-authentication mac-address 0012.e200.1234 10
```

### Display items

None

### Impact on communication

None

## Response messages

*Table 27-15:* List of response messages for the set mac-authentication mac-address command

Message	Description
Already mac address "<mac>","<vlan id>" exists.	The specified MAC address has already been registered.
Can't execute.	The command could not be executed. Re-execute the command.
Mac-authentication is not configured.	The MAC-based authentication 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.

### Operation when a stack configuration is used

This command is not supported.

### 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 27-16:* List of response messages for the remove mac-authentication mac-address command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Mac-authentication is not configured.	The MAC-based authentication 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 already 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.

### Operation when a stack configuration is used

This command is not supported.

### 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 27-17: List of response messages for the commit mac-authentication command*

Message	Description
Can not commit.	An attempt to update the authentication information failed. Execute the <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.

### Operation when a stack configuration is used

This command is not supported.

### Example

- When displaying information that is being edited:

```
# show mac-authentication mac-address edit
Date 20XX/12/01 10:52:49 UTC
Total mac-address counts:2
mac-address          VLAN
0012.e200.1234       3
0012.e201.abcd       4094
```

- When displaying information about the current internal MAC-based authentication DB:

```
# show mac-authentication mac-address commit
Date 20XX/12/01 10:52:49 UTC
Total mac-address counts:3
mac-address          VLAN
0012.e200.1234       4
0012.e201.abcd       4094
0012.e202.6789       2
```

### Display items

*Table 27-18: 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

Item	Meaning	Displayed information
VLAN	VLAN	The VLAN set for a registered MAC address. A hyphen (-) is displayed if no VLANs are set.

### Impact on communication

None

### Response messages

*Table 27-19:* List of response messages for the show mac-authentication mac-address command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Mac-authentication is not configured.	The MAC-based authentication 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.

### Operation when a stack configuration is used

This command is not supported.

### 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 27-20: List of response messages for the store mac-authentication command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Mac-authentication command is not configured.	The MAC-based authentication 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 20XX/12/01 19:46:29 JST
Flash :
```

	user area	config area	dump area	area total
used	37,063kB	65kB	16kB	37,144kB
free	616kB	7,199kB	8,152kB	15,967kB
total	37,679kB	7,265kB	8,168kB	53,112kB

Note: The underlined part (the value for `free` indicating the free capacity of the user area) must be at least 100 kB.

If the free capacity in flash memory is insufficient, use the `rm` command to delete unnecessary files before creating the backup files.

---

## load mac-authentication

---

Restores the internal MAC-based authentication DB from a backup file to the internal MAC-based authentication DB. Note that the contents registered or changed by the following commands will be replaced by the contents of the restored backup:

- set mac-authentication mac-address
- remove mac-authentication mac-address
- commit mac-authentication

### Syntax

```
load mac-authentication <file name> [-f]
```

### Input mode

Administrator mode

### Parameters

<file name>

Specify the name of the backup file from which the internal MAC-based authentication DB is to be restored.

-f

Restores the internal MAC-based authentication DB without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

### Operation when a stack configuration is used

This command is not supported.

### 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 27-21: List of response messages for the load mac-authentication command

Message	Description
Can not load.	An attempt to update the internal MAC-based authentication DB failed. Execute the <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 the MAC-based authentication program 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.

### Operation when a stack configuration is used

This command is not supported.

### 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 login terminals are canceled and communication will be impossible.

After the MAC-based authentication program is restarted, you must perform authentication again.

### Response messages

*Table 27-22: 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

### Operation when a stack configuration is used

This command is not supported.

### 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 27-23:* 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.

---

## clear mac-authentication dead-interval-timer

---

If the first RADIUS server becomes unresponsive and the dead interval functionality causes the switch to start using the second or later RADIUS server, the `clear mac-authentication dead-interval-timer` command resumes using the first RADIUS server before the time specified by the `authentication radius-server dead-interval` configuration command has elapsed.

### Syntax

```
clear mac-authentication dead-interval-timer
```

### Input mode

Administrator mode

### Parameters

None

### Operation when a stack configuration is used

This command is not supported.

### Example

The command in the following example disables the dead interval functionality so that access to the second or later RADIUS server is canceled:

```
# clear mac-authentication dead-interval-timer
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 27-24:* List of response messages for the `clear mac-authentication dead-interval-timer` command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to mac-authentication program.	Communication with the MAC-based authentication program failed. Re-execute the command. If communication fails frequently, use the <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



## Chapter

---

# 28. 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.

### Operation when a stack configuration is used

This command is not supported.

### Example

- The following shows an example of displaying all configured VLANaccessAgent information:

```
>show fense server
Date 20XX/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 fence server detail
Date 20XX/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 28-1: Items displayed for VLANAccessAgent information

Item	Meaning	Displayed information
VAA NAME	VLANAccessAgent name	Displays the name set for VLANAccessAgent of a Switch. <i>switch-name</i> : 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 <sup>#</sup>	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 &lt;vlan id list&gt; 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.

Item	Meaning	Displayed information
Status	Startup status	Indicates the startup and termination settings for VLANAccessAgent. enable: Running. disable: Disabled
Agent Status <sup>#</sup>	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 <sup>#</sup>	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 4093: Indicates the number of VLANs.

<sup>#</sup>: A parameter value which is changed dynamically according to the operating status of VLANAccessAgent. For other parameters, information is displayed according to the configuration.

The following table shows the items displayed for the detailed VLANAccessAgent information.

Table 28-2: Items displayed for detailed information about VLANAccessAgent

Item	Meaning	Displayed information
VAA NAME	VLANAccessAgent name	Displays the name set for VLANAccessAgent of a Switch. <i>switch-name</i> : 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. <i>NoSync</i> : Indicates that inter-switch asynchronous mode is enabled. <i>Sync</i> : Indicates normal mode.
Current Registered MAC <sup>#</sup>	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 &lt;vlan id list&gt; dynamic</code> command.
Server Information	Authentication server information	Lists information about the authentication server.
ID	VLANAccessAgent ID	Indicates <i>vaa_id</i> in the connection information set for VLANAccessAgent. 1 to 10: Indicates <i>vaa_id</i> .
Status	Startup status	Indicates the running or stopped settings for VLANAccessAgent. <i>enable</i> : Running. <i>disable</i> : Disabled
Agent Status <sup>#</sup>	Server status	Indicates the authentication server status from the following categories. <i>CONNECTED</i> : Indicates the status that connection with the authentication server is established. <i>DISCONNECTED</i> : Indicates the status that connection with the authentication server is disconnected. <i>SUSPENDED</i> : Indicates the status that the VLANAccessAgent functionality is disabled. <i>INVALID</i> : 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. <i>IP-address</i> : 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. <i>infinity</i> : Indicates an unlimited number of retries. 0 to 32767: Indicates the number of retries.
Current Count <sup>#</sup>	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.

Item	Meaning	Displayed information
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 4093: Indicates the number of VLANs.
Target-VLAN Information	Authenticated MAC VLAN information	Lists the information registered as authenticated MAC VLANs.
VLAN ID	VLAN ID	Indicates the ID of a VLAN set as an authenticated VLAN. 2 to 4093: 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 28-3: 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.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following shows an example of displaying statistics for all VLANAccessAgent you have set:

```
>show fense statistics
Date 20XX/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 28-4: 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 a Keep Alive message from the authentication server within the interval set by the fense alive-timer configuration 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.
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.

Item	Meaning	Displayed information
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 28-5: 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.
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.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following shows an example of displaying VLANaccessAgent operation log messages:

```
> show fense logging
Date 20XX/10/01 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 28-7: List of operation log messages* shows the list of operation log messages.

*Table 28-6: 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 28-7: 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"> <li>vaa_id</li> <li>Subnet address</li> <li>MAC address</li> </ul>
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"> <li>vaa_id</li> <li>MAC address</li> <li>error code</li> </ul>
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"> <li>vaa_id</li> <li>Subnet address</li> <li>MAC address</li> </ul>
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"> <li>vaa_id</li> <li>MAC address</li> <li>error code</li> </ul>
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"> <li>vaa_id</li> <li>Subnet address</li> </ul>
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"> <li>vaa_id</li> <li>Subnet address</li> <li>error code</li> </ul>
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"> <li>vaa_id</li> <li>MAC address</li> </ul>
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"> <li>vaa_id</li> <li>Version of the authentication server</li> <li>Authentication server IP address</li> </ul>
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"> <li>vaa_id</li> <li>Received data</li> </ul>
10	NOTICE	The connection with the authentication server succeeded. id=<vaa_id>	Successfully connected to the authentication server.	<ul style="list-style-type: none"> <li>vaa_id</li> </ul>
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"> <li>vaa_id</li> <li>The number of retries</li> </ul>

#	Level	Message text	Meaning	Additional information
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"> <li>vaa_id</li> <li>vlan_no</li> <li>MAC address</li> <li>error code</li> </ul>
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"> <li>vaa_id</li> <li>MAC address</li> </ul>
14	ERROR	Failed to open socket . Code=<error-code>	An attempt to open a socket failed.	<ul style="list-style-type: none"> <li>error code</li> </ul>
15	WARNING	The socket with L2MacManager was closed. Code=<error-code>	The socket connection to L2MacManager was closed.	<ul style="list-style-type: none"> <li>error code</li> </ul>
16	ERROR	Configuration data setting failed. Code=<error-code>	An attempt to set the Vlan-Port information failed.	<ul style="list-style-type: none"> <li>error code</li> </ul>
17	WARNING	Device open error. Code=<error-code>	An attempt to acquire a MAC address table entry failed.	<ul style="list-style-type: none"> <li>error code</li> </ul>

## Impact on communication

None

## Response messages

Table 28-8: 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.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following shows an example of clearing statistics for VLANAccessAgent.

```
> clear fense statistics
>
```

### Display items

None

### Impact on communication

None

### Response messages

Table 28-9: 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

### Operation when a stack configuration is used

This command is not supported.

### 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 28-10:* 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.

### Operation when a stack configuration is used

This command is not supported.

### 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 28-11: 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.

Message	Description
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 a file with this name already exists, the file is overwritten unconditionally. Therefore, backup 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

### Operation when a stack configuration is used

This command is not supported.

### Example

The following shows an example of specifying a VLANaccessAgent dump:

```
> dump protocols vaa
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 28-12:* 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 a file with this name already exists, the file is overwritten unconditionally. Therefore, backup the file in advance, if necessary.

## Chapter

---

# 29. 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.>
- fortygigabitethernet <nif no.>/<port no.> [AX3800S]
- 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 each parameter is omitted:

This command can display only the entries that meet the conditions specified by the parameter. If no parameters are set, entries are displayed with no condition applied. If multiple parameters are specified, the entries conforming to the conditions will be displayed.

Operation when all parameters are omitted:

Displays all entries.

## Operation when a stack configuration is used

This command is not supported.

## Example

The following figure shows an example of displaying all DHCP snooping entries.

*Figure 29-1: Result of executing the DHCP snooping binding database display command*

```
> show ip dhcp snooping binding
Date 20XX/04/20 12:00:00 UTC
Agent URL: flash
Last succeeded time: 20XX/04/20 11:50:00 UTC
Total Bindings Used/Max      :      5/   3070
Total Source guard Used/Max:    2/   3070

Bindings: 5
MAC Address      IP Address      Expire(min)  Type      VLAN  Port
0012.e287.0001   192.168.0.201    -            static*    1     0/1
0012.e287.0002   192.168.0.204    1439         dynamic    2     0/4
0012.e287.0003   192.168.0.203    -            static     3     0/3
0012.e287.0004   192.168.0.202    3666         dynamic    4     ChGr:2
0012.e2be.b0fb   192.168.100.11   59           dynamic*   12    0/11
>

> show ip dhcp snooping binding 192.168.0.202
Date 20XX/04/20 12:00:00 UTC
Agent URL: flash
Last succeeded time: 20XX/04/20 11:50:00 UTC
Total Bindings Used/Max      :      5/   3070
Total Source guard Used/Max:    2/   3070

Bindings: 1
MAC Address      IP Address      Expire(min)  Type      VLAN  Port
0012.e287.0004   192.168.0.202    3666         dynamic    4     ChGr:2
>
```

## Display items

*Table 29-1: 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 <sup>#</sup> (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"> <li>The agent URL is not specified.</li> <li>The database has never been saved.</li> <li>The number of entries to be restored is zero.</li> </ul>
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

Item	Meaning	Displayed information
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.
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 : 32

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 29-2: List of response messages for the show ip dhcp snooping binding command

Message	Description
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not operating.
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.>
- fortygigabitethernet <nif no.>/<port no.> [AX3800S]
- 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 each parameter is omitted:

This command can clear only the entries that meet the conditions specified by the parameter. If no parameters are specified, the entries are cleared without being limited by any conditions. If multiple parameters are specified, the entries conforming to the conditions will be cleared.

Operation when all parameters are omitted:

Clears all the dynamically registered entries.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure shows an example of clearing all the dynamically registered entries.

*Figure 29-2:* 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 29-3:* List of response messages for the clear ip dhcp snooping binding command

Message	Description
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not operating.
Illegal Port -- <i>&lt;port no.&gt;</i> .	The specified port number is invalid. Make sure the specified parameter is correct, and then try again. <i>&lt;port no.&gt;</i> : Indicates the port number.
Program error occurred: <i>&lt;error message&gt;</i>	A program error occurred. Re-execute the command. <i>&lt;error message&gt;</i> : Location of the error

## Notes

None

---

## show ip dhcp snooping statistics

---

Displays an example of displaying statistics for DHCP snooping.

### Syntax

```
show ip dhcp snooping statistics
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure shows an example of displaying statistics for DHCP snooping.

*Figure 29-3: Result of executing the command for displaying statistics for DHCP snooping*

```
> show ip dhcp snooping statistics
Date 20XX/04/20 12:00:00 UTC
Database Exceeded: 0
Total DHCP Packets: 8995
Port          Recv          Filter
0/1           170           170
0/3           1789          10
:
0/25          0             0
ChGr:1        3646          2457
>
```

### Display items

*Table 29-4: 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, or fortygigabitethernet when an AX3800S series switch is used, the NIF number and the port number are displayed. For port-channel, the following value is displayed: ChGr: 1 to ChGr: 32
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 29-5:* List of response messages for the show ip dhcp snooping statistics command

Message	Description
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not operating.
Program error occurred: <i>&lt;error message&gt;</i>	A program error occurred. Re-execute the command. <i>&lt;error message&gt;</i> : Location of the error

**Notes**

1. If VLAN tunneling is used on the switch and DHCP snooping is enabled for the default VLAN, access ports with no VLAN specified are also displayed using this command.
2. When port mirroring is used, if DHCP snooping is enabled 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

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure shows an example of clearing the DHCP snooping statistics.

*Figure 29-4:* 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 29-6:* List of response messages for the clear ip dhcp snooping statistics command

Message	Description
DHCP snooping doesn't seem to be running.	The command failed because DHCP snooping is not operating.
Program error occurred: <i>&lt;error message&gt;</i>	A program error occurred. Re-execute the command. <i>&lt;error message&gt;</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

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure shows an example of displaying statistics for dynamic ARP inspection.

*Figure 29-5: Result of executing the command for displaying the statistics for dynamic ARP inspection*

```
> show ip arp inspection statistics
Date 20XX/04/20 12:00:00 UTC
Port      Forwarded      Dropped  ( DB mismatch      Invalid  )
0/1        0                15      (      15          0      )
0/2        584             883      (      883         0      )
0/3        0                0        (      0           0      )
          :
ChGr:2      170             53      (      53          0      )
>
```

### Display items

*Table 29-7: Items displayed for statistics for dynamic ARP inspection*

Item	Meaning	Displayed information
Port	Port number	If the interface is gigabitethernet or tengigabitethernet, or fortygigabitethernet when an AX3800S series switch is used, the NIF number and the port number are displayed. For port-channel, the following value is displayed: ChGr:1 to ChGr:32
Forwarded	Number of forwarded ARP packets	n/a
Dropped	Total number of discarded ARP packets	Total number of packets listed in the <b>DB mismatch</b> and <b>Invalid</b> items.
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 29-8: 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.
Program error occurred: <i>&lt;error message&gt;</i>	A program error occurred. Re-execute the command. <i>&lt;error message&gt;</i> : Location of the error

## Notes

1. If VLAN tunneling is used on the switch and dynamic ARP inspection is enabled for the default VLAN, access ports with no VLAN specified are also displayed using this command.
2. When port mirroring is used, if dynamic ARP inspection is enabled in the default VLAN, the mirror port is also displayed using this command.

---

## clear ip arp inspection statistics

---

Clears the dynamic ARP inspection statistics.

### Syntax

```
clear ip arp inspection statistics
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure shows an example of clearing dynamic ARP inspection statistics.

*Figure 29-6:* 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 29-9:* 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.
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.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure shows an example of displaying an operation log message for DHCP snooping.

*Figure 29-7: Result of executing the command for displaying an operation log message of DHCP snooping*

```
> show ip dhcp snooping logging
Date 20XX/04/20 12:00:00 UTC
Apr 20 11:00:00 ID=2201 NOTICE DHCP server packets were received at an untrust
port(0/2/1/0012.e2ff.fe01/192.168.100.254) .
>
```

### Display items

The following shows the display format of a message.

```
Apr 20 11:00:00 ID=2201 NOTICE DHCP server packets were received at an untrust
(1)      (2)      (3)      (4)                                     (5)
port(0/2/1/0012.e2ff.fe01/192.168.100.254) .
```

- (1) Date: Displays the date (month and day) when the event indicated in the 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 29-10: Levels and their description*

Level	Type	Description
ERROR	Problem	Interruption of communication is detected or configurations of events were inconsistent.

Level	Type	Description
WARN	Warning	Malicious packets were detected or events that occurred when configurations were inconsistent.
NOTICE	Notification	Errors that occur during normal operation or events that occurred when configurations were inconsistent.
INFO	Regular	A normal event that occurs during normal operation

## (5) Message text

The following table shows the contents of operation log messages.

Table 29-11: 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] &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;nif no.&gt;: Indicates the NIF number.            &lt;port no.&gt;: Indicates the port number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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] &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;nif no.&gt;: Indicates the NIF number.            &lt;port no.&gt;: Indicates the port number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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] &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;nif no.&gt;: Indicates the NIF number.            &lt;port no.&gt;: Indicates the port number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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] &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;nif no.&gt;: Indicates the NIF number.            &lt;port no.&gt;: Indicates the port number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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] &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;nif no.&gt;: Indicates the NIF number.            &lt;port no.&gt;: Indicates the port number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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] &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;nif no.&gt;: Indicates the NIF number.            &lt;port no.&gt;: Indicates the port number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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:&lt;channel group number&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;channel group number&gt;: Indicates the channel group number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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:&lt;channel group number&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;channel group number&gt;: Indicates the channel group number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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:&lt;channel group number&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;channel group number&gt;: Indicates the channel group number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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:&lt;channel group number&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;channel group number&gt;: Indicates the channel group number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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:&lt;channel group number&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;channel group number&gt;: Indicates the channel group number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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:&lt;channel group number&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;channel group number&gt;: Indicates the channel group number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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.</p> <p>[Explanation of message variables] None.</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>
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.</p> <p>[Explanation of message variables] &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP server information.          &lt;nif no.&gt;: Indicates the NIF number.          &lt;port no.&gt;: Indicates the port number.          &lt;vlan id&gt;: Indicates the VLAN ID.          &lt;mac address&gt;: Indicates the MAC address.          &lt;ip address&gt;: Indicates the IP address.</p> <p>[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.</p> <p>[Explanation of message variables] &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.          &lt;nif no.&gt;: Indicates the NIF number.          &lt;port no.&gt;: Indicates the port number.          &lt;vlan id&gt;: Indicates the VLAN ID.          &lt;mac address&gt;: Indicates the MAC address.          &lt;ip address&gt;: 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
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.</p> <p>[Explanation of message variables] &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;nif no.&gt;: Indicates the NIF number.            &lt;port no.&gt;: Indicates the port number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: Indicates the IP address.</p> <p>[Action] If this occurs frequently, it might have been caused by an attack. Check the connected devices.</p>
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.</p> <p>[Explanation of message variables] &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;: Indicates ARP terminal information.            &lt;nif no.&gt;: Indicates the NIF number.            &lt;port no.&gt;: Indicates the port number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: 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.</p> <p>[Explanation of message variables] ChGr:&lt;channel group number&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP server information.            &lt;channel group number&gt;: Indicates the channel group number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: Indicates the IP address.</p> <p>[Action] Check the connected device.</p>

Message ID	Level	Message text	Description
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.</p> <p>[Explanation of message variables] ChGr:&lt;channel group number&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;channel group number&gt;: Indicates the channel group number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: Indicates the IP address.</p> <p>[Action] If this occurs frequently, it might have been caused by an attack. Check the connected devices.</p>
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:&lt;channel group number&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;channel group number&gt;: Indicates the channel group number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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:&lt;channel group number&gt;/&lt;vlan id&gt;/&lt;mac address&gt;: Indicates ARP terminal information.            &lt;channel group number&gt;: Indicates the channel group number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: 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>

Message ID	Level	Message text	Description
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. [Explanation of message variables] &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information. &lt;nif no.&gt;: Indicates the NIF number. &lt;port no.&gt;: Indicates the port number. &lt;vlan id&gt;: Indicates the VLAN ID. &lt;mac address&gt;: Indicates the MAC address. &lt;ip address&gt;: 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>
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. This message is output once every five minutes on a port-by-port basis. [Explanation of message variables] &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information. &lt;nif no.&gt;: Indicates the NIF number. &lt;port no.&gt;: Indicates the port number. &lt;vlan id&gt;: Indicates the VLAN ID. &lt;mac address&gt;: Indicates the MAC address. &lt;ip address&gt;: 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. This message is output once every five minutes on a port-by-port basis. [Explanation of message variables] &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;: Indicates ARP terminal information. &lt;nif no.&gt;: Indicates the NIF number. &lt;port no.&gt;: Indicates the port number. &lt;vlan id&gt;: Indicates the VLAN ID. &lt;mac address&gt;: 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
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. This message is output once every five minutes on a port-by-port basis.</p> <p>[Explanation of message variables] &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;: Indicates ARP terminal information. &lt;nif no.&gt;: Indicates the NIF number. &lt;port no.&gt;: Indicates the port number. &lt;vlan id&gt;: Indicates the VLAN ID. &lt;mac address&gt;: Indicates the MAC address.</p> <p>[Action] Check the connected devices because this might be caused by an attack.</p>
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] &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;: Indicates ARP terminal information. &lt;nif no.&gt;: Indicates the NIF number. &lt;port no.&gt;: Indicates the port number. &lt;vlan id&gt;: Indicates the VLAN ID. &lt;mac address&gt;: 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:&lt;channel group number&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information. &lt;channel group number&gt;: Indicates the channel group number. &lt;vlan id&gt;: Indicates the VLAN ID. &lt;mac address&gt;: Indicates the MAC address. &lt;ip address&gt;: 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
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. [Explanation of message variables] ChGr:&lt;channel group number&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.     &lt;channel group number&gt;: Indicates the channel group number.     &lt;vlan id&gt;: Indicates the VLAN ID.     &lt;mac address&gt;: Indicates the MAC address.     &lt;ip address&gt;: Indicates the IP address. [Action] Review the network configuration. If there is no problem in the configuration, then this might have been caused by an attack.</p>
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. [Explanation of message variables] ChGr:&lt;channel group number&gt;/&lt;vlan id&gt;/&lt;mac address&gt;: Indicates ARP terminal information.     &lt;channel group number&gt;: Indicates the channel group number.     &lt;vlan id&gt;: Indicates the VLAN ID.     &lt;mac address&gt;: Indicates the MAC address. [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. [Explanation of message variables] ChGr:&lt;channel group number&gt;/&lt;vlan id&gt;/&lt;mac address&gt;: Indicates ARP terminal information.     &lt;channel group number&gt;: Indicates the channel group number.     &lt;vlan id&gt;: Indicates the VLAN ID.     &lt;mac address&gt;: Indicates the MAC address. [Action] Check the connected devices because this might be caused by an attack.</p>

Message ID	Level	Message text	Description
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:&lt;channel group number&gt;/&lt;vlan id&gt;/&lt;mac address&gt;: Indicates ARP terminal information.            &lt;channel group number&gt;: Indicates the channel group number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.</p> <p>[Action] Check the connected devices because this might be caused by an attack.</p>
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]  &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;nif no.&gt;: Indicates the NIF number.            &lt;port no.&gt;: Indicates the port number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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]  &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;nif no.&gt;: Indicates the NIF number.            &lt;port no.&gt;: Indicates the port number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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>

Message ID	Level	Message text	Description
4204	ERROR	The number of the source guard entry exceeded the capacity of this port(<nif no.>/<port no.>/<vlan id>/<mac address>/<ip address>).	<p>[Meaning] The number of entries for the terminal filter exceeds the capacity limit of a port.</p> <p>[Explanation of message variables] &lt;nif no.&gt;/&lt;port no.&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;nif no.&gt;: Indicates the NIF number.            &lt;port no.&gt;: Indicates the port number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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:&lt;channel group number&gt;/&lt;vlan id&gt;/&lt;mac address&gt;/&lt;ip address&gt;: Indicates DHCP client terminal information.            &lt;channel group number&gt;: Indicates the channel group number.            &lt;vlan id&gt;: Indicates the VLAN ID.            &lt;mac address&gt;: Indicates the MAC address.            &lt;ip address&gt;: 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 29-12: 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: <error message>	A program error occurred. Re-execute the command. <error message>: Location of the error

## Notes

None

---

## clear ip dhcp snooping logging

---

Clears log messages collected by the DHCP snooping program.

### Syntax

```
clear ip dhcp snooping logging
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure shows an example of clearing log messages for the DHCP snooping.

*Figure 29-8:* 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 29-13:* 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.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 29-9:* 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 29-14:* 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.

---

## dump protocols dhcp snooping

---

Outputs to a file logs or internal information collected by the DHCP snooping program.

### Syntax

```
dump protocols dhcp snooping
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure shows an example of outputting logs or internal information for DHCP snooping to a file.

*Figure 29-10:* Result of executing the DHCP snooping dump command

```
> dump protocols dhcp snooping
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 29-15:* 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>&lt;error message&gt;</i>	A program error occurred. Re-execute the command. <i>&lt;error message&gt;</i> : Location of the error

### Notes

Output file: /usr/var/dhsn/dhcp\_snoopingd.dmp



## Chapter

---

# 30. 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 64.

[port <port list>] [channel-group-number <channel group list>]

Displays GSRP information about the specified port or the specified channel group. The port and the channel group can be specified at the same time. In that case, GSRP information for the specified port and the specified channel group is displayed.

port <port list>

For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*. 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.

### Operation when a stack configuration is used

This command is not supported.

## Example 1

Figure 30-1: Example of displaying GSRP summary information

```
> show gsrp
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 3
Local MAC Address      : 0012.e2a8.2527
Neighbor MAC Address   : 0012.e2a8.2505
Total VLAN Group Counts : 3
Layer 3 Redundancy     : On

VLAN Group ID   Local State   Neighbor State
1               Backup       Master
2               (disable)    -
8               Master       -

>
```

## Display items in Example 1

Table 30-1: Items displayed for GSRP summary information

Item	Meaning	Displayed information
GSRP ID	GSRP group ID	1-65535
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	0-64
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	1-64
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 30-2: Example of displaying GSRP information when a VLAN group ID is specified*

```

> show gsrp 3 vlan-group 1,2,8
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 3
Local MAC Address      : 0012.e2a8.2527
Neighbor MAC Address   : 0012.e2a8.2505
Total VLAN Group Counts : 3
Layer 3 Redundancy     : On

VLAN Group ID : 1
VLAN ID        : 110,200-2169
Member Port    : 0/6-8
Active Port    : 0/6-8
Last Transition : 20XX/07/14 10:00:00 (Master to Backup)
Transition by reason : Priority was lower than neighbor's
Master to Backup Counts : 4
Backup to Master Counts : 4
Virtual MAC Address : 0000.8758.1387

State          Local Neighbor
Acknowledged State : Backup Master
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

State          Local Neighbor
Acknowledged State : - -
Advertise Hold Timer : - -
Priority       : 100 -
Active Ports   : - -
Up Ports      : - -

VLAN Group ID : 8
VLAN ID        : 180
Member Port    : 0/6-8
Active Port    : 0/6-8
Last Transition : 20XX/07/14 11:00:00 (Backup to Master)
Transition by reason : "set gsrp master"command was executed
Master to Backup Counts : 0
Backup to Master Counts : 1
Virtual MAC Address : 0000.8758.13bf

State          Local Neighbor
Acknowledged State : Master -
Advertise Hold Timer : 0 -
Priority       : 100 -
Active Ports   : 3 -
Up Ports      : 3 -

```

>

## Display items in Example 2

Table 30-2: Items displayed for GSRP information when a VLAN group ID is specified

Item	Meaning	Displayed information
GSRP ID	GSRP group ID	1-65535
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	0-64
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	1-64
VLAN ID	VLAN ID	1-4094 When used in combination with Ring Protocol, VLANs that do not belong to the VLAN group are not included.
Member Port	Ports belonging to a VLAN which is configured for a VLAN group	- is displayed if no active ports belong to a VLAN group, or if the VLAN group is 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)	0-4294967295 - is displayed if the VLAN group is disabled.
Backup to Master Counts	Number of transitions from backup status to master status (statistics)	0-4294967295 - 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	0-255 (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 30-3: Example of displaying detailed GSRP information

```

> show gsrp detail
Date 20XX/11/07 12:00:00 UTC

GSRP ID: 3
Local MAC Address      : 0012.e2a8.2527
Neighbor MAC Address   : 0012.e2a8.2505
Total VLAN Group Counts : 3
GSRP VLAN ID          : 105
Direct Port            : 0/10-11
Limit Control          : Off
GSRP Exception Port    : 0/1-5
No Neighbor To Master  : manual
Backup Lock            : disable
Port Up Delay          : 0
Last Flush Receive Time : -
Forced Shift Time      : -

```

```

Layer 3 Redundancy      : On
Virtual Link ID        : 100 (VLAN ID : 20)

                        Local                      Neighbor
Advertise Hold Time    : 5                        5
Advertise Hold Timer   : 4                        -
Advertise Interval     : 1                        1
Selection Pattern      : ports-priority-mac      ports-priority-mac

VLAN Group ID          Local State                Neighbor State
1                      Backup                     Master
2                      (disable)                  -
8                      Master                      -
>

```

### Display items in Example 3

Table 30-3: Items displayed for detailed GSRP information

Item	Meaning	Displayed information
GSRP ID	GSRP group ID	1-65535
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	0-64
GSRP VLAN ID	VLAN ID used for transmitting Advertise frames	1-4094
Direct Port	Port used for transmitting Advertise frames	- is displayed if the port is not configured.
Limit Control	GSRP VLAN group-only control functionality	Off: Not set. On: GSRP VLAN group-only control functionality 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	1-250 - 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 advertise-holdtime configuration command is displayed.)
Advertise Hold Timer	Length of time that an Advertise frame continues to be active	0 to 120 (seconds) (- is displayed for information about the partner 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	1-64
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 30-4: Example of displaying GSRP information when a port is specified

```
> show gsrp 10 port 0/6-11
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
Port Information
0/6      GSRP      : Active      Port      : Up
        Type      : Member      Flush      : Reset      Delay      : 0
        TxFrame   : 0           RxFrame   : 0           Discard Frame : 0
0/7      GSRP      : Active      Port      : Up
        Type      : Member      Flush      : Reset      Delay      : 0
        TxFrame   : 0           RxFrame   : 0           Discard Frame : 0
0/8      GSRP      : Active      Port      : Up
        Type      : Member      Flush      : GSRP      Delay      : 0
        TxFrame   : 0           RxFrame   : 0           Discard Frame : 0
0/10     GSRP      : Not Active   Port      : Up
(CH: 1) Type      : Direct      Flush      : No           Delay      : 0
        TxFrame   : 960         RxFrame   : 954         Discard Frame : 0
0/11     GSRP      : Not Active   Port      : Up
(CH: 1) Type      : Direct      Flush      : No           Delay      : 0
        TxFrame   : 960         RxFrame   : 954         Discard Frame : 0

>
```

## Display items in Example 4

Table 30-4: Items displayed for GSRP information when a port is specified

Item	Meaning	Displayed information
GSRP ID	GSRP group ID	1-65535
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 adjacent 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 Advertise frames (statistics)	0-4294967295
RxFram	Number of received GSRP Advertise frames (statistics)	0-4294967295
Discard Frame	Number of GSRP Advertise frames discarded when they are received (statistics)	0-262140 (The maximum value is 65535 (the maximum number by reason why the frame is discarded) times 4 (the number of components).)

### Example 5

Figure 30-5: Items displayed for GSRP information when a port is specified

```
> show gsrp 10 port 0/6 detail
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
Port Information
0/6   GSRP      : Active      Port      : Up
      Type      : Member      Flush      : Reset      Delay       : 0
      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 30-5: Items displayed for GSRP information when a port is specified

Item	Meaning	Displayed information
GSRP ID	GSRP group ID	1-65535
Port Information	Port information	--
<nif no.>/<port no.>	Port number	--
CH	Channel group number	--
GSRP	Status of a port belonging to a VLAN which is configured for a VLAN group	Active: Indicates that the port status is active Not Active: Indicates that the port status is not active.
Port	Port status	Up: Indicates that the port is up. Down: Indicates that the port is down.
Type	Port type	Direct: Indicates that the port is a direct link port. Member: Indicates that the port belongs to a VLAN configured for a VLAN group.

Item	Meaning	Displayed information
Flush	Method of clearing <code>mac_address_table</code> for adjacent 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)	0-4294967295
RxFram	Number of received GSRP Advertise frames (statistics)	0-4294967295
Discard Frame	Number of GSRP Advertise frames discarded when they are received (statistics)	0-262140 (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)	0-65535
mismatch GSRP ID	Number of GSRP Advertise frames discarded due to GSRP ID mismatch (statistics)	0-65535 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)	0-65535
illegal GSRP frame	Number of GSRP Advertise frames discarded because an invalid GSRP Advertise frame was received. (statistics)	0-65535

## Impact on communication

None

## Response messages

Table 30-6: List of response messages for the show gsrp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to GSRP program.	Communication with the GSRP program failed. Re-execute the command. If the failure occurs frequently, use the <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:<gsrp group id>.	The specified GSRP group ID has not been configured. <gsrp group id>: Indicates the GSRP group ID.
Specified port is not operational.	The specified port and channel group are not active.
Specified VLAN group ID is not configured:<vlan group id>.	The specified VLAN group ID has not been configured. <vlan group id>: Indicates the VLAN group ID.

## Notes

The counter will no longer be updated when statistics reach the maximum value.

---

## show gsrp aware

---

Displays GSRP aware information.

### Syntax

show gsrp aware

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

The command can display information only for the master switch.

### Example

*Figure 30-6: Example of displaying the show gsrp aware command*

```
> show gsrp aware
Date 20XX/07/14 12:00:00 UTC

Last mac_address_table Flush Time : 20XX/07/14 11:00:00
GSRP Flush Request Parameters :
  GSRP ID : 10          VLAN Group ID : 1    Port : 1/0/8
  Source MAC Address : 0012.e2a8.2527

>
```

### Display items

*Table 30-7: 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	1-65535
VLAN Group ID	VLAN group ID for the received GSRP Flush request frame	1-64 (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 30-8:* List of response messages for the show gsrp aware command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to GSRP program.	Communication with the GSRP program failed. Re-execute the command. If the failure occurs frequently, use the <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 64.

The items to be cleared are Master to Backup Counts and Backup to Master Counts.

[port <port list>] [channel-group-number <channel group list>]

Clears statistics for GSRP relating to the specified port or channel group. Both port and channel groups can be specified at the same time. In this case, GSRP statistics for the specified port and statistics for the specified channel group are cleared.

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.

### Operation when a stack configuration is used

This command is not supported.

## Example

*Figure 30-7: Example of clearing all GSRP statistics*

```
> clear gsrp
>
```

*Figure 30-8: Example of clearing GSRP statistics when a VLAN group ID is specified*

```
> show gsrp 10 vlan-group 1
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
Local MAC Address      : 0012.e2a8.2527
Neighbor MAC Address   : 0012.e2a8.2505
Total VLAN Group Counts : 1

VLAN Group ID : 1
VLAN ID        : 110,200-2169
Member Port    : 0/6-8
Active Port    : 0/6-8
Last Transition : 20XX/07/14 10:00:00 (Master to Backup)
Transition by reason : Priority was lower than neighbor's
Master to Backup Counts : 4
Backup to Master Counts : 4

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 20XX/07/14 12:00:00 UTC

GSRP ID: 10
Local MAC Address      : 0012.e2a8.2527
Neighbor MAC Address   : 0012.e2a8.2505
Total VLAN Group Counts : 1

VLAN Group ID : 1
VLAN ID        : 110,200-2169
Member Port    : 0/6-8
Active Port    : 0/6-8
Last Transition : 20XX/07/14 10:00:00 (Master to Backup)
Transition by reason : Priority was lower than neighbor's
Master to Backup Counts : 0
Backup to Master Counts : 0

State           Local      Neighbor
Acknowledged State : Backup    Master
Advertise Hold Timer : 3        -
Priority         : 100      101
Active Ports     : 3        3
Up Ports        : 3        -
```

*Figure 30-9: Example of clearing GSRP statistics when a port is specified*

```
> show gsrp 10 port 0/10 detail
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
Port Information
```

```

0/10    GSRP      : Not Active Port      : Up
(CH: 1) Type      : Direct      Flush    : No          Delay          : 0
        TxFrame   : 1027        RxFrame   : 1020        Discard Frame   : 2
        Discard Frame by reason
            mismatch GSRP VLAN ID      : 1
            mismatch GSRP ID           : 1
            loopback GSRP frame        : 0
            illegal GSRP frame         : 0

> clear gsrp 10 port 0/10

> show gsrp 10 port 0/10 detail
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
Port Information
0/10    GSRP      : Not Active Port      : Up
(CH: 1) Type      : Direct      Flush    : No          Delay          : 0
        TxFrame   : 0          RxFrame   : 0          Discard Frame   : 0
        Discard Frame by reason
            mismatch GSRP VLAN ID      : 0
            mismatch GSRP ID           : 0
            loopback GSRP frame        : 0
            illegal GSRP frame         : 0

```

## Display items

None

## Impact on communication

None

## Response messages

Table 30-9: List of response messages for the clear gsrp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to GSRP program.	Communication with the GSRP program failed. Re-execute the command. If the failure occurs frequently, use the <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 64.

-f

Switches the status to master status without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 30-10:* 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 30-10:* List of response messages for the set gsrp master command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
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>&lt;gsrp group id&gt;</i>	The specified GSRP group ID has not been configured. <i>&lt;gsrp group id&gt;</i> : Indicates the GSRP group ID.
Specified VLAN group ID is not configured: <i>&lt;vlan group id&gt;</i> .	The specified VLAN group ID has not been configured. <i>&lt;vlan group id&gt;</i> : 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.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 30-11: Example of executing the clear gsrp port-up-delay command*

```
> show gsrp 10 port 0/6-10
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
Port Information
0/6      GSRP      : Not Active Port      : Up
        Type      : Member      Flush      : Reset      Delay          : 43172
        TxFrame    : 0           RxFrame    : 0           Discard Frame   : 0
0/7      GSRP      : Not Active Port      : Up
        Type      : Member      Flush      : Reset      Delay          : 43174
        TxFrame    : 0           RxFrame    : 0           Discard Frame   : 0
0/8      GSRP      : Active      Port      : Up
        Type      : Member      Flush      : GSRP      Delay          : 0
        TxFrame    : 0           RxFrame    : 0           Discard Frame   : 0
0/10     GSRP      : Not Active Port      : Up
(CH: 1) Type      : Direct      Flush      : No         Delay          : 0
        TxFrame    : 1993       RxFrame    : 1987       Discard Frame   : 0

> clear gsrp port-up-delay

> show gsrp 10 port 0/6-10
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
Port Information
```

```

0/6      GSRP      : Active      Port      : Up
        Type       : Member      Flush     : Reset      Delay       : 0
        TxFrame    : 0           RxFrame   : 0          Discard Frame : 0
0/7      GSRP      : Active      Port      : Up
        Type       : Member      Flush     : Reset      Delay       : 0
        TxFrame    : 0           RxFrame   : 0          Discard Frame : 0
0/8      GSRP      : Active      Port      : Up
        Type       : Member      Flush     : GSRP        Delay       : 0
        TxFrame    : 0           RxFrame   : 0          Discard Frame : 0
0/10     GSRP      : Not Active   Port      : Up
(CH: 1) Type       : Direct      Flush     : No         Delay       : 0
        TxFrame    : 2073       RxFrame   : 2068       Discard Frame : 0
>

```

*Figure 30-12: Example of executing the port-up-delay command when a port is specified*

```

> show gsrp 10 port 0/6
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
Port Information
0/6      GSRP      : Not Active   Port      : Up
        Type       : Member      Flush     : Reset      Delay       : 43180
        TxFrame    : 0           RxFrame   : 0          Discard Frame : 0

> clear gsrp port-up-delay port 0/6

> show gsrp 10 port 0/6
Date 20XX/07/14 12:00:00 UTC

GSRP ID: 10
Port Information
0/6      GSRP      : Active      Port      : Up
        Type       : Member      Flush     : Reset      Delay       : 0
        TxFrame    : 0           RxFrame   : 0          Discard Frame : 0
>

```

## Display items

None

## Impact on communication

None

## Response messages

*Table 30-11: List of response messages for the clear gsrp port-up-delay command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to GSRP program.	Communication with the GSRP program failed. Re-execute the command. If the failure occurs frequently, use the <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.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 30-13:* Example of disabling the GSRP automatic-transition-to-master wait time

```
> clear gsrp forced-shift 1
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 30-12:* List of response messages for the clear gsrp forced-shift command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to GSRP program.	Communication with the GSRP program failed. Re-execute the command. If the failure occurs frequently, use the <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.

### Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the `remote command` command.

```
remote command {<switch no.> | all} restart gsrp [-f] [core-file]
```

### Example

*Figure 30-14: 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 30-13: List of response messages for the restart gsrp command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
GSRP program failed to be restarted.	An attempt to restart the GSRP program by using this command failed. Re-execute the command.

## Notes

The storage directory and the name of the core file are as follows.

Storage directory: `/usr/var/core/`

Core file: `gsrpd.core`

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance if necessary.

---

## dump protocols gsrp

---

Dumps detailed event trace information and control table information collected by the GSRP program to a file.

### Syntax

```
dump protocols gsrp
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the `remote command` command.

```
remote command {<switch no.> | all} dump protocols gsrp
```

### Example

*Figure 30-15: Example of executing GSRP dump*

```
> dump protocols gsrp
```

```
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 30-14: List of response messages for the dump protocols gsrp command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to GSRP program.	Communication with the GSRP program failed. Re-execute the command. If the failure occurs frequently, use the <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

---

# 31. 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 status of VRRP virtual routers.

### Syntax

```
show vrrpstatus [detail] [statistics] [protocol ip] [interface vlan <vlan id>] [vrid <vrid>]]
```

### Input mode

User mode and administrator mode

### Parameters

detail

Displays detailed information about the virtual router status.

Operation when this parameter is omitted:

Displays an overview of virtual routers.

statistics

Display statistics for virtual routers.

Operation when this parameter is omitted:

Displays information about the virtual router status.

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.

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.

Operation when this parameter is omitted:

Displays information about virtual routers for all interfaces.

vrid <vrid>

Specifies the router ID.

Operation when this parameter is omitted:

Displays information about all virtual routers for the specified interface.

Operation when all parameters are omitted:

Displays a list of virtual routers, and information about their statuses.

### Operation when a stack configuration is used

This command is not supported.

### Example 1

*Figure 31-1:* Example of displaying summary information about IPv4 protocol virtual routers

```
> show vrrpstatus protocol ip
```

```

Date 20XX/12/10 12:00:00 UTC
VLAN0010 VRID 1 VRF 2 MASTER virtual-ip 170.10.10.2 priority 150/150
VLAN0030 VRID 2 BACKUP virtual-ip 170.10.10.3 priority 100/100
>

```

## Display items in Example 1

Table 31-1: Example of displaying summary information about IPv4 protocol virtual routers

Item	Meaning	Displayed information
<i>&lt;interface name&gt; VRID &lt;vrid&gt; [VRF &lt;vrf id&gt;] &lt;state&gt; virtual-ip &lt;virtual ip address&gt; priority &lt;priority&gt;/&lt;original priority&gt;</i>		
Summary information	<i>&lt;interface name&gt;</i>	Name of the interface where a virtual router is operating
	VRID <i>&lt;vrid&gt;</i>	Virtual router ID
	VRF <i>&lt;vrf id&gt;</i> [OS-L3SA]	VRF ID
	<i>&lt;state&gt;</i>	Current status of a virtual router MASTER: Indicates the master status. BACKUP: Indicates the backup status. INITIAL: Indicates the initial status.
	virtual-ip <i>&lt;virtual ip address&gt;</i>	Virtual IP address
	priority <i>&lt;priority&gt;/&lt;original priority&gt;</i>	Virtual router priority <i>&lt;priority&gt;</i> : Indicates the current virtual router priority. <i>&lt;original priority&gt;</i> : Indicates the priority set in the configuration. If configuration settings are omitted, the initial value, 100, is displayed.

## Example 2

Figure 31-2: Example of displaying the detailed virtual router status

```

> show vrrpstatus detail interface vlan 10 vrid 1
Date 20XX/12/10 12:00:00 UTC
VLAN0010: VRID 1 VRF 2
  Virtual Router IP Address : 170.10.10.2
  Virtual MAC Address : 0000.5e00.0101
  Current State : MASTER
  Admin State : enable
  Priority : 80 /100
  IP Address Count : 1
  Master Router's IP Address : 170.10.10.2
  Primary IP Address : 170.10.10.1
  Authentication Type : SIMPLE TEXT PASSWORD
  Authentication Key : ABCDEFG
  Advertisement Interval : 1 sec
  Preempt Mode : ON
  Preempt Delay : 60
  Non Preempt swap timer : 30
  Accept Mode : ON
  Virtual Router Up Time : Mon Dec 6 16:55:00 20XX
  track 10 VLAN0022 VRF 3 Status : (IF UP) Down Priority : 50
    Target Address : 192.168.0.20
    Vrrp Polling Status : reachable
  track 20 VLAN0023 Status : (IF UP) Down Priority : 40
  track 30 gigabitethernet 0/10 Status : (IF DOWN) Down Priority : 20
  track 40 port-channel 2 Status : (IF UP) Down Priority : 20
>

```

## Display items in Example 2

Table 31-2: Items displayed for the virtual router status

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. This is not displayed if the virtual router is operating in a global network. [OS-L3SA]
Virtual Router IP Address : <ip address>[(ADDRESS OWNER)]	IP address of the virtual router	(ADDRESS OWNER) : Displayed if the user is the owner of the address.
Virtual MAC Address : <mac address>	MAC address of a virtual router	--
Current State : <status>	Current status of a virtual router	MASTER: Indicates the master status. BACKUP: Indicates the backup status. INITIAL: Indicates 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. (NOIP) : The IP address of the applicable interface was not set. (NOJOIN) : An attempt to join a multicast group failed. (S/W FAIL) : An attempt to register a virtual MAC address in the hardware failed.
Priority : <priority> /<original priority>	Virtual router priority	<priority>: Indicates the current virtual router priority.  <original priority>: Indicates the priority set in the configuration. If configuration settings are omitted, the initial value, 100, is displayed.
IP Address Count : <N>	Number of virtual router IP addresses	--
Master Router's IP Address : <ip address>	IP address of a router currently in the master status	--
Primary IP Address : <ip address>	IP address of an interface for which VRRP is configured	--

Item	Meaning	Displayed information
Authentication Type : <type>	Packet authentication type	NONE: No packet authentication is performed. SIMPLE TEXT PASSWORD: Indicates a text password.
Authentication Key : <text>	Text password	--
Advertisement Interval : <second> sec	Interval for sending ADVERTISEMENT packets (in seconds)	1-255
Preempt Mode : {ON OFF}	Automatic switch-back setting	ON: Indicates that the automatic switch-back functionality is enabled. OFF: Indicates that the automatic switch-back functionality is suppressed.
Preempt Delay : <second> [(Now Waiting, <N> sec left)]	Suppression timer setting period (in seconds)	(Now Waiting, <N>sec left): Displays the remaining time until the state is changed to master while switching to master is suppressed by this setting. N: Indicates a value from 1 to 65535.
Non Preempt swap timer : <second> [ (Now Waiting, <N> sec left)]	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.
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>&lt;track-number&gt;: Indicates the number of the track assigned to a virtual router.</p> <p>&lt;interface name&gt;: Indicates the interface name of the VLAN interface that monitors for failures.</p> <p>VRF &lt;vrf id&gt;: Indicates the VRF ID. When the destination for VRRP polling is a global network, this item is not displayed. [OS-L3SA]</p> <p>&lt;interface type&gt; &lt;interface number&gt;: Indicates an interface that monitors for failures. gigabitethernet &lt;nif no.&gt;/&lt;port no.&gt;: Indicates a 10BASE-T, 100BASE-TX, 1000BASE-T, 100BASE-FX, or 1000BASE-X interface that monitors for failures. tengigabitethernet &lt;nif no.&gt;/&lt;port no.&gt;: Indicates a 10GBASE-R interface that monitors for failures. fortygigabitethernet &lt;nif no.&gt;/&lt;port no.&gt;: Indicates a 40GBASE-R interface that monitors for failures. [AX3800S]</p> <p>port-channel &lt;channel group number&gt;: Indicates a channel-group interface that monitors for failures.</p> <p>&lt;status&gt;: Indicates the current status of an interface that monitors for failures. (IF UP): Indicates that the interface is in the UP status. (IF DOWN): Indicates that the interface is in the DOWN status.</p> <p>Method for changing priority Down Priority : &lt;priority&gt;: Indicates the priority is decreased if an interface that monitors failures is in the DOWN status. Critical Priority : &lt;priority&gt;: 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>&lt;target-address&gt;: Indicates the destination address for VRRP polling. This item is not displayed if the destination IP address for VRRP polling has not been specified, or for an interface that monitors for 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>&lt;status&gt;: Indicates connectivity by VRRP polling.</p> <p>    reachable: Indicates that communication is possible.</p> <p>    unreachable: Indicates that communication is impossible.</p> <p>&lt;reason&gt;: Provides a detailed reason why communication is impossible. This information is displayed if &lt;status&gt; is unreachable.</p> <p>    (interface down): Indicates that the source interface for polling is in the DOWN status.</p> <p>    (no response): Indicates that there were no responses from the polling destination.</p> <p>    (no route): Indicates that there are no routes to the polling destination.</p> <p>    (invalid response): When the track check-reply-interface configuration command is set, responses from interfaces other than the interface that sent the polling request were received.</p>

### Example 3

Figure 31-3: Example of displaying virtual router statistics

```
> show vrrpstatus statistics interface vlan 10 vrid 1
Date 20XX/12/10 12:00:00 UTC
VLAN0010: VRID 1 VRF 2
  5 times transitions to master
  1500 advertisement received
    0 with bad advertisement interval
    0 with authentication failed
    0 with bad ip ttl
    3 with priority zero
    0 with invalid type
    0 with bad ip address list
    0 with bad authentication type
    0 with authentication type mismatch
    0 with packet length error
    0 with different VRRP version
    0 with low priority
  1300 advertisement sent
    0 with priority zero
  0 change by command
  0 change by interface down
  0 change by receiving advertisement with high priority
  0 change by Master_Down_Timer timeout
  0 master transition delay count
track 10  VLAN0022 VRF 3 Target-Address : 192.168.0.20
  VRRP Polling round-trip min/avg/max = 0.266/0.274/0.286 ms
  1 priority down by detected
track 20  VLAN0023 line-protocol
  0 priority down by detected
track 30  gigabitethernet 0/10 line-protocol
  0 priority down by detected
track 40  port-channel 2 line-protocol
```

0 priority down by detected  
>

### Display items in Example 3

Table 31-3: Items displayed for virtual router statistics

Item	Meaning	Displayed information
<i>&lt;interface name&gt;</i> : VRID <i>&lt;vrid&gt;</i> [VRF <i>&lt;vrf id&gt;</i> ]	Name of the interface where a virtual router is operating, and its VRID information	<i>&lt;interface name&gt;</i> : Indicates the name of the interface where the virtual router is operating.  <i>&lt;vrid&gt;</i> : Indicates the virtual router ID.  VRF <i>&lt;vrf id&gt;</i> : Indicates the VRF ID. This is not displayed if the virtual router is operating in a global network. [OS-L3SA]
<i>&lt;number of packets&gt;</i> times transitions to master	Number of transitions to the master status	--
<i>&lt;number of packets&gt;</i> advertisement received	Number of received ADVERTISEMENTS packets	--
<i>&lt;number of packets&gt;</i> with bad advertisement interval	Number of received ADVERTISEMENTS packets that have invalid packet-sending intervals	--
<i>&lt;number of packets&gt;</i> with authentication failed	Number of received ADVERTISEMENTS packets of which authentication failed	--
<i>&lt;number of packets&gt;</i> with bad ip ttl	Number of received ADVERTISEMENTS packets whose TTL for the IP header is not 255	--
<i>&lt;number of packets&gt;</i> with priority zero	Number of received ADVERTISEMENTS packets whose priority level is 0	--
<i>&lt;number of packets&gt;</i> with invalid type	Number of received ADVERTISEMENTS packets that had an invalid type field	--

Item	Meaning	Displayed information
<number of packets> with bad ip address list	Number of received ADVERTISESEME NT packets that have invalid virtual router IPv4 addresses	--
<number of packets> with bad authentication type	Number of received ADVERTISESEME NT packets with invalid packet authentication types	--
<number of packets> with authentication type mismatch	Number of received ADVERTISESEME NT packets whose packet authentication type did not match the local setting.	--
<number of packets> with packet length error	Number of received ADVERTISESEME NT packets whose packet length was invalid	--
<number of packets> with different VRRP version	Number of received packets whose version of ADVERTISESEME NT packets and that of VRRP operation mode do not match	--
<number of packets> with low priority	Number of received ADVERTISESEME NT packets with lower priority	--
<number of packets> advertisement sent	Number of sent ADVERTISESEME NT packets	--
<number of packets> with priority zero	Number of sent ADVERTISESEME NT packets whose priority is 0	--
<N> change by command	Number of times that the <code>swap vrrp</code> command was executed	--

Item	Meaning	Displayed information
<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	--
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>&lt;track-number&gt;: Indicates the number of the track assigned to a virtual router.</p> <p>&lt;interface name&gt;: Indicates the name of an interface that monitors for failures.</p> <p>VRF &lt;vrf id&gt;: Indicates the VRF ID. When the destination for VRRP polling is a global network, this item is not displayed. [OS-L3SA]</p> <p>&lt;interface type&gt; &lt;interface number&gt;: Indicates an interface that monitors for failures.  gigabitethernet &lt;nif no.&gt; / &lt;port no.&gt;: Indicates a 10BASE-T, 100BASE-TX, 1000BASE-T, 100BASE-FX, or 1000BASE-X interface that monitors for failures.  tengigabitethernet &lt;nif no.&gt; / &lt;port no.&gt;: Indicates a 10GBASE-R interface that monitors for failures.  fortygigabitethernet &lt;nif no.&gt; / &lt;port no.&gt;: Indicates a 40GBASE-R interface that monitors for failures. [AX3800S]  port-channel &lt;channel group number&gt;: Indicates a channel-group interface that monitors for failures.</p> <p>Target-Address : &lt;target-address&gt;: 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 destination IP address for VRRP polling has not been specified, or for an interface that monitors failures.</p> <p>&lt;minimum&gt;/&lt;average&gt;/&lt;maximum&gt;: 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	--

**Impact on communication**

None

**Response messages***Table 31-4:* List of response messages for the show vrrpstatus (IPv4) command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
no entries.	There are no applicable virtual routers.

**Notes**

None

---

## clear vrrpstatus (IPv4)

---

Clears the counter for VRRP virtual router statistics.

### Syntax

```
clear vrrpstatus [protocol ip] [interface vlan <vlan id> [vrid <vrid>]]
```

### Input mode

User mode and administrator mode

### Parameters

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.

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.

Operation when this parameter is omitted:

Clears the statistics on virtual routers for all interfaces.

vrid <vrid>

Specifies the virtual router ID.

Operation when this parameter is omitted:

Clears the statistics on all virtual routers for the specified interface.

Operation when all parameters are omitted:

Clears the counter for all virtual router statistics.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 31-4: Example of clearing the counter for virtual router statistics*

```
> clear vrrpstatus interface vlan 10 vrid 1
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 31-5: 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.

Message	Description
no entries.	There are no applicable virtual routers.

**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] 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.

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.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure shows how to change VRID 1 and VRID 20 virtual routers that are configured for VLAN 10, which are currently operating in the master status, to the backup status.

*Figure 31-5: 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

Communication might stop temporarily because of state transitions in VRRP.

## Response messages

*Table 31-6:* 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 owner's virtual router.	This command cannot be executed for the virtual router of the address owner.
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.
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 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 four seconds by default.
- In a configuration where the `no vrrp preempt` and the `vrrp timers non-preempt-swap` configuration commands are set for all devices that make up the VRRP, if a 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 in the VRRP. If all the devices are in the backup status, you can make one of the devices the master device by executing the switch-back 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 31-7: 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 status of VRRP virtual routers.

### Syntax

```
show vrrpstatus [detail] [statistics] [protocol ipv6] [interface vlan <vlan id>]
[vrid <vrid>]]
```

### Input mode

User mode and administrator mode

### Parameters

detail

Displays detailed information about the virtual router status.

Operation when this parameter is omitted:

Displays an overview of virtual routers.

statistics

Display statistics for virtual routers.

Operation when this parameter is omitted:

Displays information about the virtual router status.

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.

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.

Operation when this parameter is omitted:

Displays information about virtual routers for all interfaces.

vrid <vrid>

Specifies the router ID.

Operation when this parameter is omitted:

Displays information about all virtual routers for the specified interface.

Operation when all parameters are omitted:

Displays a list of virtual routers, and information about their statuses.

### Operation when a stack configuration is used

This command is not supported.

### Example 1

*Figure 31-6:* Example of displaying summary information about IPv6-protocol virtual routers

```
> show vrrpstatus protocol ipv6
```

```

Date 20XX/12/10 12:00:00 UTC
VLAN0010 VRID 1 VRF 2 MASTER virtual-ip 100:0:11::100 priority 150/150
VLAN0013 VRID 1 BACKUP virtual-ip 100:0:13::100 priority 100/100
>

```

## Display items in Example 1

Table 31-8: Example of displaying summary information about IPv6-protocol virtual routers

Item	Meaning	Displayed information
<i>&lt;interface name&gt; VRID &lt;vrid&gt; [VRF &lt;vrf id&gt;] &lt;state&gt; virtual-ip &lt;virtual ip address&gt; priority &lt;priority&gt;/&lt;original priority&gt;</i>		
Summary information	<i>&lt;interface name&gt;</i>	Name of the interface where a virtual router is operating
	VRID <vrid>	Virtual router ID
	VRF <vrf id> [OS-L3SA]	VRF ID
	<state>	MASTER: Indicates the master status. BACKUP: Indicates the backup status. INITIAL: Indicates the initial status.
	virtual-ip <virtual ip address>	Virtual IP address
	priority <priority>/<original 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.

## Example 2

Figure 31-7: Example of displaying the detailed virtual router status

```

> show vrrpstatus detail interface vlan 10 vrid 3
Date 20XX/12/10 12:00:00 UTC
VLAN0010: VRID 3 VRF 2
  Virtual Router IP Address : fe80::1234
  Virtual MAC Address : 0000.5e00.0203
  Current State : MASTER
  Admin State : enable
  Priority : 100/120
  IP Address Count : 1
  Master Router's IP Address : fe80::abcd
  Primary IP Address : fe80::abcd
  Authentication Type : SIMPLE TEXT PASSWORD(Disable)
  Authentication Key : ABCDEFG(Disable)
  Advertisement Interval : 1 sec
  Preempt Mode : ON
  Preempt Delay : 60
  Non Preempt swap timer : 30
  Accept Mode : ON
  Virtual Router Up Time : Mon Dec 6 16:55:00 20XX
  track 10 VLAN0022 VRF 3 Status : (IF UP) Down Priority : 50
    Target Address : fe80::ba
    Vrrp Polling Status : reachable
  track 20 VLAN0023 Status : (IF UP) Down Priority : 40
  track 30 gigabitethernet 0/10 Status : (IF DOWN) Down Priority : 20
  track 40 port-channel 2 Status : (IF UP) Down Priority : 20

```

IPv6 Advertisement Type : ietf-ipv6-spec-07-mode

&gt;

## Display items in Example 2

Table 31-9: Items displayed for the virtual router status

Item	Meaning	Displayed information
<interface name> : VRID <vrid> [VRF <vrfid>]	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 <vrfid>: Indicates the VRF ID. This is not displayed if the virtual router is operating in a global network. [OS-L3SA]
Virtual Router IP Address : <ip address>[(ADDRESS OWNER)]	IP address of the virtual router	(ADDRESS OWNER) : Displayed if the user is the owner of the address.
Virtual MAC Address : <mac address>	MAC address of a virtual router	--
Current State : <status>	Current status of a virtual router	MASTER: Indicates the master status. BACKUP: Indicates the backup status. INITIAL: Indicates 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. (NOIP) : The IP address of the applicable interface was not set. (NOJOIN) : An attempt to join a multicast group failed. (S/W FAIL) : An attempt to register a virtual MAC address in the hardware failed.
Priority : <priority> / <original priority>	Virtual router priority	<priority>: Indicates the current virtual router priority.  <original priority>: Indicates the priority set in the configuration. If configuration settings are omitted, the initial value, 100, is displayed.
IP Address Count : <N>	Number of virtual router IP addresses	--
Master Router's IP Address : <ip address>	IP address of a router currently in the master status	--
Primary IP Address: <ip address>	IP address of an interface for which VRRP is configured	--

Item	Meaning	Displayed information
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. This functionality is disabled if the router is not supported in VRRP operation mode.
Authentication Key : <text>[(Disable)]	Text password	(Disable): Indicates that the operation is invalid. This functionality is disabled if the router is not supported in VRRP operation mode.
Advertisement Interval : <second> sec	Interval for sending ADVERTISEMENT packets (in seconds)	1-255
Preempt Mode : {ON OFF}	Automatic preemption setting	ON: Indicates that the automatic preemption functionality is enabled. OFF: Indicates that the automatic preemption functionality is suppressed.
Preempt Delay : <second> [(Now Waiting, <N>sec left)]	Suppression timer setting period (in seconds)	(Now Waiting, <N>sec left): Displays the remaining time until the state is changed to master while switching to master is suppressed by this setting. N: Indicates a value from 1 to 65535.
Non Preempt swap timer : <second> [(Now Waiting, <N>sec left)]	Preemption suppression time (in seconds) while automatic preemption is suppressed	(Now Waiting, <N>sec left): Displays the remaining time until the state is changed to master while switching to master is suppressed by this setting. N: Indicates a value from 1 to 65535.
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> <interface type> <interface number>} Status : <status> {Down Priority Critical Priority} : <priority>	Information about a track assigned to a virtual router	<p>&lt;track-number&gt;: Indicates the number of the track assigned to a virtual router.</p> <p>&lt;interface name&gt;: Indicates the interface name of the VLAN interface that monitors failures.</p> <p>&lt;interface type&gt; &lt;interface number&gt;: Indicates an interface that monitors failures.  gigabitethernet &lt;nif no.&gt; /&lt;port no.&gt;: Indicates a 10BASE-T, 100BASE-TX, 1000BASE-T, 100BASE-FX, or 1000BASE-X interface that monitors for failures.  tengigabitethernet &lt;nif no.&gt; /&lt;port no.&gt;: Indicates a 10GBASE-R interface that monitors failures.  port-channel &lt;channel group number&gt;: Indicates a channel-group interface that monitors failures.</p> <p>&lt;status&gt;: 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.</p> <p>Method for changing priority  Down Priority : &lt;priority&gt;: Indicates the priority is decreased if an interface that monitors failures is in the DOWN status.  Critical Priority : &lt;priority&gt;: 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>&lt;target-address&gt;: 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>&lt;status&gt;: Indicates connectivity by VRRP polling.            reachable: Indicates that communication is possible.            unreachable: Indicates that communication is impossible.</p> <p>&lt;reason&gt;: Provides a detailed reason why communication is impossible.          This information is displayed if &lt;status&gt; 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>	Type of sending ADVERTISEMENT packets	<p>Type of sending ADVERTISEMENT packets</p> <p>ietf-ipv6-spec-02-mode: Sends ADVERTISEMENT packets according to draft-ietf-vrrp-ipv6-spec-02.</p> <p>ietf-ipv6-spec-07-mode: Sends ADVERTISEMENT packets according to draft-ietf-vrrp-ipv6-spec-07.</p>

### Example 3

Figure 31-8: Example of displaying virtual router statistics

```
> show vrrpstatus statistics interface vlan 10 vrid 3
Date 20XX/12/10 12:00:00 UTC
VLAN0010: VRID 3 VRF 2
  1 times transitions to master
 247 advertisement received
    0 with bad advertisement interval
    0 with authentication failed
    0 with bad ipv6 hoplimit
    0 with priority zero
    0 with invalid type
    0 with bad ipv6 address
    0 with bad authentication type
    0 with authentication type mismatch
    0 with packet length error
    0 with different VRRP version
    0 with low priority
1747 advertisement sent
    0 with priority zero
  0 change by command
  0 change by interface down
  0 change by receiving advertisement with high priority
  0 change by Master_Down_Timer timeout
  0 master transition delay count
track 10 VLAN0022 VRF 3 Target-Address : fe80::ba
  VRRP Polling round-trip min/avg/max = 0.266/0.274/0.286 ms
```

1 priority down by detected  
>

### Display items in Example 3

Table 31-10: Items displayed for virtual router statistics

Item	Meaning	Displayed information
<i>&lt;interface name&gt;</i> : VRID <i>&lt;vrid&gt;</i> [VRF <i>&lt;vrf id&gt;</i> ]	Name of the interface where a virtual router is operating, and its VRID information	<i>&lt;interface name&gt;</i> : Indicates the name of the interface where the virtual router is operating.  <i>&lt;vrid&gt;</i> : Indicates the virtual router ID.  VRF <i>&lt;vrf id&gt;</i> : Indicates the VRF ID. This is not displayed if the virtual router is operating in a global network. [OS-L3SA]
<i>&lt;number of packets&gt;</i> times transitions to master	Number of transitions to the master status	--
<i>&lt;number of packets&gt;</i> advertisement received	Number of received ADVERTISEMENT packets	--
<i>&lt;number of packets&gt;</i> with bad advertisement interval	Number of received ADVERTISEMENT packets that have invalid packet-sending intervals	--
<i>&lt;number of packets&gt;</i> with authentication failed	Number of received ADVERTISEMENT packets of which authentication failed	--
<i>&lt;number of packets&gt;</i> with bad ipv6 hoplimit	Number of received ADVERTISEMENT packets whose HopLimit for the IPv6 header was not 255	--
<i>&lt;number of packets&gt;</i> with priority zero	Number of received ADVERTISEMENT packets whose priority level is 0	--
<i>&lt;number of packets&gt;</i> with invalid type	Number of received packets that had an invalid type field	--
<i>&lt;number of packets&gt;</i> with bad ipv6 address	Number of received ADVERTISEMENT packets that had invalid virtual router IPv6 addresses	--
<i>&lt;number of packets&gt;</i> with bad authentication type	Number of received ADVERTISEMENT packets with invalid packet authentication types	--
<i>&lt;number of packets&gt;</i> 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	--
<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> <interface type> <interface number>} {Target-Address : <target-address> line-protocol}	VRRP polling information assigned to a virtual router	<p>&lt;track-number&gt;: Indicates the number of the track assigned to a virtual router.</p> <p>&lt;interface name&gt;: Indicates the name of an interface that monitors failures.</p> <p>&lt;interface type&gt; &lt;interface number&gt;: Indicates an interface that monitors failures.</p> <p>gigabitethernet &lt;nif no.&gt; /&lt;port no.&gt;: Indicates a 10BASE-T, 100BASE-TX, 1000BASE-T, 100BASE-FX, or 1000BASE-X interface that monitors for failures.</p> <p>tengigabitethernet &lt;nif no.&gt; /&lt;port no.&gt;: Indicates a 10GBASE-R interface that monitors failures.</p> <p>port-channel &lt;channel group number&gt;: Indicates a channel-group interface that monitors failures.</p> <p>Target-Address : &lt;target-address&gt;: 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>&lt;minimum&gt;/&lt;average&gt;/&lt;maximum&gt;: 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	--

### Impact on communication

None

### Response messages

Table 31-11: List of response messages for the show vrrpstatus (IPv6) command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
no entries.	There are no applicable virtual routers.

### Notes

None

---

## clear vrrpstatus (IPv6)

---

Clears the counter for VRRP virtual router statistics.

### Syntax

```
clear vrrpstatus [protocol ipv6] [interface vlan <vlan id> [vrid <vrid>]]
```

### Input mode

User mode and administrator mode

### Parameters

protocol ipv6

Clears the counter for IPv6-protocol virtual router statistics.

Operation when this parameter is omitted:

Clears the statistics for both IPv4 and IPv6-protocol virtual routers.

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.

Operation when this parameter is omitted:

Clears the statistics on virtual routers for all interfaces.

vrid <vrid>

Specifies the router ID.

Operation when this parameter is omitted:

Clears the statistics on all virtual routers for the specified interface.

Operation when all parameters are omitted:

Clears the counter for all virtual router statistics.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 31-9: Example of clearing the counter for virtual router statistics*

```
> clear vrrpstatus interface vlan 10 vrid 3
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 31-12: 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.

Message	Description
no entries.	There are no applicable virtual routers.

**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] 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.

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.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure shows how to switch VRID 3 and VRID 40 virtual routers configured for VLAN 10, which are currently operating in the master status, to the backup status.

*Figure 31-10: 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

Communication might stop temporarily because of state transitions in VRRP.

## Response messages

*Table 31-13:* 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 owner's virtual router.	This command cannot be executed for the virtual router of the address owner.
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.
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 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 four seconds by default.
- In a configuration where the `no vrrp preempt` and the `vrrp timers non-preempt-swap` configuration commands are set for all devices that make up the VRRP, if a 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 31-14: 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.>
- fortygigabitethernet <nif no.>/<port no.> [AX3800S]

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.

## Operation when a stack configuration is used

This command is not supported.

### Example

- The following figure shows an example of displaying the list of IPv4 protocol tracks.

*Figure 31-11: Example of displaying IPv4 protocol track information*

```
> show track protocol ip
Date 20XX/12/10 12:00:00 UTC
track : 10   interface : VLAN0022   Mode : (interface)
track : 20   interface : VLAN0031 VRF 10 Mode : (polling)
>
```

- The following figure shows an example of displaying detailed track information.

*Figure 31-12: Example of displaying detailed track information*

```
> show track detail interface vlan 31
Date 20XX/12/10 12:00:00 UTC
track : 20   interface : VLAN0031 VRF 10 Mode : (polling)
    Target Address : 170.10.10.10
    Assigned to :
        VLAN0010: VRID 1
        VLAN0100: VRID 100 VRF 20
>
```

## Display items

Table 31-15: 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>&lt;track-number&gt;: Indicates the number of the track assigned to a virtual router.</p> <p>interface : {&lt;interface name&gt; [VRF &lt;vrf id&gt;] &lt;interface type&gt; &lt;interface number&gt;} : Information about the interface for which failure monitoring is performed. (not assigned) is displayed if the track interface configuration command is not set.</p> <p>&lt;interface name&gt;: Indicates the interface name of the VLAN interface that monitors for failures.</p> <p>VRF &lt;vrf id&gt;: Indicates the VRF ID. This item is not displayed if the VLAN interface that monitors failures is a global network. [OS-L3SA]</p> <p>&lt;interface type&gt; &lt;interface number&gt;: Indicates an interface that monitors for failures. gigabitethernet &lt;nif no.&gt; / &lt;port no.&gt;: Indicates a 10BASE-T, 100BASE-TX, 1000BASE-T, 100BASE-FX, or 1000BASE-X interface that monitors for failures. tengigabitethernet &lt;nif no.&gt; / &lt;port no.&gt;: Indicates a 10GBASE-R interface that monitors for failures. fortygigabitethernet &lt;nif no.&gt; / &lt;port no.&gt;: Indicates a 40GBASE-R interface that monitors for failures. [AX3800S] port-channel &lt;channel group number&gt;: Indicates a channel-group interface that monitors for failures.</p> <p>Mode : &lt;mode&gt;: 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
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

Item	Meaning	Displayed information
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	<p>This item is not displayed if no tracks are assigned to a virtual router.</p> <p>&lt;interface name&gt;: Indicates the name of an interface for which a virtual router, to which a track is assigned, is configured.</p> <p>&lt;vrid&gt;: Indicates the virtual router ID of a virtual router to which a track is assigned.</p> <p>VRF &lt;vrf id&gt;: Indicates the VRF ID. This is not displayed if the virtual router is operating in a global network. [OS-L3SA]</p>

## Impact on communication

None

## Response messages

Table 31-16: 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.>
- fortygigabitethernet <nif no.>/<port no.> [AX3800S]

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.

## Operation when a stack configuration is used

This command is not supported.

### Example

- The following figure shows an example of displaying the list of IPv6 protocol tracks.

*Figure 31-13: Example of displaying IPv6 protocol track information*

```
> show track protocol ipv6
Date 20XX/12/10 12:00:00 UTC
track : 10  interface : VLAN0022  Mode : (interface)
track : 30  interface : VLAN0032 VRF 10 Mode : (polling)
>
```

- The following figure shows an example of displaying detailed track information.

*Figure 31-14: Example of displaying detailed track information*

```
> show track detail interface vlan 32
Date 20XX/12/10 12:00:00 UTC
track : 30  interface : VLAN0032 VRF 10 Mode : (polling)
  Target Address : 100::6789
  Assigned to :
    VLAN0010: VRID 3
    VLAN0100: VRID 200 VRF 20
>
```

## Display items

Table 31-17: 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>&lt;track-number&gt;: Indicates the number of the track assigned to a virtual router.</p> <p>interface : {&lt;interface name&gt; [VRF &lt;vrf id&gt;] &lt;interface type&gt; &lt;interface number&gt;}: Information about the interface for which failure monitoring is performed. (not assigned) is displayed if the track interface configuration command is not set.</p> <p>&lt;interface name&gt;: Indicates the interface name of the VLAN interface that monitors for failures.</p> <p>VRF &lt;vrf id&gt;: Indicates the VRF ID. This item is not displayed if the VLAN interface that monitors failures is a global network. [OS-L3SA]</p> <p>&lt;interface type&gt; &lt;interface number&gt;: Indicates an interface that monitors for failures. gigabitethernet &lt;nif no.&gt;/&lt;port no.&gt;: Indicates a 10BASE-T, 100BASE-TX, 1000BASE-T, 100BASE-FX, or 1000BASE-X interface that monitors for failures. tengigabitethernet &lt;nif no.&gt;/&lt;port no.&gt;: Indicates a 10GBASE-R interface that monitors for failures. fortygigabitethernet &lt;nif no.&gt;/&lt;port no.&gt;: Indicates a 40GBASE-R interface that monitors for failures. [AX3800S] port-channel&lt;channel group number&gt;: Indicates a channel-group interface that monitors for failures.</p> <p>Mode : &lt;mode&gt;: 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

Item	Meaning	Displayed information
failure_detection_times : <count>	Number of attempts until the status is changed when VRRP polling detects a failure	This item is not displayed if it has not been set. Initial value: 3
recovery_detection_interval : <seconds>	Interval (in seconds) between attempts when VRRP polling detects a failure	This item is not displayed if it has not been set. Initial value: 2
recovery_detection_times : <count>	Number of attempts until the status is changed when VRRP polling detects restoration	This item is not displayed if it has not been set. Initial value: 3
check_reply_interface : on	Whether to check if the interface sent by VRRP polling and the interface that received the response match	This item is not displayed if it has not been set.
Assigned to : <interface name>: VRID <vrid> [VRF <vrf id>]	List of virtual routers to which a track is assigned	This item is not displayed if no tracks are assigned to a virtual router.  <interface name>: Indicates the name of an interface for which a virtual router, to which a track is assigned, is configured.  <vrid>: Indicates the virtual router ID of a virtual router to which a track is assigned.  VRF <vrf id>: Indicates the VRF ID. This is not displayed if the virtual router is operating in a global network. [OS-L3SA]

## Impact on communication

None

## Response messages

Table 31-18: List of response messages for the show track (IPv6) command

Message	Description
no entries.	There are no applicable tracks.

## Notes

None

## Chapter

---

# 32. Uplink Redundancy

---

```
show switchport-backup
set switchport-backup active
restart uplink-redundant
dump protocols uplink-redundant
show switchport-backup statistics
clear switchport-backup statistics
```

---

## show switchport-backup

---

Displays information about the uplink redundancy functionality.

### Syntax

```
show switchport-backup [port <port list>] [channel-group-number <channel group list>]
[detail]
```

### Input mode

User mode and administrator mode

### Parameters

port <port list>

Specify the port for which you want to display the information about the uplink redundancy functionality. Uplink port information is displayed for whichever you specify, the primary port or secondary port.

For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Specify the channel group number for which you want to display the information about the uplink redundancy functionality. Uplink port information is displayed for whichever you specify, the primary port or secondary port.

For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when each parameter is omitted:

This command can display only the information relevant to the condition applied by a parameter that has been set. If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information conforming to the conditions will be displayed.

detail

Displays detailed information about the uplink redundancy functionality.

Operation when this parameter is omitted:

Information about the uplink redundancy functionality is displayed.

Operation when all parameters are omitted:

All information about the uplink redundancy functionality is displayed.

### Operation when a stack configuration is used

This command is not supported.

### Example 1

The following is an example of displaying information about the uplink redundancy functionality.

*Figure 32-1: Example of displaying uplink redundancy functionality information*

```
> show switchport-backup
Date 20XX/04/04 16:48:07 UTC
startup active port selection: primary only
Switchport Backup pairs
```

Primary	Status	Secondary	Status	Preemption		Flush	Update
Port		Port		Delay	Rest	VLAN	
0/1	Forwarding	0/24	Blocking	-	-	4094	-
0/10	Down	ChGr 4	Forwarding	-	-	-	1
*Port 0/11	Down	Port 0/15	Blocking	-	-	10	-

```
*Port 0/20 Down      Port 0/21 Down      -      -      200      -
>
```

## Display items in Example 1

Table 32-1: Items displayed for the uplink redundancy information

Item		Meaning	Displayed information
startup active port selection		Setting of the functionality that permanently assigns the active port at device startup	primary only: The functionality to fix the active port at Switch startup is enabled. This item is displayed only when this functionality is enabled.
Switchport Backup pairs	Primary	The number of the primary port or the channel group	If an asterisk (*) is displayed at the beginning, the port is an uplink port and the secondary port cannot be used for communication because the functionality to fix the active port at Switch startup is enabled.
	Status	Status of the primary port	Forwarding: Forwarding Blocking: Blocking Down: The port or channel group is in the Down status.
	Secondary	The number of the secondary port or the channel group	--
	Status	Status of the secondary port	Forwarding: Forwarding Blocking: Blocking Down: The port or channel group is in the Down status.
Preemption	Delay	Period for automatic switchbacks (in seconds)	The time that must pass before the active port is automatically switched back. - is displayed when this item is not set.
	Rest	Remaining time for automatic switchbacks (in seconds)	The time remaining before the active port is switched back. If this setting has not been specified or no switchback conditions apply, a hyphen (-) is displayed.
Flush VLAN		VLAN ID of the VLAN sending flush control frames	If the VLAN specified in configuration mode does not exist for the access port, protocol port, or MAC port, a VLAN ID different from the specified ID might be displayed.  If any of the following conditions applies and flush control frames are not sent, a hyphen (-) is displayed: <ul style="list-style-type: none"> <li>• Sending of flush control frames is not set in configuration mode.</li> <li>• The VLAN specified in configuration mode does not exist for the trunk port.</li> <li>• The native VLAN does not exist when no VLAN is specified in configuration mode for the trunk port.</li> </ul>
Update		Number of MAC address update frames sent	If the MAC address update functionality is disabled, a hyphen (-) is displayed.

## Example 2

The following is an example of displaying detailed information about the uplink redundancy functionality.

Figure 32-2: Example of displaying detailed uplink redundancy functionality information

```
> show switchport-backup detail
Date 20XX/04/04 16:49:07 UTC
startup active port selection: primary only
```

```

Switchport-backup pair
Primary      Status      Secondary  Status      Preemption  Flush
Port 0/1    Forwarding Port 0/24  Blcoking    Delay  Rest   VLAN  Update
VLAN
: 4051-4094
MAC Address update Exclude-VLAN : -
Last change factor                : primary down
Last change time                   : 20XX/04/03 16:52:21 UTC
Last Flush Tx time                 : 20XX/04/03 16:52:22 UTC
Last MAC Address update Tx time    : -

Switchport-backup pair
Primary      Status      Secondary  Status      Preemption  Flush
Port 0/10    Down          ChGr 4     Forwarding    Delay  Rest   VLAN  Update
VLAN
: 4000-4049
MAC Address update Exclude-VLAN : 4000-4010
Last change factor                : command
Last change time                   : 20XX/04/03 09:52:21 UTC
Last Flush Tx time                 : -
Last MAC Address update Tx time    : 20XX/04/03 09:52:22 UTC

Switchport-backup pair
Primary      Status      Secondary  Status      Preemption  Flush
*Port 0/11   Down          Port 0/15  Blocking     Delay  Rest   VLAN  Update
VLAN
: 10-19,21-30
MAC Address update Exclude-VLAN : -
Last change factor                : -
Last change time                   : -
Last Flush Tx time                 : -
Last MAC Address update Tx time    : -

Switchport-backup pair
Primary      Status      Secondary  Status      Preemption  Flush
*Port 0/20   Down          Port 0/21  Down         Delay  Rest   VLAN  Update
VLAN
: 200-204
MAC Address update Exclude-VLAN : -
Last change factor                : -
Last change time                   : -
Last Flush Tx time                 : -
Last MAC Address update Tx time    : -
>

```

## Display items in Example 2

Table 32-2: Items displayed for the detailed uplink redundancy information

Item		Meaning	Displayed information
startup active port selection		Setting of the functionality that permanently assigns the active port at device startup	primary only: The functionality to fix the active port at Switch startup is enabled. This item is displayed only when this functionality is enabled.
Switchport-backup pair	Primary	The number of the primary port or the channel group	If an asterisk (*) is displayed, the port is an uplink port and the secondary port cannot be used for communication because the functionality to fix the active port at Switch startup is enabled.
	Status	Status of the primary port	Forwarding: Forwarding Blocking: Blocking Down: The port or channel group is in the Down status.
	Secondary	The number of the secondary port or the channel group	--
	Status	Status of the secondary port	Forwarding: Forwarding Blocking: Blocking Down: The port or channel group is in the Down status.

Item		Meaning	Displayed information
Preemption	Delay	Period for automatic switchbacks (in seconds)	The time that must pass before the active port is automatically switched back. - is displayed when this item is not set.
	Rest	Remaining time for automatic switchbacks (in seconds)	The time remaining before the active port is switched back. If this setting has not been specified or no switchback conditions apply, a hyphen (-) is displayed.
Flush VLAN		VLAN ID of the VLAN sending flush control frames	If the VLAN specified in configuration mode does not exist for the access port, protocol port, or MAC port, a VLAN ID different from the specified ID might be displayed.  If any of the following conditions applies and flush control frames are not sent, a hyphen (-) is displayed: <ul style="list-style-type: none"> <li>• Sending of flush control frames is not set in configuration mode.</li> <li>• The VLAN specified in configuration mode does not exist for the trunk port.</li> <li>• The native VLAN does not exist when no VLAN is specified in configuration mode for the trunk port.</li> </ul>
Update		Number of MAC address update frames sent	If the MAC address update functionality is disabled, a hyphen (-) is displayed.
VLAN		ID of the VLAN set for the primary port	If no VLAN exists in the primary port, a hyphen (-) is displayed.
MAC Address update Exclude-VLAN		VLAN not subject to MAC address updating	- is displayed when this item is not set.
Last change factor		Last factor that determined the active port	command: An operation command was entered. config: A configuration command was entered. <sup>#</sup> primary down: The primary port went down. primary up: The primary port was activated. secondary down: The secondary port went down. secondary up: The secondary port was activated. preemption delay: An automatic switchback was performed. A hyphen (-) is displayed if an active port has never been defined.
Last change time		The date and time an active port was last defined.	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second A hyphen (-) is displayed if an active port has never been defined.
Last Flush Tx time		Date and time a flush control frame was last sent	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second Displays the last time a flush control frame was sent on the relevant uplink port. - is displayed if the frame has never been sent. This information is not cleared even if the flush control frame functionality is disabled by using a configuration command.
Last MAC Address update Tx time		The date and time MAC address update frame was last sent.	yyyy/mm/dd hh:mm:ss year/month/day hour:minute:second Displays the last time a MAC address update frame was sent on the relevant uplink port. - is displayed if the frame has never been sent. This information is not cleared even if the MAC address update functionality is disabled by using a configuration command.

<sup>#</sup>: This item is displayed if the secondary port operating as the active port is changed by using a configuration command before the active port is switched back to the primary port by the automatic switchback functionality.

**Impact on communication**

None

**Response messages***Table 32-3:* List of response messages for the show switchport-backup command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Uplink Redundant program.	Communication with the uplink redundancy program failed. Re-execute the command.
No operational Port.	There are no available ports or channel groups. Make sure the specified parameter is correct, and then try again.

**Notes**

None

---

## set switchport-backup active

---

Switches the standby port to the active port. You can use this command when you want to manually switch the active port from the secondary port back to the primary port. This could occur, for example, if the primary port is placed in standby status due to a failure.

### Syntax

```
set switchport-backup active { port <nif no.>/<port no.>
                             | channel-group-number <channel group> } [-f]
```

### Input mode

User mode and administrator mode

### Parameters

port <nif no.>/<port no.>

Specify the port that you want to activate. For details about the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group>

Specifies the channel group number which becomes the active port. The specifiable range of channel group numbers is from 1-32.

-f

Switches to the active port without displaying a confirmation message.

Operation when this parameter is omitted:

A confirmation message is displayed.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following is an example of switching the standby port to the active port.

*Figure 32-3: Example of executing the command that switches the active port*

```
> set switchport-backup active port 0/1
Are you sure to change the forwarding port to specified port? (y/n): y
>
```

### Display items

None

### Impact on communication

When the port used for communication is switched, communication might temporarily be interrupted.

### Response messages

*Table 32-4: List of response messages for the set switchport-backup active command*

Message	Description
Can't change, Because port is changing in an active port.	For the specified port or channel group, a switchover or switchback of the active port is being performed.
Can't change, Because port is down.	The specified port or channel group has gone down.

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Uplink Redundant program.	Communication with the uplink redundancy program failed. Re-execute the command.
No operational Port.	There are no available ports or channel groups. Make sure the specified parameter is correct, and then try again.
Port is already active port.	The specified port or channel group is already operating as the active port.

**Notes**

Make sure that the port that you want to activate is in linkup status before you execute the command.

---

## restart uplink-redundant

---

Restarts the uplink redundancy program.

### Syntax

```
restart uplink-redundant [-f] [core-file]
```

### Input mode

User mode and administrator mode

### Parameters

-f

Restarts the uplink redundancy program without outputting any confirmation messages.

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:

After a restart confirmation message is output, the uplink redundancy program is restarted.

### Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the `remote command` command.

```
remote command {<switch no.> | all} restart uplink-redundant [-f] [core-file]
```

### Example

*Figure 32-4: Example of restarting uplink redundancy*

```
> restart uplink-redundant
Uplink Redundant restart OK? (y/n): y
>
```

### Display items

None

### Impact on communication

Ports for which uplink redundancy is enabled temporarily become unable to send or receive data.

### Response messages

*Table 32-5: List of response messages for the restart uplink-redundant command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Uplink Redundant program failed to be restarted.	An attempt to restart the uplink redundancy program by this command failed. Re-execute the command.

## Notes

- The storage directory and the name of the core file are as follows.

Storage directory: `/usr/var/core/`

File name: `stpd.core`

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

- When this command is executed, the Spanning Tree program is also restarted.
- When the program is restarted, `stpd restarted.` is displayed as an operation log message.

---

## dump protocols uplink-redundant

---

Outputs to a file containing detailed event trace information and control table information collected for an uplink redundancy program.

### Syntax

```
dump protocols uplink-redundant
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the `remote command` command.

```
remote command {<switch no.> | all} dump protocols uplink-redundant
```

### Example

The following figure is an example of outputting detailed event trace information and control table information to a file.

*Figure 32-5: Example of outputting detailed event trace information and control table information*

```
> dump protocols uplink-redundant
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 32-6: List of response messages for the dump protocols uplink-redundant command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Uplink Redundant program.	Communication with the uplink redundancy program failed. Re-execute the command.
File open error.	An attempt to open or access a dump file failed.

### Notes

The storage directory and the name of the output dump file are as follows.

Storage directory: `/usr/var/ulr/`

Output file: `ulrd_dump.gz`

If necessary, back up the file in advance because the specified file is unconditionally overwritten if it already exists.

---

## show switchport-backup statistics

---

Displays statistics pertaining to uplink redundancy.

### Syntax

```
show switchport-backup statistics [port <port list>]
                                [channel-group-number <channel group list>]
```

### Input mode

User mode and administrator mode

### Parameters

port <port list>

Specify the port for which you want to display the statistics about the uplink redundancy functionality. Uplink port statistics are displayed for whichever you specify, the primary port or secondary port.

For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Specify the channel group number for which you want to display the uplink redundancy statistics. Uplink port statistics are displayed for whichever you specify, the primary port or secondary port.

For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when each parameter is omitted:

This command can display only the information relevant to the condition applied by a parameter that has been set. If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information conforming to the conditions will be displayed.

Operation when all parameters are omitted:

All uplink redundancy statistics are displayed.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 32-6: Example of displaying uplink redundancy statistics*

```
> show switchport-backup statistics port 0/1,10
Date 20XX/04/04 17:34:51 UTC
Switchport-backup pair
Primary
Port 0/1
  Flush Transmit      :      0
  MAC Address update  :      0
  Transmit            :     101
  Over flow count     :      0
Switchport-backup pair
Secondary
Port 0/24
  Flush Transmit      :      0
  MAC Address update  :      0
  Transmit            :     100
  Over flow count     :      0
Became active count :      5
Switchport-backup pair
Primary
Port 0/10
  Flush Transmit      :      6
  MAC Address update  :      0
  Transmit            :      0
  Over flow count     :      0
Switchport-backup pair
Secondary
ChGr 4
  Flush Transmit      :      5
  MAC Address update  :      0
  Transmit            :      0
  Over flow count     :      0
```

&gt;

## Display items

Table 32-7: Items displayed for uplink redundancy statistics

Item		Meaning	Displayed information
Switchport-backup pair	Primary	Primary port number	--
	Secondary	Secondary port number	--
Became active count		Number of times the port became the active port	Number of times the active port was determined by the uplink redundancy functionality
Flush Transmit		Number of times a flush control frame was sent	--
MAC Address Update	Transmit	Number of MAC address update frames that have been sent	--
	Over flow count	Number of overflows of MAC address update frames	This value is incremented if the maximum number of entries allowed on the device is exceeded when a MAC address update frame is sent at the time of a switchover or switchback.

## Impact on communication

None

## Response messages

Table 32-8: List of response messages for the show switchport-backup statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to Uplink Redundant program.	Communication with the uplink redundancy program failed. Re-execute the command.
No operational Port.	There are no available ports or channel groups. Make sure the specified parameter is correct, and then try again.

## Notes

None

---

## clear switchport-backup statistics

---

Clears uplink redundancy statistics. All uplink redundancy statistics are cleared.

### Syntax

```
clear switchport-backup statistics [port <port list>]
                                [channel-group-number <channel group list>]
```

### Input mode

User mode and administrator mode

### Parameters

port <port list>

Specify the port for which you want to clear the uplink redundancy statistics. Uplink port statistics are cleared for whichever you specify, the primary port or secondary port.

For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Specify the channel group number for which you want to clear the uplink redundancy statistics. Uplink port statistics are cleared for whichever you specify, the primary port or secondary port.

For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when each parameter is omitted:

This command can clear only the uplink redundancy statistics relevant to the condition applied by a parameter that has been set. If no parameter is specified, the uplink redundancy statistics is cleared without being limited by any conditions. If multiple parameters are specified, the uplink redundancy statistics that meets the conditions will be cleared.

Operation when all parameters are omitted:

All uplink redundancy statistics are cleared.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 32-7: Example of clearing uplink redundancy statistics*

```
> clear switchport-backup statistics
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 32-9: List of response messages for the clear switchport-backup statistics command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
Connection failed to Uplink Redundant program.	Communication with the uplink redundancy program failed. Re-execute the command.

**Notes**

If a port or channel group is specified, the uplink redundancy statistics on the paired port or channel group are also cleared.



## Chapter

---

# 33. 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.

### Operation when a stack configuration is used

The command can display information only for the master switch.

### Example 1

The following figure is an example of displaying brief information related to the IEEE 802.3ah/OAM configuration.

*Figure 33-1: Displaying IEEE 802.3ah/OAM brief configuration information*

```
> show efmoam
Date 20XX/10/02 23:59:59 UTC
Status: Enabled
udld-detection-count: 30
Port      Link status      UDLD status      Dest MAC
1/0/1     Up                detection        * 0012.e298.dc20
1/0/2     Down              active            unknown
1/0/4     Down(uni-link)    detection        unknown
>
```

## Display items in Example 1

Table 33-1: Items displayed for the IEEE 802.3ah/OAM brief configuration 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	Switch number/NIF number/port number of the port whose information is to be displayed
Link status	Link status of the applicable port	Up: Indicates that the port status is Up. Down: Indicates that the port status is Down. Down (uni-link): Indicates that the port status is Down (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 33-2: Example of displaying detailed IEEE 802.3ah/OAM configuration information

```
> show efmoam detail
Date 20XX/10/02 23:59:59 UTC
Status: Enabled
udld-detection-count: 30
Port      Link status  UDLD status  Dest MAC
1/0/1     Up           detection    * 0012.e298.dc20
1/0/2     Down        active       unknown
1/0/3     Up          passive      0012.e298.7478
1/0/4     Down (uni-link) detection    unknown
>
```

## Display items in Example 2

Table 33-2: Items displayed for the detailed IEEE 802.3ah/OAM configuration 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	Switch number/NIF number/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 a failure is detected. active: Indicates that OAMPDU frames are being sent and responses are received. passive: Only OAMPDU frames are responded to.
Dest MAC	MAC address of the 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 33-3: List of response messages for the show efmoam command*

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to IEEE802.3ah/OAM program.	Communication with the IEEE 802.3ah/OAM program failed. Re-execute the command. If the failure occurs frequently, use the <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

## 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.

### Operation when a stack configuration is used

The command can display information only for the master switch.

### Example

The following figure is an example of displaying statistics for all configured IEEE 802.3ah/OAM.

*Figure 33-3: Example of displaying statistics for IEEE 802.3ah/OAM*

```
>show efmoam statistics
Date 20XX/10/02 23:59:59 UTC
Port 1/0/1 [detection]
  OAMPDUs   :Tx      =      295  Rx      =      295
              Invalid =        0  Unrecogn.=        0
  TLVs      :Invalid =        0  Unrecogn.=        0
  Info TLV  :Tx_Local =      190  Tx_Remote=      105  Rx_Remote=      187
              Timeout =        3  Invalid  =        0  Unstable  =        0
  Inactivate:TLV    =        0  Timeout  =        0
Port 1/0/2 [active]
  OAMPDUs   :Tx      =      100  Rx      =      100
              Invalid =        0  Unrecogn.=        0
  TLVs      :Invalid =        0  Unrecogn.=        0
  Info TLV  :Tx_Local =      100  Tx_Remote=      100  Rx_Remote=      100
              Timeout =        0  Invalid  =        0  Unstable  =        0
  Inactivate:TLV    =        0  Timeout  =        0
Port 1/0/3 [passive]
  OAMPDUs   :Tx      =      100  Rx      =      100
              Invalid =        0  Unrecogn.=        0
  TLVs      :Invalid =        0  Unrecogn.=        0
  Info TLV  :Tx_Local =        0  Tx_Remote=      100  Rx_Remote=      100
              Timeout =        0  Invalid  =        0  Unstable  =        0
  Inactivate:TLV    =        0  Timeout  =        0
>
```

### Display items

*Table 33-4: Items displayed for the IEEE 802.3ah/OAM statistics*

Item	Meaning	Displayed information
Port	Port information	Switch number/NIF number/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	0-4294967295
Rx	Number of OAMPDUs that have been received for each port	0-4294967295
Invalid	Number of OAMPDUs that have been received but were discarded because they were invalid	0-4294967295
Unrecogn.	Number of unsupported OAMPDUs that have been received	0-4294967295
TLVs	TLV statistics	--
Invalid	Number of TLVs that were determined as having format errors and discarded	0-4294967295
Unrecogn.	Number of TLVs that conform to regulations but cannot be recognized by the current version	0-4294967295
Info TLV	TLV statistics for Information OAMPDU frames	--
Tx_Local	Number of times that Local Information TLV was sent	0-4294967295
Tx_Remote	Number of times that Local Information TLV from the partner device was received and Remote Information TLV was edited and then sent	0-4294967295
Rx_Remote	Number of received Local Information TLVs for responses from the partner device	0-4294967295
Timeout	Number of times that response timeout occurred on a port	0-4294967295
Invalid	Number of TLVs that were determined as having format errors and discarded	0-4294967295
Unstable	Number of times that control frames were received from a different device on a currently connected port	0-4294967295 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	0-4294967295
Timeout	Number of times that failures were detected through consecutive response timeouts	0-4294967295

**Impact on communication**

None

**Response messages***Table 33-5:* List of response messages for the show efmoam statistics command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to IEEE802.3ah/OAM program.	Communication with the IEEE 802.3ah/OAM program failed. Re-execute the command. If the failure occurs frequently, use the <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.

### Operation when a stack configuration is used

The command can clear information only from the master switch.

### Example

*Figure 33-4: Example of clearing IEEE 802.3ah/OAM statistics*

```
> clear efmoam statistics
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 33-6: List of response messages for the clear efmoam statistics command*

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
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.

### Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the `remote command` command.

```
remote command {<switch no.> | all} restart efmoam [-f] [core-file]
```

### Example

*Figure 33-5: 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 33-7: List of response messages for the restart efmoam command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
IEEE802.3ah/OAM doesn't seem to be running.	This command failed because the IEEE 802.3ah/OAM program is being restarted. Re-execute the command.

## Notes

1. The storage directory and the name of the core file are as follows:

Storage directory: `/usr/var/core/`

Core file: `efmoamd.core`

If a file with this name already exists, the file is overwritten unconditionally. Therefore, back up the file in advance, if necessary.

2. While the Switch is operating with the `udld` parameter specified by the `efmoam active` configuration command in the partner switch, if this command is executed after the master switch substitutes for the backup switch when a stack is configured or when the statuses of multiple VLANs are being changed concurrently, a unidirectional link failure might be incorrectly detected in the partner switch.

---

## dump protocols efmoam

---

Outputs to a file detailed event trace information and control table information collected for IEEE 802.3ah/OAM.

### Syntax

```
dump protocols efmoam
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the `remote command` command.

```
remote command {<switch no.> | all} dump protocols efmoam
```

### Example

*Figure 33-6:* Example of performing a dump for IEEE 802.3ah/OAM

```
> dump protocols efmoam
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 33-8:* 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

---

# 34. 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.

### Operation when a stack configuration is used

The command can display information only for the master switch.

### Example

The following figure shows an example of displaying L2 loop detection information.

*Figure 34-1: Example of displaying L2 loop detection information*

```
> show loop-detection
Date 20XX/04/21 12:10:10 UTC
Interval Time           :10
Output Rate             :30pps
Threshold               :1000
Hold Time               :300
Auto Restore Time       :3600
VLAN Port Counts
  Configuration         :103          Capacity      :300
Port Information
  Port   Status   Type      DetectCnt  RestoringTimer  SourcePort  Vlan
  1/0/1   Up      send-inact  100        -              1/0/3       4090
  1/0/2   Down    send-inact   0          -              -           -
  1/0/3   Up      send       100        -              1/0/1       4090
  1/0/4   Up      exception   0          -              -           -
  1/0/5   Down(loop) send-inact 1000        1510         CH:32 (U)    100
  CH:1    Up      trap        0          -              -           -
  CH:32   Up      uplink      -          -              1/0/5       100
>
```

## Display items

Table 34-1: Items displayed for L2 loop detection information

Item	Meaning	Displayed information
Interval Time	Interval for sending L2 loop detection frames (in seconds)	--
Output Rate	L2 loop detection frame transmission rate (packets/s)	The current transmission rate for L2 loop detection frames is displayed.
Threshold	Number of detections 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 <sup>#</sup> 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 <sup>#</sup> where L2 loop detection frames can be sent at the defined transmission rate is displayed.
Port	Port number or channel group number	<switch no.> / <nif no.> / <port no.>: Indicates the port number. CH: <channel group number>: Indicates the channel group number.
Status	Port 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. <switch no.>/<nif no.>/<port no.>: Indicates the port number. CH: <channel group number>: Indicates the channel group number. For the receive uplink port, (U) is displayed. - is displayed if no L2 loop detection frames have been received.
Vlan	Source VLAN ID of the L2 loop detection frame	Displays the source VLAN ID when an L2 loop detection frame was last received.

#: Total number of VLANs set for the applicable physical ports or channel groups.

### Impact on communication

None

### Response messages

Table 34-2: List of response messages for the show loop-detection command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Loop Detection program.	Communication with the L2 loop detection program failed. Re-execute the command.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the 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.

### Operation when a stack configuration is used

The command can display information only for the master switch.

### Example

The following figure is an example of displaying L2 loop detection statistics.

*Figure 34-2: Example of displaying L2 loop detection statistics*

```
> show loop-detection statistics
Date 20XX/04/21 12:10:10 UTC
Port:1/0/1   Up           Type :send-inact
  TxFrame      :           10000000  RxFrame      :           1200
  Inactive Count:           3         RxDiscard     :           30
  Last Inactive : 20XX/04/10 19:20:20 Last RxFrame  : 20XX/04/21 12:02:10
Port:1/0/2   Down        Type :send-inact
  TxFrame      :           0         RxFrame      :           0
  Inactive Count:           0         RxDiscard     :           0
  Last Inactive :           -         Last RxFrame  :           -
Port:1/0/3   Up           Type :send
  TxFrame      :           10000000  RxFrame      :           600
  Inactive Count:           0         RxDiscard     :           0
  Last Inactive :           -         Last RxFrame  : 20XX/04/10 19:20:20
Port:1/0/4   Up           Type :exception
  TxFrame      :           0         RxFrame      :           0
  Inactive Count:           0         RxDiscard     :           0
  Last Inactive :           -         Last RxFrame  :           -
Port:1/0/5   Down(loop)  Type :send-inact
```

```

TxFrame      :          12000  RxFrame      :          1
Inactive Count:          1    RxDiscard    :          0
Last Inactive : 20XX/04/21 09:30:50 Last RxFrame : 20XX/04/21 09:30:50
CH:1         Up              Type :trap
TxFrame      :          0    RxFrame      :          0
Inactive Count:          0    RxDiscard    :          0
Last Inactive :          -    Last RxFrame :          -
CH:32        Up              Type :uplink
TxFrame      :          0    RxFrame      :         100
Inactive Count:          0    RxDiscard    :          0
Last Inactive :          -    Last RxFrame : 20XX/04/21 09:30:50
>

```

## Display items

Table 34-3: Items displayed for L2 loop detection statistics

Item	Meaning	Displayed information
Port	Port number	<switch no.> / <nif no.> / <port no.>: Indicates the port number.
CH	Channel group number	<channel group number>: Indicates the channel group number.
Up	The port is in Up status.	--
Down	The port is in Down status.	--
Down(loop)	The port status is Down due to the L2 loop detection 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 34-4:* List of response messages for the show loop-detection statistics command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Loop Detection program.	Communication with the L2 loop detection program failed. Re-execute the command.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the 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

### Operation when a stack configuration is used

The command can display information only for the master switch.

### Example

The following figure is an example of displaying log information about the received L2 loop detection frames.

*Figure 34-3: Example of displaying log information for received L2 loop detection frames*

```
> show loop-detection logging
Date 20XX/04/21 12:10:10 UTC
20XX/04/21 12:10:10 1/0/1 Source: 1/0/3 Vlan: 4090 Inactive
20XX/04/21 12:10:09 1/0/1 Source: 1/0/3 Vlan: 1
20XX/04/21 12:10:08 1/0/1 Source: 1/0/3 Vlan: 4090
20XX/04/21 12:10:07 1/0/3 Source: 1/0/1 Vlan: 4090
20XX/04/21 12:10:06 1/0/3 Source: 1/0/1 Vlan: 4090
20XX/04/20 05:10:10 CH:32 Source: CH:32 Vlan: 4090 Uplink Inactive
20XX/04/10 04:10:10 1/0/20 Source: CH:32 Vlan: 4090
20XX/03/21 03:10:10 1/0/20 Source: 1/0/12 Vlan: 4093
20XX/03/21 02:12:50 1/0/20 Source: 1/0/12 Vlan: 4093
20XX/03/21 02:12:10 1/0/20 Source: 1/0/12 Vlan: 4093
20XX/03/21 02:12:09 1/0/20 Source: 1/0/12 Vlan: 12
20XX/09/05 20:00:00 CH:32 Source: 1/0/12 Vlan: 12 Uplink
20XX/09/05 00:00:00 CH:32 Source: 1/0/12 Vlan: 12 Uplink
>
```

### Display items

*Table 34-5: 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
<switch no.>/<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.

Item	Meaning	Displayed information
Source	The number of the port from which the L2 loop detection frame was sent	Displays the number of the port from which the L2 loop detection frame was sent. <code>&lt;switch no.&gt; / &lt;nif no.&gt; / &lt;port no.&gt;</code> : Indicates the port number. <code>CH: &lt;channel group number&gt;</code> : Indicates the channel group number.
Vlan	VLAN ID	Displays the VLAN ID when an L2 loop detection frame was sent.
Uplink	Uplink port	Indicates that an L2 loop detection frame was received on an uplink port.
Inactive	The status is changed to inactive status.	Indicates that the status is changed to inactive status.

### Impact on communication

None

### Response messages

Table 34-6: List of response messages for the show loop-detection logging command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Loop Detection program.	Communication with the L2 loop detection program failed. Re-execute the command.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the 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.

### Operation when a stack configuration is used

The command can clear information only from the master switch.

### Example

The following figure is an example of clearing L2 loop detection statistics.

*Figure 34-4: Example of clearing L2 loop detection statistics*

```
> clear loop-detection statistics
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 34-7: List of response messages for the clear loop-detection statistics command*

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.

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.

**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

### Operation when a stack configuration is used

The command can clear information only from the master switch.

### Example

The following figure is an example of clearing the log information for received L2 loop detection frames.

*Figure 34-5: 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 34-8: List of response messages for the clear loop-detection statistics command*

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to L2 Loop Detection program.	Communication with the L2 loop detection program failed. Re-execute the command.
L2 Loop Detection is not configured.	L2 loop detection has not been set, or the 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.

### Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the `remote command` command.

```
remote command {<switch no.> | all} restart loop-detection [-f] [core-file]
```

### Example

The following figure is an example of restarting the L2 loop detection program.

*Figure 34-6: 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 34-9: 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

### Operation when a stack configuration is used

To execute this command for member switches other than the master switch, use the `remote command` command.

```
remote command {<switch no.> | all} dump protocols loop-detection
```

### Example

The following figure is an example of outputting detailed event trace information and control table information to a file.

*Figure 34-7: 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 34-10: 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

---

# 35. 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

```
i2ping {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.

## Operation when a stack configuration is used

This command is not supported.

## Example

The following figure is an example of executing the l2ping command.

*Figure 35-1: Example of executing the l2ping command*

```
>l2ping remote-mep 1010 domain-level 7 ma 1000 mep 1020 count 3
L2ping to MP:1010(0012.e220.00a3) on Level:7 MA:1000 MEP:1020 VLAN:20
Time:20XX/03/10 19:10:24
1: L2ping Reply from 0012.e220.00a3 64bytes Time= 751 ms
2: L2ping Reply from 0012.e220.00a3 64bytes Time= 752 ms
3: L2ping Reply from 0012.e220.00a3 64bytes Time= 753 ms

--- L2ping Statistics ---
Tx L2ping Request : 3 Rx L2ping Reply : 3 Lost Frame : 0%
Round-trip Min/Avg/Max : 751/752/753 ms
>
```

## Display items

*Table 35-1: 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	0-7
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 (%)	--

Item	Meaning	Displayed information
Round-trip Min/Avg/Max	Minimum, average, and maximum response time	--

## Impact on communication

None

## Response messages

*Table 35-2: List of response messages for the l2ping command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.
No such Remote MEP.	The specified remote MEP is unknown. Make sure the specified parameter is correct, and then try again.
Now another user is using CFM command, please try again.	Another user is using the CFM command. Wait a while, and then retry the operation.
Specified Domain Level is not configured.	The specified domain level has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MA is not configured.	The specified MA ID number or the primary VLAN for the specified MA has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MEP is not configured.	The specified MEP ID has not been configured. Make sure the specified parameter is correct, and then try again.

## Notes

- To halt execution of this command, press **Ctrl + C**.
- This command cannot be used concurrently by multiple users.
- If you want to specify 1477 bytes or more for the `framesize` parameter, use the `mtu` or `system mtu` configuration command to set the MTU value for jumbo frames to 1500 bytes or more.
- To verify connectivity, use the MAC address for the remote MP. Even when `remote-mep` is specified, the connectivity is verified by using the MAC address that corresponds to the MEP ID. Therefore, even when the specified MEP ID does not exist, due to a configuration change or another reason, a reply is sent if an MEP or MIP has that MAC address.

---

## l2tracertoute

---

Verifies the route from the Switch's MEP to a remote MEP or MIP.

### Syntax

```
l2tracertoute {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.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure is an example of executing the `l2tracertoute` command.

*Figure 35-2: Example of executing the l2tracertoute command*

```
>l2tracertoute remote-mep 1010 domain-level 7 ma 1000 mep 1020 ttl 255
```

```

L2tracert to MP:1010(0012.e220.00a3) on Level:7  MA:1000  MEP:1020  VLAN:20
Time:20XX/03/17 10:42:20
254 0012.e220.00c2 Forwarded
253 0012.e210.000d Forwarded
252 0012.e220.00a3 NotForwarded Hit
>

```

## Display items

Table 35-3: 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	0-7
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	0-255
<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 35-4: List of response messages for the l2tracert command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.
No such Remote MEP.	The specified remote MEP is unknown. Make sure the specified parameter is correct, and then try again.

Message	Description
Now another user is using CFM command, please try again.	Another user is using the CFM command. Wait a while, and then retry the operation.
Specified Domain Level is not configured.	The specified domain level has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MA is not configured.	The specified MA ID number or the primary VLAN for the specified MA has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MEP is not configured.	The specified MEP ID has not been configured. Make sure the specified parameter is correct, and then try again.

## Notes

- To halt execution of this command, press **Ctrl + C**.
- This command cannot be used concurrently by multiple users.
- If you execute this command multiple times for the same remote MP, only the last execution result is retained in the linktrace database.
- Information about some replies is not displayed if those replies are received after being forwarded by a number of devices that exceeds the number of devices on the routes that can be registered in the linktrace database.
- The MAC address of the remote MP is used to verify the route. Even when `remote-mep` is specified, the route is verified by using the MAC address that corresponds to the MEP ID. Therefore, even when the specified MEP ID does not exist, due to a configuration change or another reason, a reply is sent if an MEP or MIP has that MAC address.

---

## show cfm

---

Displays the configuration information for domains and MPs, and the CFM information related to detected failures.

### Syntax

```
show cfm [{[domain-level <level>] [ma <no.>] [mep <mepid>] | summary}]
```

### Input mode

User mode and administrator mode

### Parameters

```
{[domain-level <level>] [ma <no.>] [mep <mepid>] | summary}
```

domain-level <level>

Displays CFM information for the specified domain level.

ma <no.>

Displays CFM information for the specified MA ID number.

mep <mepid>

Displays CFM information for the specified MEP ID.

Operation when each parameter is omitted:

Only the CFM information conforming to the specified parameter condition can be displayed. If the parameter is not specified, the CFM information is displayed with no condition applied. If multiple parameters are specified, the CFM information conforming to the conditions will be displayed.

summary

Displays the number of MPs and CFM ports that can be accommodated.

Operation when this parameter is omitted:

All CFM information is displayed.

### Operation when a stack configuration is used

This command is not supported.

### Example 1

The following figure is an example of displaying the CFM configuration information.

*Figure 35-3: Example of displaying the CFM configuration information*

```
>show cfm
Date 20XX/03/15 18:32:10 UTC
Domain Level 3 Name(str): ProviderDomain_3
  MA 300   Name(str) : Tokyo_to_Osaka
    Primary VLAN:300   VLAN:10-20,300
    CC:Enable   Interval:1min
    Alarm Priority:2   Start Time: 2500ms   Reset Time:10000ms
    MEP Information
      ID:8012 UpMEP    CH1 (Up)    Enable   MAC:0012.e200.00b2   Status:Timeout
  MA 400   Name(str) : Tokyo_to_Nagoya
    Primary VLAN:400   VLAN:30-40,400
    CC:Enable   Interval:1min
    Alarm Priority:2   Start Time: 2500ms   Reset Time:10000ms
    MEP Information
      ID:8014 DownMEP  0/21(Up)    Disable  MAC:0012.e220.0040   Status:-
```

```

MIP Information
  0/12 (Up)    Enable   MAC:0012.e200.0012
  0/22 (Down) Disable   MAC:-
Domain Level 4 Name(str): ProviderDomain_4
MIP Information
  CH12 (Up)   Enable   MAC:0012.e220.00b2
>

```

## Display items in Example 1

Table 35-5: 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"> <li>0: Indicates that no alarms are reported.</li> <li>1: Indicates that a failure was detected on the remote MEP.</li> <li>2: Indicates a port failure on the remote MEP.</li> <li>3: Indicates CCM timeout.</li> <li>4: Indicates that an invalid CCM was received from the remote MEP in the MA.</li> <li>5: Indicates that a CCM was received from another MA.</li> </ul> - is displayed if CC is disabled.

Item	Meaning	Displayed information
Start Time	Time from the detection of a failure until an alarm is generated	2500-10000ms: The time elapsed from the detection of a failure until an alarm is generated. - is displayed if CC is disabled.
Reset Time	Time from the detection of a failure until an alarm is canceled	2500-10000ms: The time elapsed from the detection of a failure until an alarm is canceled. - is displayed if CC is disabled.
MEP Information	MEP information	--
ID	MEP ID	MEP ID for the Switch
UpMEP	Up MEP	MEP facing the relay side
DownMEP	Down MEP	MEP facing the line
<nif no.>/<port no.>	Port number	MEP port number
CH<channel group number>	Channel group number	MEP channel group number
Up	The port is in Up status.	Indicates that the port is in Up status. If link aggregation is used, this means that the channel group is in Up status.
Down	The port is in Down status.	Indicates that the port is in Down status. If link aggregation is used, this means that the channel group is in Down status.
Enabled	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"> <li>• OtherCCM: Indicates that a CCM was received from another MA.</li> <li>• ErrorCCM: Indicates that a CCM that contains an invalid MEP ID, or a CCM with an invalid transmission interval, was received.</li> <li>• Timeout: Indicates CCM timeout.</li> <li>• PortState: Indicates that a CCM reporting a port failure was received.</li> <li>• RDI: Indicates a CCM reporting failure detection was received.</li> </ul> - 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.
Enabled	CFM on a port is enabled.	--

Item	Meaning	Displayed information
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 35-4:* Example of displaying the number of entities accommodated in the CFM configuration

```
>show cfm summary
Date 20XX/03/14 18:32:20 UTC
DownMEP Counts      :      2
UpMEP Counts        :      2
MIP Counts           :      5
CFM Port Counts      :      9
>
```

## Display items in Example 2

*Table 35-6:* 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 35-7:* List of response messages for the show cfm command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.
Specified Domain Level is not configured.	The specified domain level has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MA is not configured.	The specified MA ID has not been configured. Make sure the specified parameter is correct, and then try again.

Message	Description
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 each parameter is omitted:

This command can display only the information relevant to the condition applied by a parameter that has been set. If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information conforming to the conditions will be displayed.

detail

Displays the 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.

### Operation when a stack configuration is used

This command is not supported.

### Example 1

The following figure is an example of displaying remote MEP information.

*Figure 35-5: Example of displaying remote MEP information*

```
>show cfm remote-mep
Date 20XX/03/20 18:05:12 UTC
Total RMEP Counts:      4
Domain Level 3 Name(str): ProviderDomain_3
  MA 100   Name(str) : Tokyo_to_Osaka
    MEP ID:101   0/20 (Up)   Enable   Status:Timeout
      RMEP Information Counts: 2
        ID:3      Status:Timeout   MAC:0012.e220.1224   Time:20XX/03/20 17:55:20
        ID:15     Status:-         MAC:0012.e200.005a   Time:20XX/03/20 18:04:54
```

```

MA 200   Name(str) : Tokyo_to_Nagoya
MEP ID:8012 CH1 (Up)   Enable   Status:-
RMEP Information Counts: 2
ID:8003 Status:-      MAC:0012.e20a.1241   Time:20XX/03/20 12:12:20
ID:8004 Status:-      MAC:0012.e20d.12a1   Time:20XX/03/20 12:12:15
>

```

## Display items in Example 1

Table 35-8: Items displayed for remote MEP information

Item	Meaning	Displayed information
Total RMEP Counts	Total number of remote MEPs	--
Domain Level <i>&lt;level&gt;</i>	Domain level and domain name	<i>&lt;level&gt;</i> : Indicates the domain level. Name: -: Indicates that the domain name is not used. Name(str): <i>&lt;name&gt;</i> : Indicates that a character string is used for the domain name. Name(dns): <i>&lt;name&gt;</i> : Indicates that the domain name server name is used for the domain name. Name(mac): <i>&lt;mac&gt;</i> ( <i>&lt;id&gt;</i> ): Indicates that the MAC address and ID are used for the domain name.
MA <i>&lt;no.&gt;</i>	MA ID number and MA name	<i>&lt;no.&gt;</i> : Indicates the MA ID number when the configuration was set. Name(str): <i>&lt;name&gt;</i> : Indicates that a character string is used for the MA name. Name(id): <i>&lt;id&gt;</i> : Indicates that a numeric value is used for the MA name. Name(vlan): <i>&lt;vlan id&gt;</i> : Indicates that the VLAN ID is used for the MA name.
MEP ID	MEP ID for the Switch	--
<i>&lt;nif no.&gt;/&lt;port no.&gt;</i>	Port number	MEP port number
CH <i>&lt;channel group number&gt;</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"> <li>OtherCCM: Indicates that a CCM was received from another MA.</li> <li>ErrorCCM: Indicates that a CCM that contains an invalid MEP ID, or a CCM with an invalid transmission interval, was received.</li> <li>Timeout: Indicates CCM timeout.</li> <li>PortState: Indicates that a CCM reporting a port failure was received.</li> <li>RDI: Indicates a CCM reporting failure detection was received.</li> </ul> - is displayed if no failure has been detected.
RMEP Information	Remote MEP information	--
Counts	Number of remote MEPs	--

Item	Meaning	Displayed information
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"> <li>• OtherCCM: Indicates that a CCM was received from another MA.</li> <li>• ErrorCCM: Indicates that a CCM that contains an invalid MEP ID, or a CCM with an invalid transmission interval, was received.</li> <li>• Timeout: Indicates CCM timeout.</li> <li>• PortState: Indicates that a CCM reporting a port failure was received.</li> <li>• RDI: Indicates a CCM reporting failure detection was received.</li> </ul> - 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 35-6: Example of displaying detailed remote MEP information*

```
> show cfm remote-mep detail
Date 20XX/03/20 18:19:03 UTC
Total RMEP Counts:      4
Domain Level 3 Name(str): ProviderDomain_3
  MA 100  Name(str) : Tokyo_to_Osaka
    MEP ID:101  0/20(Up)  Enable  Status:Timeout
      RMEP Information Counts: 2
        ID:3  Status:Timeout  MAC:0012.e220.1224  Time:20XX/03/20 17:55:20
          Interface:Up  Port:Forwarding  RDI:On
          Chassis ID Type:MAC  Info: 0012.e220.1220
        ID:15  Status:-  MAC:0012.e200.005a  Time:20XX/03/20 18:04:54
          Interface:Up  Port:Forwarding  RDI:-
          Chassis ID Type:MAC  Info: 0012.e200.0050
>
```

## Display items in Example 2

*Table 35-9: 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 <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.
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"> <li>• OtherCCM: Indicates that a CCM was received from another MA.</li> <li>• ErrorCCM: Indicates that a CCM that contains an invalid MEP ID, or a CCM with an invalid transmission interval, was received.</li> <li>• Timeout: Indicates CCM timeout.</li> <li>• PortState: Indicates that a CCM reporting a port failure was received.</li> <li>• RDI: Indicates a CCM reporting failure detection was received.</li> </ul> - 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"> <li>• OtherCCM: Indicates that a CCM was received from another MA.</li> <li>• ErrorCCM: Indicates that a CCM that contains an invalid MEP ID, or a CCM with an invalid transmission interval, was received.</li> <li>• Timeout: Indicates CCM timeout.</li> <li>• PortState: Indicates that a CCM reporting a port failure was received.</li> <li>• RDI: Indicates a CCM reporting failure detection was received.</li> </ul> - 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"> <li>• Up: Indicates Up status.</li> <li>• Down: Indicates Down status.</li> <li>• Testing: Indicates that the test is being performed.</li> <li>• Unknown: The status is unknown.</li> <li>• Dormant: Waiting for an external event</li> <li>• NotPresent: There is no component for the interface.</li> <li>• LowerLayerDown: Indicates that the status of the lower-layer interface is Down.</li> </ul> <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"> <li>• Forwarding: Indicates Forwarding status.</li> <li>• Blocked: Indicates blocking status.</li> </ul> <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"> <li>• On: Indicates that a failure is being detected.</li> </ul> <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 of the chassis ID	<p>Type of the information displayed for Info.</p> <ul style="list-style-type: none"> <li>• CHAS-COMP: Indicates that entPhysicalAlias of the Entity MIB is displayed for Info.</li> <li>• CHAS-IF: Indicates that ifAlias of the interface MIB is displayed for Info.</li> <li>• PORT: Indicates that portEntPhysicalAlias of the Entity MIB is displayed for Info.</li> <li>• MAC: Indicates that macAddress of the CFM MIB is displayed for Info.</li> <li>• NET: Indicates that networkAddress of the CFM MIB is displayed for Info.</li> <li>• NAME: Indicates that ifName of the interface MIB is displayed for Info.</li> <li>• LOCAL: Indicates that local of the CFM MIB is displayed for Info.</li> </ul> <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 35-10:* List of response messages for the show cfm remote-mep command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.
No such Remote MEP.	The specified remote MEP is unknown. Make sure the specified parameter is correct, and then try again.
Specified Domain Level is not configured.	The specified domain level has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MA is not configured.	The specified MA ID 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 each parameter is omitted:

This command can display only the information relevant to the condition applied by a parameter that has been set. If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information conforming to the conditions will be displayed.

detail

Displays detailed information about a failure.

Operation when this parameter is omitted:

Summary information about a failure is displayed.

Operation when all parameters are omitted:

Summary information about all failures is displayed.

### Operation when a stack configuration is used

This command is not supported.

### Example 1

The following figure is an example of displaying summary information about a CFM failure.

*Figure 35-7: Example of displaying failure information*

```
>show cfm fault
Date 20XX/03/21 10:24:12 UTC
MD:7 MA:1000 MEP:1000 Fault      Time:20XX/03/21 10:15:21
```

```

MD:7  MA:1010  MEP:1011  Cleared  Time:-
MD:6  MA:100   MEP:600   Cleared  Time:-
>

```

## Display items in Example 1

Table 35-11: Items displayed for failure information

Item	Meaning	Displayed information
MD	Domain level	0-7
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 35-8: Example of displaying detailed failure information

```

>show cfm fault domain-level 7 detail
Date 20XX/03/21 12:00:15 UTC
MD:7  MA:1000  MEP:1000  Fault
  OtherCCM : -   RMEP:1001 MAC:0012.e220.11a1 VLAN:1000 Time:20XX/03/21 11:22:17
  ErrorCCM : -
  Timeout  : On  RMEP:1001 MAC:0012.e220.11a1 VLAN:1000 Time:20XX/03/21 11:42:10
  PortState: -
  RDI      : -
MD:7  MA:1010  MEP:1011  Cleared
  OtherCCM : -
  ErrorCCM : -
  Timeout  : -   RMEP:1001 MAC:0012.e220.22a1 VLAN:200   Time:20XX/03/21 10:22:17
  PortState: -
  RDI      : -
>

```

## Display items in Example 2

Table 35-12: Items displayed for detailed failure information

Item	Meaning	Displayed information
MD	Domain level	0-7
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 35-13: List of response messages for the show cfm fault command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.
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.

### Operation when a stack configuration is used

This command is not supported.

### Example 1

The following figure is an example of displaying route information in the linktrace database.

*Figure 35-9: Example of displaying linktrace database information*

```
> show cfm l2traceroute-db
Date 20XX/03/15 10:05:30 UTC
L2traceroute to MP:0012.e220.00a3 on Level:7 MA:1000 MEP:1020 VLAN:1000
Time:20XX/03/14 17:42:20
254 0012.e220.00c0 Forwarded
253 0012.e210.000d Forwarded
252 0012.e220.00a3 NotForwarded Hit

L2traceroute to MP:2010(0012.e220.1040) on Level:7 MA:2000 MEP:2020 VLAN:20
Time:20XX/03/14 17:37:55
63 0012.e220.10a9 Forwarded
62 0012.e220.10c8 NotForwarded
>
```

## Display items in Example 1

Table 35-14: 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	0-7
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	0-255
<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 35-10: Example of displaying detailed linktrace database information

```
> show cfm l2traceroute-db remote-mep 2010 domain-level 7 ma 2000 detail
Date 20XX/03/15 10:30:12 UTC
L2traceroute to MP:2010(0012.e220.1040) on Level:7 MA:2000 MEP:2020 VLAN:20
Time:20XX/03/14 17:37:55
63 0012.e220.10a9 Forwarded
  Last Egress : 0012.e210.2400 Next Egress : 0012.e220.10a0
  Relay Action: MacAdrTbl
  Chassis ID   Type: MAC           Info: 0012.e228.10a0
  Ingress Port MP Address: 0012.e220.10a9 Action: OK
  Egress Port  MP Address: 0012.e220.10aa Action: OK
62 0012.e228.aa38 NotForwarded
  Last Egress : 0012.e220.10a0 Next Egress : 0012.e228.aa30
  Relay Action: MacAdrTbl
  Chassis ID   Type: MAC           Info: 0012.e228.aa30
  Ingress Port MP Address: 0012.e228.aa38 Action: OK
  Egress Port  MP Address: 0012.e228.aa3b Action: Down
>
```

## Display items in Example 2

Table 35-15: Items displayed for the detailed 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	0-7
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
<tll>	Time to Live	0-255
<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"> <li>• RlyHit: A linktrace message was not forwarded because it had reached the destination (the destination remote MEP or MIP).</li> <li>• MacAdrTbl: A linktrace message was forwarded by using the MAC address table.</li> <li>• MPCCMDB: A linktrace message was forwarded by using the MIPCCM database.</li> </ul> - 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"> <li>CHAS-COMP: Indicates that entPhysicalAlias of the Entity MIB is displayed for Info.</li> <li>CHAS-IF: Indicates that ifAlias of the interface MIB is displayed for Info.</li> <li>PORT: Indicates that portEntPhysicalAlias of the Entity MIB is displayed for Info.</li> <li>MAC: Indicates that macAddress of the CFM MIB is displayed for Info.</li> <li>NET: Indicates that networkAddress of the CFM MIB is displayed for Info.</li> <li>NAME: Indicates that ifName of the interface MIB is displayed for Info.</li> <li>LOCAL: Indicates that local of the CFM MIB is displayed for Info.</li> </ul> <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"> <li>OK: Indicates normal status.</li> <li>Down: Indicates Down status.</li> <li>Blocked: Indicates Blocked status.</li> <li>NOVLAN: Indicates that there is no VLAN setting for linktrace messages.</li> </ul> <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"> <li>OK: Indicates normal status.</li> <li>Down: Indicates Down status.</li> <li>Blocked: Indicates Blocked status.</li> <li>NOVLAN: Indicates that there is no VLAN setting for linktrace messages.</li> </ul> <p>- is displayed if this information is not found in the received linktrace reply.</p>

**Impact on communication**

None

**Response messages***Table 35-16:* List of response messages for the show cfm l2traceroute-db command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.

**Notes**

Information about some replies is not displayed if those replies are received after being forwarded by a number of devices that exceeds the number of devices on the routes that can be registered in the linktrace database.

---

## show cfm statistics

---

Displays the CFM statistics.

### Syntax

```
show cfm statistics [domain-level <level>] [ma <no.>] [mep <mepid>]
```

### Input mode

User mode and administrator mode

### Parameters

domain-level <level>

Displays the CFM statistics for the specified domain level.

ma <no.>

Displays the CFM statistics for the specified MA ID number.

mep <mepid>

Displays the CFM statistics for the specified MEP ID.

Operation when each parameter is omitted:

This command can display only the information relevant to the condition applied by a parameter that has been set. If the parameter has not been set, information is displayed with no condition applied. If multiple parameters are specified, information conforming to the conditions will be displayed.

Operation when all parameters are omitted:

All CFM statistics are displayed.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure is an example of displaying CFM statistics.

*Figure 35-11: Example of displaying CFM statistics*

```
>show cfm statistics domain-level 3
Date 20XX/03/15 18:32:10 UTC
Domain Level 3 Name(str): ProviderDomain_3
  MA 300   Name(str) : Tokyo_to_Osaka_300
    MEP ID:10   0/47(Up)   CFM:Disable
      CCM Tx:      80155 Rx:      784 RxDiscard:      6
      LBM Tx:       2 Rx:       11 RxDiscard:      1
      LBR Tx:      12 Rx:       2 RxDiscard:      0
      LTM Tx:       0 Rx:       0 RxDiscard:      0
      LTR Tx:       0 Rx:       0 RxDiscard:      0
                                Other RxDiscard:      0

    MIP Information
      0/48(Up)   CFM:Enable
        CCM Tx:      - Rx:      - RxDiscard:      -
        LBM Tx:      - Rx:      0 RxDiscard:      1
        LBR Tx:       0 Rx:      - RxDiscard:      -
        LTM Tx:      - Rx:      3 RxDiscard:      0
        LTR Tx:       3 Rx:      - RxDiscard:      -
                                Other RxDiscard:      0

>
```

## Display items

Table 35-17: Items displayed for CFM statistics

Item		Meaning	Displayed information
Domain Level <i>&lt;level&gt;</i>		Domain level and domain name	<i>&lt;level&gt;</i> : Indicates the domain level. Name: -: Indicates that the domain name is not used. Name(str) : <i>&lt;name&gt;</i> : Indicates that a character string is used for the domain name. Name(dns) : <i>&lt;name&gt;</i> : Indicates that the domain name server name is used for the domain name. Name(mac) : <i>&lt;mac&gt;</i> ( <i>&lt;id&gt;</i> ) : Indicates that the MAC address and ID are used for the domain name.
MA <i>&lt;no.&gt;</i>		MA ID number and MA name	<i>&lt;no.&gt;</i> : Indicates the MA ID number when the configuration was set. Name(str) : <i>&lt;name&gt;</i> : Indicates that a character string is used for the MA name. Name(id) : <i>&lt;id&gt;</i> : Indicates that a numeric value is used for the MA name. Name(vlan) : <i>&lt;vlan id&gt;</i> : Indicates that the VLAN ID is used for the MA name.
MEP ID		MEP ID for the Switch	--
<i>&lt;nif no.&gt;/&lt;port no.&gt;</i>		Port number	MEP port number
CH <i>&lt;channel group number&gt;</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.
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	--
<i>&lt;nif no.&gt;/&lt;port no.&gt;</i>		Port number	MIP port number
CH <i>&lt;channel group number&gt;</i>		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"> <li>• CCM with an invalid format</li> <li>• CCM for another MA</li> <li>• CCM with the same MEP ID as the one set for the Switch</li> <li>• CCM whose transmission interval is different from the Switch's MA</li> </ul> - 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"> <li>• A loopback message with an invalid format</li> <li>• A loopback message whose destination MAC address is not the MAC address for the receiving MP or the multicast address for CC</li> <li>• A loopback message whose source MAC address is the multicast address for a CC or a linktrace</li> <li>• A loopback message whose destination MAC address is not the MAC address for the receiving MIP (for an MIP)</li> </ul>
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"> <li>• A loopback reply with an invalid format</li> <li>• A loopback reply whose destination MAC address is different from the MAC address of the MEP</li> <li>• A loopback reply whose source MAC address is the multicast address or broadcast address</li> <li>• A loopback reply whose Loopback Transaction Identifier value is different from that in the loopback message that was sent</li> <li>• A loopback reply that was received after the wait time for a response that was set by an operation command expired</li> </ul> - 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"> <li>• A linktrace message with an invalid format</li> <li>• A linktrace message whose LTM TTL value is 0</li> <li>• A linktrace message whose destination MAC address is different from the multicast address for linktrace or the MAC address of the receiving MP</li> <li>• A linktrace message that cannot result in a linktrace reply</li> </ul>
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"> <li>• A linktrace reply with an invalid format</li> <li>• A linktrace reply whose destination MAC address is different from the MAC address of the receiving MEP</li> <li>• A linktrace reply whose LTR Transaction Identifier value is different from the value in the linktrace message</li> <li>• A linktrace reply that was received after the wait time for a response that was set by an operation command expired</li> </ul> - 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"> <li>• Unsupported CFM PDUs</li> <li>• Loopback replies and linktrace replies received by MIP</li> </ul>

## Impact on communication

None

## Response messages

Table 35-18: List of response messages for the show cfm statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.
Specified Domain Level is not configured.	The specified domain level has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MA is not configured.	The specified MA ID has not been configured. Make sure the specified parameter is correct, and then try again.
Specified MEP is not configured.	The specified MEP ID has not been configured. Make sure the specified parameter is correct, and then try again.

## Notes

None

---

## clear cfm remote-mep

---

Clears the remote MEP information.

### Syntax

```
clear cfm remote-mep [domain-level <level> [ma <no.> [mep <mepid> [remote-mep
<mepid>]]]]]
```

### Input mode

User mode and administrator mode

### Parameters

domain-level <level>

Clears the remote MEP information for the specified domain level.

ma <no.>

Clears the remote MEP information for the specified MA ID number.

mep <mepid>

Clears the remote MEP information for the specified MEP.

remote-mep <mepid>

Clears the information for the specified remote MEP ID.

Operation when each parameter is omitted:

This command can clear only the information relevant to the condition applied by a parameter that has been set. If no parameter is specified, information is cleared without being limited by any conditions. If multiple parameters are specified, the information conforming to the conditions will be cleared.

Operation when all parameters are omitted:

All remote MEP information is cleared.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure is an example of clearing remote MEP information.

*Figure 35-12: Example of clearing remote MEP information*

```
> clear cfm remote-mep
>
```

### Display items

None

### Impact on communication

None

## Response messages

*Table 35-19:* List of response messages for the clear cfm remote-mep command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.

## Notes

None

---

## clear cfm fault

---

Clears the CFM failure information.

### Syntax

```
clear cfm fault [domain-level <level> [ma <no.> [mep <mepid>]]]
```

### Input mode

User mode and administrator mode

### Parameters

domain-level <level>

Clears the failure information for the specified domain level.

ma <no.>

Clears the failure information for the specified MA ID number.

mep <mepid>

Clears the failure information for the specified MEP ID.

Operation when each parameter is omitted:

This command can clear only the information relevant to the condition applied by a parameter that has been set. If no parameter is specified, information is cleared without being limited by any conditions. If multiple parameters are specified, the information conforming to the conditions will be cleared.

Operation when all parameters are omitted:

All failure information is cleared.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure is an example of clearing CFM failure information.

*Figure 35-13: Example of clearing CFM failure information*

```
> clear cfm fault
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 35-20: List of response messages for the clear cfm fault command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.

Message	Description
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.

**Notes**

None

---

## clear cfm l2traceroute-db

---

Clears CFM linktrace database information.

### Syntax

```
clear cfm l2traceroute-db
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure is an example of clearing CFM linktrace database information.

*Figure 35-14: Example of clearing CFM linktrace database information*

```
> clear cfm l2traceroute-db
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 35-21: List of response messages for the clear cfm l2traceroute-db command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.

### Notes

None

---

## clear cfm statistics

---

Clears the CFM statistics.

### Syntax

```
clear cfm statistics [domain-level <level> [ma <no.> [mep <mepid>]]]
clear cfm statistics [domain-level <level> [mip] [port <port list>]
[channel-group-number <channel group list>]]
```

### Input mode

User mode and administrator mode

### Parameters

domain-level <level>

Clears CFM statistics for the specified domain level.

ma <no.>

Clears CFM statistics for the specified MA ID number.

mep <mepid>

Clears CFM statistics for the specified MEP ID.

mip

Clears CFM statistics for MIP.

port <port list>

Clears CFM statistics for the specified port number. For details about how to specify <port list> and the specifiable range of values, see *Specifiable values for parameters*.

channel-group-number <channel group list>

Clears CFM statistics for the channel groups specified in list format in the specified link aggregation. For details about how to specify <channel group list>, see *Specifiable values for parameters*.

Operation when each parameter is omitted:

This command can clear only the information relevant to the condition applied by a parameter that has been set. If no parameter is specified, information is cleared without being limited by any conditions. If multiple parameters are specified, the information conforming to the conditions will be cleared.

Operation when all parameters are omitted:

All CFM statistics are cleared.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure is an example of clearing CFM statistics.

*Figure 35-15: Example of clearing CFM statistics*

```
> clear cfm statistics
>
```

**Display items**

None

**Impact on communication**

None

**Response messages***Table 35-22:* List of response messages for the clear cfm statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
CFM is not configured.	CFM has not been configured. Check the configuration.
Connection failed to CFM program.	Communication with the CFM program failed. Re-execute the command.

**Notes**

None

---

## restart cfm

---

Restarts the CFM program.

### Syntax

```
restart cfm [-f] [core-file]
```

### Input mode

User mode and administrator mode

### Parameters

-f

Restarts the CFM program without 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.

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure is an example of restarting the CFM program.

*Figure 35-16: 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 35-23: 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

### Operation when a stack configuration is used

This command is not supported.

### Example

The following figure is an example for collecting dump information of the CFM program.

*Figure 35-17: Example of collecting dump information of the CFM program*

```
> dump protocols cfm
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 35-24: 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

---

# 36. 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
```

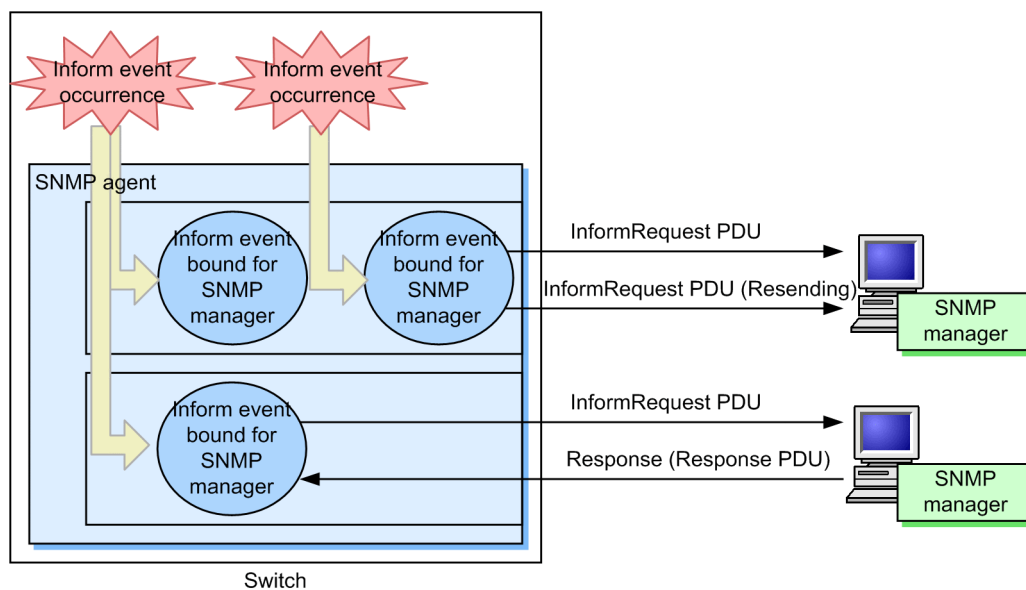
## show snmp

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 36-1: InformRequest information



### Syntax

```
show snmp
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

### Example

Figure 36-2: Example of executing the show snmp command

```
> show snmp
Date 20XX/12/27 15:06:08 UTC
Contact: Suzuki@example.com
Location: ServerRoom
SNMP packets input : 137      (get:417 set:2)
  Get-request PDUs   : 18
  Get-next PDUs     : 104
  Get-bulk PDUs      : 0
  Set-request PDUs   : 6
  Response PDUs      : 3      (with error 0)
  Error PDUs         : 7
```

```

Bad SNMP version errors: 1
Unknown community name : 5
Illegal operation       : 1
Encoding errors         : 0

SNMP packets output : 185
Trap PDUs             : 4
Inform-request PDUs   : 53
Response PDUs         : 128    (with error 4)
  No errors            : 124
  Too big errors       : 0
  No such name errors  : 3
  Bad values errors    : 1
  General errors       : 0
Timeouts              : 49
Drops                  : 0

[TRAP]
Host: 192.168.0.1, sent:1
Host: 192.168.0.2, sent:3

[INFORM]
Timeout(sec)         : 10
Retry                 : 5
Pending informs      : 1/25 (current/max)
Host: 192.168.0.3
  sent      :8          retries:26
  response:2          pending:1      failed:5      dropped:0
Host: 192.168.0.4
  sent      :3          retries:15
  response:0          pending:0      failed:3      dropped:0
Host: 2001:db8::10
  sent      :1          retries:0
  response:1          pending:0      failed:0      dropped:0

```

## Display items

*Table 36-1:* 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 <code>snmp-server contact</code> configuration command
Location	Indicates the name of the location where the Switch is installed.	Value set by the <code>snmp-server location</code> configuration command
SNMP packets input	Indicates the <code>snmpInPkts</code> value (total number of received SNMP messages).	
get	Indicates the <code>snmpInTotalReqVars</code> value (total number of MIB objects for which a MIB was successfully collected).	--
set	Indicates the <code>snmpInTotalSetVars</code> value (total number of MIB objects for which a MIB was successfully configured).	--
Get-request PDUs	Indicates the <code>snmpInGetRequests</code> value (total number of received <code>GetRequest</code> PDUs).	--
Get-next PDUs	Indicates the <code>snmpInGetNexts</code> value (total number of received <code>GetNextRequest</code> PDUs).	--
Get-bulk PDUs	Indicates the total number of received <code>GetBulkRequest</code> PDUs.	0-4294967295

Item	Meaning	Displayed information
Set-request PDUs	Indicates the <code>snmpInSetRequests</code> value (total number of received SetRequest PDUs).	--
Response PDUs	Indicates the <code>snmpInGetResponses</code> value (total number of received GetResponse PDUs).	--
with error	Indicates the number of PDUs of the received GetResponse PDUs whose error status is not <code>noError</code> .	0-4294967295
Error PDUs	Indicates the total number of errors that occurred in PDU reception processing.	0-4294967295
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.	0-4294967295
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> .	0-4294967295
No errors	Indicates the total number of sent PDUs whose error status is <code>noError</code> .	0-4294967295
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.	0-4294967295

Item	Meaning	Displayed information
Drops	Indicates the total number of inform events that were bound for the SNMP manager but were discarded because, for example, the maximum number of inform events that can wait for a response was exceeded.	0-4294967295
[TRAP]	Indicates trap information.	
Host	Indicates the host for which the trap is issued.	Value set by the <i>&lt;manager address&gt;</i> parameter of the <code>snmp-server host</code> configuration command
VRF [OS-L3SA]	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.	0-4294967295
[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>&lt;current&gt;/&lt;max&gt;</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>&lt;current&gt;</i> : The number of inform events that are currently held. <i>&lt;max&gt;</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>&lt;manager address&gt;</i> parameter of the <code>snmp-server host</code> configuration command
VRF [OS-L3SA]	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.	0-4294967295
retries	Indicates the number of resent InformRequest PDUs.	0-4294967295
response	Indicates the number of responses from the SNMP manager for inform events bound for the SNMP manager.	0-4294967295
pending	Indicates the number of inform events bound for the SNMP manager that is waiting for a response from another SNMP manager.	0-21000
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.	0-4294967295

Item	Meaning	Displayed information
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.	0-4294967295

### Impact on communication

None

### Response messages

*Table 36-2: List of response messages for the show snmp command*

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to SNMP program.	Communication with the SNMP program failed. Re-execute the command.

### Notes

1. Switches support SNMP operation commands that provide functionality equivalent to the SNMP agent and 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 when the Switch starts, 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 temporarily counted as `sent` and `pending` events.

---

## show snmp pending

---

Displays inform events bound for the SNMP manager that is waiting for a response from another SNMP manager.

### Syntax

```
show snmp pending
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

### Example

*Figure 36-3: Example of executing the show snmp pending command*

```
> show snmp pending
Date 20XX/12/27 15:06:10 UTC
Req ID: 48, Dest: 192.168.0.1, Remaining Retry: 2, Expires in seconds: 3
Req ID: 49, Dest: 192.168.0.2, Remaining Retry: 4, Expires in seconds: 3
Req ID: 50, Dest: 192.168.0.3, Remaining Retry: 2, Expires in seconds: 7
Req ID: 51, Dest: 192.168.0.4, Remaining Retry: 4, Expires in seconds: 7
Req ID: 52, Dest: 2001:db8::10, Remaining Retry: 10, Expires in seconds: 30
```

### Display items

*Table 36-3: 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>&lt;manager address&gt;</i> parameter of the <i>snmp-server</i> host configuration command
VRF [OS-L3SA]	VRF ID of the SNMP manager	Value set by the <i>vrf &lt;vrf id&gt;</i> parameter of the <i>snmp-server</i> host configuration command
Remaining Retry	Remaining number of retries	0-100 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 36-4:* List of response messages for the show snmp pending command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to SNMP program.	Communication with the SNMP program failed. Re-execute the command.
no entries.	There are no inform events bound for the SNMP manager.

## Notes

If this command is executed when inform events bound for the SNMP manager time out simultaneously, the command might display 0 for all sessions as the remaining time before a timeout (as shown in the following example).

### Example

```
> show snmp pending
Date 20XX/12/27 17:06:10 UTC
Req ID: 88, Dest: 192.168.0.1, Remaining Retry: 0, Expires in seconds: 0
Req ID: 89, Dest: 192.168.0.2, Remaining Retry: 0, Expires in seconds: 0
Req ID: 90, Dest: 192.168.0.3, Remaining Retry: 0, Expires in seconds: 0
```

---

## snmp lookup

---

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.

### Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

### Example

*Figure 36-4:* 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 36-5:* List of response messages for the snmp lookup command

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
No match found for <MIB object name>	The applicable <MIB object name> cannot be found by using this command.

### Notes

None

---

## snmp get

---

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.

### Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

### Example

*Figure 36-5: Example of executing the snmp get command*

```
> snmp get sysDescr.0

Name: sysDescr.0
Value: ALAXALA AX3xxxS xxxx Ver. 11.6
> snmp get 1.3.6.1.2.1.1.1.0

Name: sysDescr.0
Value: ALAXALA AX3xxxS xxxx Ver. 11.6
```

### Display items

*Table 36-6: 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 36-7: List of response messages for the snmp get command*

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot translate variable class: <MIB Object Name>	The object name <MIB Object Name> is invalid.

Message	Description
Error code set in packet - General error: <i>&lt;Number&gt;</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>&lt;Number&gt;</i> .
Error code set in packet - No such variable name. Index: <i>&lt;Number&gt;</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>&lt;Number&gt;</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>&lt;Code&gt;</i>	An SNMP frame containing response status code <i>&lt;Code&gt;</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>&lt;ID1&gt;</i> , expected: <i>&lt;ID2&gt;</i>	A frame whose request ID number of the SNMP frame is <i>&lt;ID2&gt;</i> was expected, but an SNMP frame whose request ID number is <i>&lt;ID1&gt;</i> 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.

### Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

### Example

*Figure 36-6: 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 36-8: 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 36-9: List of response messages for the snmp getnext command*

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot translate variable class: <MIB Object Name>	The object name <MIB Object Name> is invalid.

Message	Description
Error code set in packet - General error: <i>&lt;Number&gt;</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>&lt;Number&gt;</i> .
Error code set in packet - No such variable name. Index: <i>&lt;Number&gt;</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>&lt;Number&gt;</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>&lt;Code&gt;</i>	An SNMP frame containing response status code <i>&lt;Code&gt;</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>&lt;ID1&gt;</i> , expected: <i>&lt;ID2&gt;</i>	A frame whose request ID number of the SNMP frame is <i>&lt;ID2&gt;</i> was expected, but an SNMP frame whose request ID number is <i>&lt;ID1&gt;</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.

### Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

### Example

*Figure 36-7: 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 36-10: 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 36-11: List of response messages for the snmp walk command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot translate variable class: <MIB Object Name>	The object name <MIB Object Name> is invalid.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
make_obj_id_from_dot, bad character : x,y,z	An object ID specified in dot notation contains invalid characters, such as x, y, and z.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
receive error.	A receive error occurred.
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 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.

### Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

### Example

*Figure 36-8: 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 36-12: 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)
		down (disabled)
		test (being tested)
InOctets	Indicates the number of octets received on an interface (ifInOctets).	--

Item	Meaning	Displayed information
OutOctets	Indicates the number of octets sent from an interface (ifOutOctets).	--
InPkts	Indicates the number of packets received on an interface (ifInUcastPkts+ifInNUcastPkts).	--
OutPkts	Indicates the number of packets sent from an interface (ifOutUcastPkts+ifOutNUcastPkts).	--

## Impact on communication

None

## Response messages

Table 36-13: List of response messages for the snmp getif command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
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

- 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.
- 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.

### Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

### Example

Figure 36-9: 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 36-14: 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)

Item	Meaning	Displayed information
		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 36-15: List of response messages for the snmp getroute command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
No routing information available.	There were no routing table entries.
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.

### Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

### Example

*Figure 36-10:* 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 36-16:* 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 36-17:* List of response messages for the snmp getarp command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.

Message	Description
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Error code set in packet - General error: <i>&lt;Number&gt;</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>&lt;Number&gt;</i> .
Error code set in packet - No such variable name. Index: <i>&lt;Number&gt;</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>&lt;Number&gt;</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>&lt;Code&gt;</i>	An SNMP frame containing response status code <i>&lt;Code&gt;</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>&lt;ID1&gt;</i> , expected: <i>&lt;ID2&gt;</i>	A frame whose request ID number of the SNMP frame is <i>&lt;ID2&gt;</i> was expected, but an SNMP frame whose request ID number is <i>&lt;ID1&gt;</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 (the 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.

### Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

### Example

Figure 36-11: Example of executing the snmp getforward command

```
> snmp getforward
Index  Destination      NextHop      Metric1 Type    Proto    Age  NH-AS
 2202  0.0.0.0/0         192.168.0.1      0 remote netmgmt  855  0
    0  127.0.0.0/8       0.0.0.0          0 other  local   974  0
    1  127.0.0.1/32      127.0.0.1        0 local  local   974  0
 2202  192.168.0.0/24    192.168.0.34     0 local  local   855  0
 2202  192.168.0.34/32   192.168.0.34     0 local  local   855  0

VRF 3
Index  Destination      NextHop      Metric1 Type    Proto    Age  NH-AS
 2210  10.10.10.0/24     10.10.10.1      0 local  local   855  0

VRF 4
Index  Destination      NextHop      Metric1 Type    Proto    Age  NH-AS
 2211  20.1.1.0/24       20.1.1.1        0 local  local   855  0
 2212  20.20.20.0/24     20.20.20.1      0 local  local   855  0
```

### Display items

Table 36-18: 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)

Item	Meaning	Displayed information
		other (others)
Proto	Indicates the protocol that learned this route (ipForwardProto).	rip (RIP)
		ospf (OSPF)
		bgp (BGP)
		local (static routing)
		netmgmt (static routing)
		other (others)
Age	Indicates the time (in seconds) elapsed since this route was learned or updated (ipForwardAge).	--
NH-AS	Indicates the autonomous system number of the next hop (ipForwardNextHopAS).	--

Table 36-19: Items displayed when the snmp getforward command is executed (by VRF) [OS-L3SA]

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)
		other (others)
Age	Indicates the time (in seconds) elapsed since this route was learned or updated (axsVrfIpFwAge).	--
NH-AS	Indicates the autonomous system number of the next hop (axsVrfIpFwNextHopAS).	--

## Impact on communication

None

## Response messages

Table 36-20: List of response messages for the snmp getforward command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
No forwarding information available.	There were no forwarding table entries.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
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.

### Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

### Example

*Figure 36-12:* Example of executing the snmp rget command

```
> snmp rget version 2 192.168.11.35 public sysObjectID.0
```

```
Name: sysObjectID.0
```

```
Value: ax3600s
```

### Display items

*Table 36-21:* 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 36-22: List of response messages for the snmp rget command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot translate variable class: <MIB Object Name>	The object name <MIB Object Name> is invalid.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
make_obj_id_from_dot, bad character : x,y,z	An object ID specified in dot notation contains invalid characters, such as x, y, and z.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
receive error.	A receive error occurred.
request ID mismatch. Got: <ID1>, expected: <ID2>	A frame whose request ID number of the SNMP frame is <ID2> was expected, but an SNMP frame whose request ID number is <ID1> was received.
unable to connect to socket.	An attempt to send an SNMP frame was made, but failed.

## Notes

None

---

## snmp rgetnext

---

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.

### Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

### Example

*Figure 36-13:* 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 36-23:* 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 36-24: List of response messages for the snmp rgetnext command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot translate variable class: <MIB Object Name>	The object name <MIB Object Name> is invalid.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
make_obj_id_from_dot, bad character : x,y,z	An object ID specified in dot notation contains invalid characters, such as x, y, and z.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
receive error.	A receive error occurred.
request ID mismatch. Got: <ID1>, expected: <ID2>	A frame whose request ID number of the SNMP frame is <ID2> was expected, but an SNMP frame whose request ID number is <ID1> was received. Alternatively, a timeout occurred 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.

### Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

### Example

*Figure 36-14:* 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 36-25:* 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 36-26: List of response messages for the snmp rwalk command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Cannot translate variable class: <MIB Object Name>	The object name <MIB Object Name> is invalid.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
make_obj_id_from_dot, bad character : x,y,z	An object ID specified in dot notation contains invalid characters, such as x, y, and z.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
receive error.	A receive error occurred.
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.

### Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

### Example

*Figure 36-15:* 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 36-27:* 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)

Item	Meaning	Displayed information
Proto	Indicates the routing protocol (ipRouteProto).	rip (RIP)
		ospf (OSPF)
		bgp (bgp)
		local (static routing)
		netmgmt (static routing)
		other (others)
Age	Indicates the number of seconds elapsed after this route was last updated or confirmed (ipRouteAge).	--

## Impact on communication

None

## Response messages

Table 36-28: List of response messages for the snmp rgetroute command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
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 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.

### Operation when a stack configuration is used

The command can acquire valid information only from the master switch.

### Example

*Figure 36-16: 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 36-29: 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 36-30: List of response messages for the snmp rgetarp command

Message	Description
<SNMP agent IP address>: host unknown.	An invalid SNMP agent address was specified.
Can't execute this command in backup switch or transit switch.	The command cannot be executed on a backup switch or a transit switch.
Error code set in packet - General error: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is being managed but the MIB value could not be acquired correctly was received. The object ID specified at the following position could not be acquired: <Number>.
Error code set in packet - No such variable name. Index: <Number>.	A response from the applicable SNMP agent indicating that the specified object ID is not managed was returned. The object ID specified at the following position is not managed: <Number>.
Error code set in packet - Return packet too big.	The response indicating that an attempt to return a MIB value exceeding the allowable size was made in the applicable SNMP agent was returned.
Error code set in packet - Unknown status code: <Code>	An SNMP frame containing response status code <Code>, which is undefined (non-standard), was received.
error parsing packet.	An SNMP frame in an invalid format was received.
error parsing pdu packet.	A frame that contains an SNMP PDU frame format error was received.
No ARP information available.	There were no ARP table entries.
No response - retrying	The command is being retried because there were no responses from the applicable SNMP agent.
No response - try again.	There were no responses from the applicable SNMP agent.
receive error.	A receive error occurred.
request ID mismatch. Got: <ID1>, expected: <ID2>	A frame whose request ID number of the SNMP frame is <ID2> was expected, but an SNMP frame whose request ID number is <ID1> was received. Alternatively, a timeout occurred 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

---

# 37. 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.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 37-1: Example of displaying the setting status and the operating status of sFlow statistics*

```
> show sflow
Date 20XX/01/26 20:04:01 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared: 8:00:05
sFlow agent data :
  sFlow service version : 4
  CounterSample interval rate: 60 seconds
  Default configured rate: 1 per 2048 packets
  Default actual rate : 1 per 2048 packets
  Configured sFlow ingress ports : 0/2-4
  Configured sFlow egress ports : ----
  Received sFlow samples : 37269 Dropped sFlow samples : 2093
  Exported sFlow samples : 37269 Couldn't export sFlow samples : 0
  Overflow time of sFlow queue : 0 seconds
sFlow collector data :
  Collector IP address: 192.168.4.199 UDP:6343 Source IP address: 130.130.130
.1
  Send FlowSample UDP packets : 12077 Send failed packets: 0
  Send CounterSample UDP packets: 621 Send failed packets: 0
  Collector IP address: 192.168.4.203 UDP:65535 Source IP address: 130.130.13
0.1
  Send FlowSample UDP packets : 12077 Send failed packets: 0
  Send CounterSample UDP packets: 621 Send failed packets: 0
```

*Figure 37-2: Example of displaying detailed information about the setting status and the operating status of sFlow statistics*

```
> show sflow detail
Date 20XX/01/26 20:04:01 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared: 8:00:05
sFlow agent data :
  sFlow service version : 4
  CounterSample interval rate: 60 seconds
  Default configured rate: 1 per 2048 packets
  Default actual rate : 1 per 2048 packets
  Configured sFlow ingress ports : 0/2-4
  Configured sFlow egress ports : ----
  Received sFlow samples : 37269 Dropped sFlow samples : 2093
```

```

Exported sFlow samples : 37269   Couldn't export sFlow samples :      0
Overflow time of sFlow queue : 0 seconds
sFlow collector data :
Collector IP address: 192.168.4.199  UDP:6343  Source IP address: 130.130.130
.1
  Send FlowSample UDP packets : 12077  Send failed packets:      0
  Send CounterSample UDP packets: 621  Send failed packets:      0
Collector IP address: 192.168.4.203  UDP:65535  Source IP address: 130.130.13
0.1
  Send FlowSample UDP packets : 12077  Send failed packets:      0
  Send CounterSample UDP packets: 621  Send failed packets:      0
Detail data :
Max packet size: 1400 bytes
Packet information type: header
Max header size: 128 bytes
Extended information type: switch,router,gateway,user,url
Url port number: 80,8080
Sampling mode: random-number
Sampling rate to collector: 1 per 2163 packets
Target ports for CounterSample: 0/2-4

```

## Display items

Table 37-1: 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. <i>hh:mm:ss</i> : (when the elapsed time is within 24 hours: <i>hh</i> = hours, <i>mm</i> = minutes, <i>ss</i> = seconds) <i>D</i> day: (when the elapsed time is over 24 hours: <i>D</i> = 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.)
Overflow time of sFlow queue	Length of time (in seconds) during which the sFlow statistics queue was full after the <code>clear sflow statistics</code> command was executed. If this value has increased, adjust the sampling interval.
Exported sFlow samples	Total number of sample packets contained in UDP packets sent to the collector
Couldn't export sFlow samples	Total number of sample packets contained in UDP packets that could not be sent

Item	Displayed information
Collector IP address	IP address of the collector set in the configuration
UDP	UDP port number
Source IP address	Address used as an agent IP when packets are sent to the collector
Send FlowSample UDP packets	Number of UDP packets for flow samples sent to the collector
Send failed packets	Number of UDP packets that could not be sent to the collector
Send CounterSample UDP packets	Number of UDP packets for counter samples sent to the collector
Max packet size	Maximum sFlow packet size
Packet information type	Basic data format for flow samples
Max header size	The maximum size of the sample packet when the header type is used as the basic data format
Extended information type	Extended data format for flow samples
Url port number	Port number used to determine if a packet is an HTTP packet when URL information is used for the extended data format
Sampling mode	Sampling method
random-number	Collection at a rate (random numbers) according to the sampling interval
Sampling rate to collector	Recommended sampling interval at which no packets are discarded. If there are problems at the current sampling interval, an applicable value is displayed. The value cannot be smaller than the value set in the configuration. If the sampling interval is changed, execute the clear sflow statistics command. The correct value might not be displayed until the command is executed.
Target ports for CounterSample	Target port for counter samples

## Impact on communication

None

## Response messages

Table 37-2: List of response messages for the show sflow command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
sflow doesn't seem to be running.	This command failed because the flow statistics program is not started. If this message appears when sFlow statistics are enabled, wait until the sFlow statistics program is restarted, and then re-execute the command.

## Notes

If the number of packets or the statistics counter exceeds the maximum value (32 bit counter), the value is reset to 0.

If no IP addresses or ports are set in the configuration, ---- is displayed.

---

## clear sflow statistics

---

Clears statistics managed by sFlow statistics.

### Syntax

```
clear sflow statistics
```

### Input mode

User mode and administrator mode

### Parameters

None

### Operation when a stack configuration is used

This command is not supported.

### Example

```
>clear sflow statistics
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 37-3: List of response messages for the clear sflow statistics command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
sflow doesn't seem to be running.	This command failed because the flow statistics program is not started. If this message appears when sFlow statistics are enabled, wait until the sFlow statistics program is restarted, and then re-execute the command.

### 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.

### Operation when a stack configuration is used

This command is not supported.

### Example

```
>restart sflow
sflow program restart OK? (y/n): y
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 37-4: 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

### Operation when a stack configuration is used

This command is not supported.

### Example

```
>dump sflow
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 37-5: List of response messages for the dump sflow command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
sflow doesn't seem to be running.	This command failed because the flow statistics program is not started. If this message appears when sFlow statistics are enabled, wait until the sFlow statistics program is restarted, and then re-execute the command.

### Notes

The storage directory and the name of the output dump file are as follows:

Storage directory: `/usr/var/flowd/`

File: `sflow.trc`

If a file with this name already exists, the file is overwritten unconditionally. Back up the file in advance, if necessary.

## Chapter

---

# 38. 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.

### Operation when a stack configuration is used

This command is not supported.

### Example 1

The following figure is an example of displaying the LLDP configuration information in a simplified format.

*Figure 38-1: Example of displaying the LLDP configuration information and neighboring device information in a simplified format*

```
> show lldp
Date 20XX/11/09 19:16:20 UTC
Status: Enabled Chassis ID: Type=MAC Info=0012.e268.2c21
Interval Time: 30 Hold Count: 4 TTL: 120
Port Counts=3
  0/1 (CH:10) Link: Up Neighbor Counts: 2
  0/2 Link: Down Neighbor Counts: 0
  0/3 Link: Down Neighbor Counts: 0
>
```

## Display items in Example 1

*Table 38-1:* Simplified display of LLDP setting 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)	5-32768
Hold Count	Multiplier for Interval Time, used for calculating the LDPDU retention time to be reported to neighboring devices	2-10
TTL	LDPDU retention time to be reported to neighboring devices	10-65535
Port Counts	Number of ports	Number of ports that has been set for enable-port
<nif no.>/<port no.>	Port number	NIF number/port number of the port whose information is to be displayed
CH	Channel group number	This item is displayed if the applicable port belongs to 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 38-2:* Example of displaying detailed LLDP configuration information and neighboring device information

```

> show lldp detail
Date 20XX/11/09 19:16:34 UTC
Status: Enabled Chassis ID: Type=MAC Info=0012.e268.2c21
Interval Time: 30 Hold Count: 4 TTL: 120
System Name: LLDP1
System Description: ALAXALA AX3650S AX-3650-48T4XW-A [AX3650S-48T4XW] Switching
software Ver. 11.6 [OS-L3SA]
Total Neighbor Counts=2
Port Counts=3
Port 0/1 (CH:10) Link: Up Neighbor Counts: 2
  Port ID: Type=MAC Info=0012.e298.5cc0
  Port Description: GigabitEther 0/1
  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 AX2430S AX-2430S-48T [AX2430S-48T] Switching
software Ver. 11.6 [OS-L2]

```

```

Port ID: Type=MAC          Info=0012.e298.dc20
Port Description: GigabitEthernet 0/5
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 AX3630S AX-3630S-24T2X [AX3630S-24T2X]
Switching software Ver. 11.6 [OS-L3L]
Port ID: Type=MAC          Info=0012.e298.7478
Port Description: GigabitEthernet 0/24
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 0/2          Link: Down Neighbor Counts: 0
Port 0/3          Link: Down Neighbor Counts: 0
>

```

1. Information about the Switch's port
2. Information about neighboring device
3. Information about neighboring device

## Display items in Example 2

*Table 38-2:* Detailed display of LLDP setting 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)	5-32768
Hold Count	Multiplier for Interval Time, used for calculating the LDPDU retention time to be reported to neighboring devices	2-10
TTL	LDPDU retention time to be reported to neighboring devices	10-65535
System Name	System name of the Switch	A character string set by using the name 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 (sysDescr)
Total Neighbor Counts	Total number of neighboring devices connected to the Switch	Number of neighboring devices whose information is retained by the Switch. 0-50
Port Counts	Number of ports	Number of ports that has been set for enable-port
Port	Applicable port number	<nif no.> / <port no.>

Item	Meaning	Displayed information
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
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). GigabitEther: Indicates a 1 Gbit/s or slower Ethernet. TenGigabitEther: Indicates a 10 Gbit/s Ethernet. FortyGigabitEther: Indicates a 40 Gbit/s Ethernet. [AX3800X]
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)	0-65535
Chassis ID	Chassis ID of the neighboring device	-

Item	Meaning	Displayed information
Type	Subtype for the chassis ID	<p>CHAS-COMP: Indicates that entPhysicalAlias of the Entity MIB is displayed for Info.</p> <p>CHAS-IF: Indicates that ifAlias of the interface MIB is displayed for Info.</p> <p>PORT: Indicates that portEntPhysicalAlias of the Entity MIB is displayed for Info.</p> <p>BACK-COMP: Indicates that backplaneEntPhysicalAlias of the Entity MIB is displayed for Info.</p> <p>MAC: Indicates that macAddress of the LLDP MIB is displayed for Info.</p> <p>NET: Indicates that networkAddress of the LLDP MIB is displayed for Info.</p> <p>LOCL: Indicates that local of the LLDP MIB is displayed for Info.</p>
Info	Information about the chassis ID	Information displayed for the subtype
System Name	System name of the neighboring device	This item is not displayed if it has not been reported.
System Description	System description of the neighboring device	This item is not displayed if it has not been reported.
Port ID	Port ID for the neighboring device	-
Type	Subtype for the port ID	<p>PORT: Indicates that ifAlias of the InterfaceMIB is displayed for Info.</p> <p>ENTRY: Indicates that portEntPhysicalAlias of the Entity MIB is displayed for Info.</p> <p>BACK-COMP: Indicates that backplaneEntPhysicalAlias of the Entity MIB is displayed for Info.</p> <p>MAC: Indicates that macAddr of the LLDP MIB is displayed for Info.</p> <p>NET: Indicates that networkAddr of the LLDP MIB is displayed for Info.</p> <p>LOCL: Indicates that local of the LLDP MIB is displayed for Info.</p>
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	<p>VLAN ID list</p> <p>This item is not displayed if it has not been reported.</p>
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.

Item	Meaning	Displayed information
<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 38-3: List of response messages for the show lldp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to LLDP program.	Communication with the LLDP program failed. Re-execute the command. If the failure occurs frequently, use the <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.

### Operation when a stack configuration is used

This command is not supported.

### Example

Figure 38-3: Example of displaying LLDP statistics

```
> show lldp statistics
Date 20XX/11/09 23:09:59 UTC
Port Counts: 3
Port 0/1   LDPDUs      : Tx   =      1300 Rx   =      1294 Invalid=      0
           Discard TLV: TLVs=      0 LDPDUs=      0
Port 0/2   LDPDUs      : Tx   =      890 Rx   =      547 Invalid=      0
           Discard TLV: TLVs=      0 LDPDUs=      0
Port 0/3   LDPDUs      : Tx   =      0 Rx   =      0 Invalid=      0
           Discard TLV: TLVs=      0 LDPDUs=      0
>
```

### Display items

Table 38-4: Items displayed for the 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	0-4294967295
Rx	Number of LDPDUs that have been received	0-4294967295
Invalid	Number of invalid LDPDUs	0-4294967295
Discard TLV	TLV statistics	0 is displayed for the disabled ports.
TLVs	Number of TLVs that have been discarded	0-4294967295

Item	Meaning	Displayed information
LDPDUs	Number of LDPDUs that contain discarded TLVs	0-4294967295

### Impact on communication

None

### Response messages

*Table 38-5:* List of response messages for the show lldp statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to LLDP program.	Communication with the LLDP program failed. Re-execute the command. If the failure occurs frequently, use the <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.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 38-4: Example of executing the clear lldp command*

```
> clear lldp
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 38-6: List of response messages for the clear lldp command*

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to LLDP program.	Communication with the LLDP program failed. Re-execute the command. If the failure occurs frequently, use the <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.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 38-5:* Example of executing the clear lldp statistics command

```
> clear lldp statistics
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 38-7:* List of response messages for the clear lldp statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to LLDP program.	Communication with the LLDP program failed. Re-execute the command. If the failure occurs frequently, use the <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.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 38-6: Example of restarting the LLDP program*

```
> restart lldp
LLDP restart OK? (y/n): y
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 38-8: 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

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 38-7: Example of specifying LLDP dump*

```
> dump protocols lldp
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 38-9: 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

---

# 39. 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.

### Operation when a stack configuration is used

This command is not supported.

### Example 1

The following figure is an example of displaying OADP/CDP configuration information in a simplified format.

*Figure 39-1: Example of displaying OADP configuration information and neighboring device information in a simplified format*

```
> show oadp
Date 20XX/11/09 19:50:20 UTC
OADP/CDP status: Enabled/Disabled   Device ID: OADP-1
Interval Time: 60   Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 0/1-5,16,20
                CH 10

Total Neighbor Counts=2
Local   VID Holdtime Remote   VID Device ID           Capability Platform
0/1     0           35 0/8     0 OADP-2                 RS      AX3630S-24T2X
0/16    0           9 0/1     0 OADP-3                 S       AX2430S-48T

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
>

> show oadp port 0/1
Date 20XX/11/09 19:50:30 UTC
OADP/CDP status: Enabled/Disabled   Device ID: OADP-1
Interval Time: 60   Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 0/1-5,16,20
                CH 10

Total Neighbor Counts=1
Local   VID Holdtime Remote   VID Device ID           Capability Platform
0/1     0           35 0/8     0 OADP-2                 RS      AX3630S-24T2X

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
>

> show oadp device-id OADP-3
Date 20XX/11/09 19:50:40 UTC
OADP/CDP status: Enabled/Disabled   Device ID: OADP-1
Interval Time: 60   Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 0/1-5,16,20
                CH 10

Total Neighbor Counts=1
Local   VID Holdtime Remote   VID Device ID           Capability Platform
0/16    0           9 0/1     0 OADP-3                 S       AX2430S-48T

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
>
```

## Display items in Example 1

*Table 39-1: 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.

Item	Meaning	Displayed information
Interval Time	Interval for sending OADP frames that has been set on the Switch (in seconds)	5-254
Hold Time	OADP frame retention time to be reported to neighboring devices (in seconds)	10-255
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.	0-100
Local	Received port number	<NIF number>/<port number>, <channel group number>
VID	VLAN ID of the IEEE 802.1Q VLAN Tag attached to the receive frame	VLAN ID
Holdtime	Remaining retention time for neighboring device information (in seconds)	OADP: 0 to 255 CDP: Time set for a Cisco 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 39-2: Example of displaying detailed OADP configuration information and neighboring device information*

```

> show oadp detail
Date 20XX/11/09 19:55:52 UTC
OADP/CDP status: Enabled/Disabled   Device ID: OADP-1
Interval Time: 60   Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 0/1-5,16,20
Total Neighbor Counts=2
-----
Port: 0/1      VLAN ID: 0
Holdtime      : 6(sec)
Port ID       : 0/8   VLAN ID(TLV): 0
Device ID     : OADP-2

```

1  
2  
2

```

Capabilities : Router,Switch
Platform    : AX3630S-24T2X
Entry address(es):
  IP address : 192.16.170.87
  IPv6 address: fe80::200:4cff:fe71:5d1c
IfSpeed     : 1G Duplex : FULL
Version     : ALAXALA AX3630S AX-3630S-24T2X [AX3630S-24T2X]
Switching software Ver. 11.6 [OS-L3L]
-----
Port: 0/16      VLAN ID: 0
Holdtime       : 10(sec)
Port ID        : 0/1  VLAN ID(TLV): 0
Device ID      : OADP-3
Capabilities   : Switch
Platform       : AX2430S-48T
Entry address(es):
  IP address   : 192.16.170.100
IfSpeed        : 1G Duplex : FULL
Version        : ALAXALA AX2430S AX-2430S-48T [AX2430S-48T] Switching software Ver. 11.6 [OS-L2]
-----
>

```

1. Configuration information of the Switch
2. Information about the Switch's port
3. Information about neighboring devices

## Display items in Example 2

Table 39-2: 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)	5-254
Hold Time	OADP frame retention time to be reported to neighboring devices (in seconds)	10-255
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.	0-100
Port	Received port number	<NIF number>/<port number>, <channel group number>
VLAN ID	VLAN ID of the IEEE 802.1Q VLAN Tag attached to the receive frame	VLAN ID

Item	Meaning	Displayed information
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>
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: 10 Mbit/s, 1G: 1 Gbit/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 39-3: List of response messages for the show oadp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to OADP.	Communication with the OADP program failed. Re-execute the command. If the failure occurs frequently, use the <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.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 39-3: Example of displaying OADP/CDP statistics*

```
> show oadp statistics
Date 20XX/11/09 23:12:23 UTC
Port Counts: 3
Port 0/6   OADP PDUs   : Tx   =          9 OADP/CDP PDUs   : Rx   =          14
           RX PDUs    : OADP=    6 CDPv1 =          0 CDPv2 =          8
           Discard/ERR: Head=    0 cksum =          0 capacity=    0
Port 0/7   OADP PDUs   : Tx   =         10 OADP/CDP PDUs   : Rx   =          18
           RX PDUs    : OADP=    9 CDPv1 =          0 CDPv2 =          9
           Discard/ERR: Head=    0 cksum =          0 capacity=    0
Port 0/8   OADP PDUs   : Tx   =          0 OADP/CDP PDUs   : Rx   =          0
           RX PDUs    : OADP=    0 CDPv1 =          0 CDPv2 =          0
           Discard/ERR: Head=    0 cksum =          0 capacity=    0
>
```

### Display items

*Table 39-4: Items displayed for OADP/CDP statistics*

Item	Meaning	Displayed information
Port counts	Number of ports subject to this statistics	--

Item	Meaning	Displayed information
Port	Port number	NIF number/ port number of the port whose information is to be displayed
OADP PDUs Tx	Number of sent OADP PDUs	0-4294967295
OADP/CDP PDUs Rx	Number of received OADP/CDP PDUs	0-4294967295
Rx PDUs	Statistics for receive frames	--
OADP	Number of OADP PDUs	0-4294967295
CDPv1	Number of CDP version 1 PDUs	0-4294967295
CDPv2	Number of CDP version 2 PDUs	0-4294967295
Discard/ERR	Statistics for error frames	--
Head	Number of header error PDUs	0-4294967295
cksum	Number of checksum error PDUs	0-4294967295
capacity	Number of PDUs exceeding the accommodation limit	0-4294967295

## Impact on communication

None

## Response messages

*Table 39-5:* List of response messages for the show oadp statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
Connection failed to OADP.	Communication with the OADP program failed. Re-execute the command. If the failure occurs frequently, use the <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.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 39-4:* Example of executing the clear oadp command

```
> clear oadp
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 39-6:* List of response messages for the clear oadp command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
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 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.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 39-5:* Example of executing the clear oadp statistics command

```
> clear oadp statistics
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 39-7:* List of response messages for the clear oadp statistics command

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.

Message	Description
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

---

## 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.

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 39-6:* Example of restarting the OADP program

```
> restart oadp
OADP restart OK? (y/n): y
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 39-8:* 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

### Operation when a stack configuration is used

This command is not supported.

### Example

*Figure 39-7: Example of specifying OADP dump*

```
> dump protocols oadp
>
```

### Display items

None

### Impact on communication

None

### Response messages

*Table 39-9: 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.



---

# Appendix

---

A. List of operation commands supported by the `remote command` command

## A. List of operation commands supported by the remote command command

When a stack configuration is used, you can execute the `remote command` command to execute an operation command for a member switch that was specified from the master switch. The following table lists the operation commands supported by the `remote command` command.

*Table A-1: Operation commands supported by the remote command command*

Chapter	Operation command
Terminals and Remote Operations	set exec-timeout, set terminal help, set terminal pager
Configurations and File Operations	ls, dir, cat, cp, mkdir, mv, rm, rmdir, delete, undelete, squeeze
Stack	show switch, dump stack
Login Security and RADIUS or TACACS+	show sessions (who), killuser
Time Settings and NTP	show clock, restart ntp
Utilities	diff, grep, tail, hexdump
Checking Software Versions and Device Statuses	show version, show system, clear control-counter, show environment, reload, show tech-support, backup, restore
Power Saving Functionality	show power, clear power
Checking Internal Memory and Memory Cards	show mc, format mc, show flash
Log	show logging, clear logging, show logging console, set logging console
Software Management	ppupdate, set license, show license, erase license
Resource Information	show cpu, show processes, show memory, df, du
Dump Information	erase dumpfile, show dumpfile
Ethernet	show interfaces, clear counters, show port, activate, inactivate
Link Aggregation	show channel-group statistics, restart link-aggregation, dump protocols link-aggregation
MAC Address Table	show mac-address-table
VLANs	restart vlan, dump protocols vlan
Spanning Tree Protocol	restart spanning-tree, dump protocols spanning-tree
Filters	show access-filter, clear access-filter
QoS	show qos-flow, clear qos-flow, show qos queueing, clear qos queueing
GSRP	restart gsrp, dump protocols gsrp
Uplink Redundancy	restart uplink-redundant, dump protocols uplink-redundant
IEEE 802.3ah/UDLD	restart efmoam, dump protocols efmoam
L2 Loop Detection	restart loop-detection, dump protocols loop-detection
IPv4, ARP, and ICMP	show netstat(netstat), clear netstat, clear tcp
IPv4 Multicast Routing Protocols	restart ipv4-multicast, dump protocols ipv4-multicast, erase protocol-dump ipv4-multicast

Chapter	Operation command
Routing Protocol Common to IPv4 and IPv6	restart unicast, debug protocols unicast, no debug protocols unicast, dump protocols unicast, erase protocol-dump unicast
IPv6, NDP, and ICMPv6	show netstat(netstat), clear netstat, clear tcp



---

# Index

---

## A

activate 303  
adduser 88

## B

backup 173

## C

cat 56  
cd 49  
clear access-filter 459  
clear accounting 108  
clear axrp 423  
clear axrp preempt-delay 425  
clear cfm fault 813  
clear cfm l2traceroute-db 815  
clear cfm remote-mep 811  
clear cfm statistics 816  
clear channel-group statistics lacp 335  
clear control-counter 147  
clear counters 283  
clear dot1x auth-state 497  
clear dot1x logging 516  
clear dot1x statistics 495  
clear efmoam statistics 760  
clear fense logging 637  
clear fense statistics 635  
clear gsrp 686  
clear gsrp forced-shift 693  
clear gsrp port-up-delay 691  
clear igmp-snooping 438  
clear ip arp inspection statistics 652  
clear ip dhcp snooping binding 645  
clear ip dhcp snooping logging 666  
clear ip dhcp snooping statistics 649  
clear lldp 876  
clear lldp statistics 877  
clear logging 200  
clear loop-detection logging 776  
clear loop-detection statistics 774  
clear mac-address-table 346  
clear mac-authentication auth-state 598  
clear mac-authentication dead-interval-timer 617  
clear mac-authentication logging 600  
clear mac-authentication statistics 601  
clear mld-snooping 446  
clear oadp 889  
clear oadp statistics 891  
clear password 95  
clear power 184

clear qos queueing 476  
clear qos-flow 466  
clear sflow statistics 863  
clear spanning-tree detected-protocol 406  
clear spanning-tree statistics 404  
clear switchport-backup statistics 750  
clear vrrpstatus (IPv4) 710  
clear vrrpstatus (IPv6) 724  
clear web-authentication auth-state 562  
clear web-authentication dead-interval-timer 573  
clear web-authentication html-files 570  
clear web-authentication logging 554  
clear web-authentication statistics 555  
command description format 2  
commit mac-authentication 606  
commit web-authentication 556  
configure (configure terminal) 15  
copy 42  
cp 57

## D

delete 68  
df 220  
diff 122  
dir 53  
disable 11  
du 221  
dump protocols accounting 111  
dump protocols axrp 429  
dump protocols cfm 820  
dump protocols dhcp snooping 669  
dump protocols dot1x 504  
dump protocols efmoam 763  
dump protocols gsrp 697  
dump protocols link-aggregation 339  
dump protocols lldp 880  
dump protocols loop-detection 779  
dump protocols mac-authentication 616  
dump protocols oadp 895  
dump protocols snooping 450  
dump protocols spanning-tree 413  
dump protocols uplink-redundant 747  
dump protocols vaa 640  
dump protocols vlan 368  
dump protocols web-authentication 566  
dump sflow 866  
dump stack 85

## E

enable 10

erase configuration 45  
erase dumpfile 224  
erase license 210  
exit 13

## F

format mc 192  
ftp 28

## G

grep 124

## H

hexdump 128

## I

inactivate 305

## K

killuser 102

## L

l2ping 782  
l2traceroute 785  
less 126  
load mac-authentication 612  
load web-authentication 560  
logout 14  
ls 51

## M

mkdir 60  
more 125  
mv 62

## N

no test interfaces 311

## O

operation commands supported by remote command 898

## P

password 93  
ppupdate 204  
pwd 50

## Q

quit 12

## R

reauthenticate dot1x 500  
reload 154

remote command 78  
remove mac-authentication mac-address 604  
remove web-authentication user 524  
restart accounting 109  
restart axrp 427  
restart cfm 818  
restart dhcp snooping 667  
restart dot1x 502  
restart efmoam 761  
restart gsrp 695  
restart link-aggregation 337  
restart lldp 878  
restart loop-detection 777  
restart mac-authentication 614  
restart ntp 120  
restart oadp 893  
restart sflow 864  
restart snooping 448  
restart spanning-tree 411  
restart uplink-redundant 745  
restart vaa 638  
restart vlan 366  
restart web-authentication 564  
restore 176  
rm 64  
rmdir 66  
rmuser 91

## S

set clock 115  
set exec-timeout 18  
set gsrp master 689  
set license 207  
set logging console 202  
set mac-authentication mac-address 602  
set power-control schedule 185  
set switch 84  
set switchport-backup active 743  
set terminal help 20  
set terminal pager 22  
set web-authentication html-files 567  
set web-authentication passwd 520  
set web-authentication user 518  
set web-authentication vlan 522  
show access-filter 454  
show accounting 104  
show axrp 416  
show cfm 788  
show cfm fault 799  
show cfm l2traceroute-db 802  
show cfm remote-mep 793  
show cfm statistics 807  
show channel-group 316  
show channel-group statistics 327  
show clock 114  
show cpu 212

- show dot1x 485
  - show dot1x logging 506
  - show dot1x statistics 480
  - show dumpfile 225
  - show efmoam 754
  - show efmoam statistics 757
  - show environment 148
  - show fense logging 632
  - show fense server 620
  - show fense statistics 625
  - show file 46
  - show flash 194
  - show gsrp 672
  - show gsrp aware 684
  - show history 24
  - show igmp-snooping 432
  - show interfaces (1000BASE-X) 251
  - show interfaces (100BASE-FX) 243
  - show interfaces (10BASE-T/100BASE-TX/1000BASE-T) 228
  - show interfaces (10GBASE-R) 267
  - show interfaces (40GBASE-R) 275
  - show ip arp inspection statistics 650
  - show ip dhcp snooping binding 642
  - show ip dhcp snooping logging 653
  - show ip dhcp snooping statistics 647
  - show license 209
  - show lldp 868
  - show lldp statistics 874
  - show logging 198
  - show logging console 201
  - show loop-detection 766
  - show loop-detection logging 772
  - show loop-detection statistics 769
  - show mac-address-table 342
  - show mac-authentication 591
  - show mac-authentication logging 578
  - show mac-authentication login 576
  - show mac-authentication mac-address 608
  - show mac-authentication statistics 595
  - show mc 190
  - show memory 218
  - show mld-snooping 440
  - show ntp associations 117
  - show oadp 882
  - show oadp statistics 887
  - show port 285
  - show power 182
  - show power-control port 186
  - show power-control schedule 180
  - show processes 215
  - show qos queueing 468
  - show qos-flow 462
  - show running-config (show configuration) 40
  - show sessions (who) 97
  - show sflow 860
  - show snmp 822
  - show snmp pending 827
  - show spanning-tree 370
  - show spanning-tree port-count 408
  - show spanning-tree statistics 397
  - show startup-config 41
  - show switch 81
  - show switchport-backup 738
  - show switchport-backup statistics 748
  - show system 134
  - show tcpdump (tcpdump) 161
  - show tech-support 156
  - show track (IPv4) 729
  - show track (IPv6) 733
  - show version 130
  - show vlan 350
  - show vlan mac-vlan 363
  - show vrrpstatus (IPv4) 700
  - show vrrpstatus (IPv6) 715
  - show web-authentication 546
  - show web-authentication html-files 571
  - show web-authentication logging 530
  - show web-authentication login 528
  - show web-authentication statistics 551
  - show web-authentication user 526
  - show whoami (who am i) 99
  - snmp get 830
  - snmp getarp 842
  - snmp getforward 844
  - snmp getif 836
  - snmp getnext 832
  - snmp getroute 839
  - snmp lookup 829
  - snmp rget 847
  - snmp rgetarp 856
  - snmp rgetnext 849
  - snmp rgetroute 853
  - snmp rwalk 851
  - snmp walk 834
  - squeeze 72
  - store mac-authentication 610
  - store web-authentication 558
  - supported operation commands
    - remote command 898
  - swap vrrp (IPv4) 712
  - swap vrrp (IPv6) 726
- T**
- tail 127
  - telnet 25
  - test interfaces 307
  - tftp 34
- U**
- undelete 70

**Z**

zmodem 74