AX6700S/AX6600S/AX6300S Software Manual

Configuration Command Reference Vol. 1

For Version 11.7

AX63S-S004X-C0

AlaxalA

■ Relevant products

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

■ Export restrictions

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

■ Trademarks

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

Ethernet is a registered trademark of Xerox Corporation.

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

IPX is a trademark of Novell, Inc.

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

Octpower is a registered trademark of NEC Corporation.

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

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

VitalQIP and VitalQIP Registration Manager are trademarks of Lucent Technologies.

VLANaccessClient is a trademark of NEC Soft, Ltd.

VLANaccessController and VLANaccessAgent are trademarks of NEC Corporation.

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

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

■ Reading and storing this manual

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

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

■ Notes

Information in this document is subject to change without notice.

■ Editions history

January 2012 (Edition 13) AX63S-S004X-C0

■ Copyright

History of Amendments

[For version 11.7]

Summary of amendments

Location and title	Changes
2 Connecting from an Operation Terminal	• A parameter was added to the following commands: ftp-server transport input
18 Policy-based Switching	• This chapter was added.
21 Error Messages Displayed When Editing the Configuration	• The subsection *Policy-based switching information* was added.

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

[For version 11.5]

Summary of amendments

Item	Changes
Login Security and RADIUS or TACACS+	• The following commands were added: aaa authentication enable attribute-user-per-method aaa authentication enable end-by-reject aaa authentication login end-by-reject
Time Settings and NTP	• Notes were added to the `ntp access-group` command.
Device Management	• The following commands were added: system fan mode system temperature-warning-level
Ring Protocol	• The `flush-request-transmit vlan` command was added.

[For version 11.4]

Summary of amendments

Item	Changes
Connecting from an Operation Terminal	• A parameter related to VRF was added to the following commands: ftp-server transport input
Login Security and RADIUS or TACACS+	• A parameter related to VRF was added to the following commands: ip access-group ipv6 access-class
Power Saving Functionality	• The following commands were added: adaptive-power-control decrease-traffic-debounce adaptive-power-control enable adaptive-power-control increase-traffic-debounce adaptive-power-control max-bsu adaptive-power-control max-psp adaptive-power-control mode adaptive-power-control port-led adaptive-power-control standby-bsu adaptive-power-control standby-psp schedule-power-control redundancy nif-group max-standby-nif

[For version 11.3]

The chapter Flow Mode and all subsequent chapters were moved to *Configuration Command Reference Vol. 2 For Version 11.7*.

[For version 11.2]

Summary of amendments

Item	Changes
Login Security and RADIUS or TACACS+	• The following commands were added: aaa authentication enable aaa authentication login console aaa authorization commands console
Time Settings and NTP	• A parameter related to VRF was added to the following commands: ntp access-group ntp peer ntp server
Device Management	• A parameter was added to the `fldm prefer` command.
Ring Protocol	• The `preempt-delay` command was added.
Flow Mode	• The note on the `flow mac mode` command was changed.
Access Lists	• The following commands were added: advance access-group advance access-list advance access-list resequence deny (advance access-list) permit (advance access-list) • The descriptions of the functions of the following commands were changed: access-list ip access-group ip access-list extended ip access-list standard ipv6 access-list ipv6 traffic-filter mac access-group mac access-list extended remark • The notes on the following commands were changed: ip access-group ipv6 traffic-filter mac access-group

Item	Changes
QoS	• The following commands were added: advance qos-flow-group advance qos-flow-list advance qos-flow-list resequence qos (advance qos-flow-list) • The descriptions of the functions of the following commands were changed: ip qos-flow-group ipv6 qos-flow-group mac qos-flow-group remark • The notes on the following commands were changed: ip qos-flow-group ip qos-flow-list ipv6 qos-flow-group ipv6 qos-flow-list mac qos-flow-group mac qos-flow-list
VRRP	• The <*interface type*> and <*interface number*> parameters were added to the `track interface` command. • The `msec` parameter was added to the `vrrp timers advertise` command.
CFM	• The following commands were added: ethernet cfm cc alarm-priority ethernet cfm cc alarm-reset-time ethernet cfm cc alarm-start-time ethernet cfm cc interval
Log Data Output Functionality	• A parameter related to VRF and the `no-date-info` parameter were added to the `logging host` command.

[For version 11.1]

Summary of amendments

Item	Changes
Power Saving Functionality	• This chapter was added.
IEEE 802.1X	• The `dot1x logging enable` command was added.
Redundancy of BSUs	• The `cold2` parameter was added to the `redundancy standby-bsu` command.
Redundancy of PSPs	• This chapter was added.
CFM	• This chapter was added.
SNMP	• The `power-control` parameter was added to the `snmp-server host` command.
Error Messages Displayed When Editing the Configuration	• The subsection *Information about the power saving functionality* was added. • The subsection *CFM information* was added.

[For version 11.0]

Summary of amendments

Item	Changes
Ethernet	• The notes on the following commands were changed: duplex mdix auto mtu speed system mtu • The `media-type` command was added.
Ring Protocol	• The note on the `axrp vlan-mapping` command was changed.
IGMP Snooping	• The `ip igmp snooping fast-leave` command was added.
uRPF	• The descriptions on Impact on communication of the following commands were changed: ip verify unicast source reachable-via ipv6 verify unicast source reachable-via
QoS	• A parameter that specifies an operation of the hierarchical shaper function was added to the following commands: qos (ip qos-flow-list) qos (ipv6 qos-flow-list) qos (mac qos-flow-list) • Notes were added to the following commands: qos-queue-group traffic-shape rate • The following commands were added: llrlq1-burst llrlq2-burst mode number-of-queue predicted-tail-drop set-default-user-priority shaper auto-configuration shaper default-user shaper llrlq1 shaper llrlq2 shaper nif shaper port buffer shaper port rate-limit shaper user shaper user-list shaper vlan-user-map shaper wgq-group rate-limit
GSRP	• The note on the `gsrp` command was changed. • The `gsrp limit-control` command was added. • A parameter was added to the `no-neighbor-to-master` command.
VRRP	• The following commands were added: vrrp follow vrrp ietf-unified-spec-02-mode vrrp name vrrp-vlan
SNMP	• A parameter related to VRF was added to the following commands: snmp-server community snmp-server host snmp-server user
Port Mirroring	• Notes on the `monitor session` command were added.

Item	Changes
Error Messages Displayed When Editing the Configuration	• An error message related to the hierarchical shaper was added to the subsection *QoS information*. • An error message was added to the subsection *Port mirroring information*.

[For version 10.7]

Summary of amendments

Item	Changes
Login Security and RADIUS or TACACS+	• A description of how to specify an IPv6 address was added to the `radius-server host` command.
BSU/NIF Management	• The following commands were added: system nif-hdc restart system nif-hdc software-bundle
Ethernet	• The following commands were added: link up-debounce mdix auto
VLAN	• The following commands were added: down-debounce up-debounce
Spanning Tree Protocols	• The notes on the following commands were changed: instance spanning-tree mode
Ring Protocol	• The notes on the following commands were changed: axrp axrp virtual-link axrp vlan-mapping axrp-primary-port axrp-ring-port
MAC-based Authentication	• A description of how to specify an IPv6 address was added to the `mac-authentication radius-server host` command.
GSRP	• The notes on the following commands were changed: gsrp gsrp no-flush-port gsrp reset-flush-port
L2 Loop Detection	• This chapter was added.
SNMP	• The `loop-detection` parameter was added to the `snmp-server host` command.

[For version 10.6]

Summary of amendments

Item	Changes
VLAN	• The `l2-isolation` command was added.
Ring Protocol	• The `axrp virtual-link` command was added.

Item	Changes
Web Authentication	• The following commands were added: web-authentication ip address web-authentication jump-url web-authentication logging enable web-authentication logout ping tos-windows web-authentication logout ping ttl web-authentication logout polling count web-authentication logout polling enable web-authentication logout polling interval web-authentication logout polling retry-interval web-authentication port web-authentication static-vlan max-user web-authentication web-port
MAC-based Authentication	• This chapter was added.
Configuring Basic Switching Units for Redundancy	• The following commands were added: redundancy bsu-load-balancing redundancy bsu-mode
Log Data Output Functionality	• The descriptions of the following commands were changed: logging email-event-kind logging event-kind
Error Messages Displayed When Editing the Configuration	• The subsection *MAC-based authentication information* was added. • The subsection *redundancy information* was added.

[For version 10.5]

Summary of amendments

Item	Changes
Spanning Tree Protocols	• Notes on supporting the STP compatibility mode were added to the `spanning-tree link-type` command.
Log Data Output Functionality	• The `logging syslog-dump` command was added.

[For version 10.4]

Summary of amendments

Item	Changes
Ring Protocol	• This chapter was added.
Authentication VLAN	• The `fense vaa-sync` command was added.
Error Messages Displayed When Editing the Configuration	• The subsection *Ring Protocol information* was added.

[For version 10.3]

Summary of amendments

Item	Changes
Dial-up IP Connection	• This chapter was added.
Login Security and RADIUS or TACACS+	• `local` was added to the <*method*> parameter of the `aaa authorization commands` command. • The `commands exec`, `parser view`, and `username` commands were added.

Item	Changes
Device Management	• The `fldm prefer` command was added. • The `system recovery` command was added.
BSU/NIF Management	• The `bsu` parameter was added to the `power enable` command.
MAC Address Table	• The description of the `mac-address-table static` command was changed.
IGMP Snooping	• This chapter was added.
MLD Snooping	• This chapter was added.
VLAN Lists	• This chapter was added.
Access Lists	• The range specification function was added. • `slow-protocol` was added as a destination MAC address name that can be specified.
uRPF	• This chapter was added.
QoS	• The range specification function was added. • `slow-protocol` was added as a destination MAC address name that can be specified. • The bandwidth monitoring functionality was added. • The `qos-queue-group` command was added. • The `qos-queue-list` command was added. • The `traffic-shape rate` command was added.
Web Authentication	• This chapter was added.
Configuring Basic Switching Units for Redundancy	• This chapter was added.
Storm Control	• This chapter was added.
IEEE 802.3ah/UDLD	• This chapter was added.
sFlow Statistics	• This chapter was added.
Port Mirroring	• This chapter was added.
Error Messages Displayed When Editing the Configuration	• The subsection *Switch management information* was added. • The subsection *IGMP snooping information* was added. • The subsection *MLD snooping information* was added. • The subsection *Web authentication information* was added. • The subsection *Storm control information* was added. • The subsection *sFlow statistics* was added. • The subsection *Port mirroring information* was added.

Preface

Applicable products and software versions

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

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

Unless otherwise noted, this manual describes functionality applicable to AX6700S, AX6600S, and AX6300S series switches. Functionality specific to a model is indicated as follows:

[AX6700S]:

The description applies to the AX6700S series.

[AX6600S]:

The description applies to the AX6600S series.

[AX6300S]:

The description applies to the AX6300S series.

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

[OP-BGP]:

The description applies to the OP-BGP optional license.

[OP-DH6R]:

The description applies to the OP-DH6R optional license.

[OP-MBSE]:

The description applies to the OP-MBSE optional license.

[OP-NPAR]:

The description applies to the OP-NPAR optional license.

[OP-VAA]:

The description applies to the OP-VAA optional license.

Corrections to the manual

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

Intended readers

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

Readers must have an understanding of the following:

- The basics of network system management

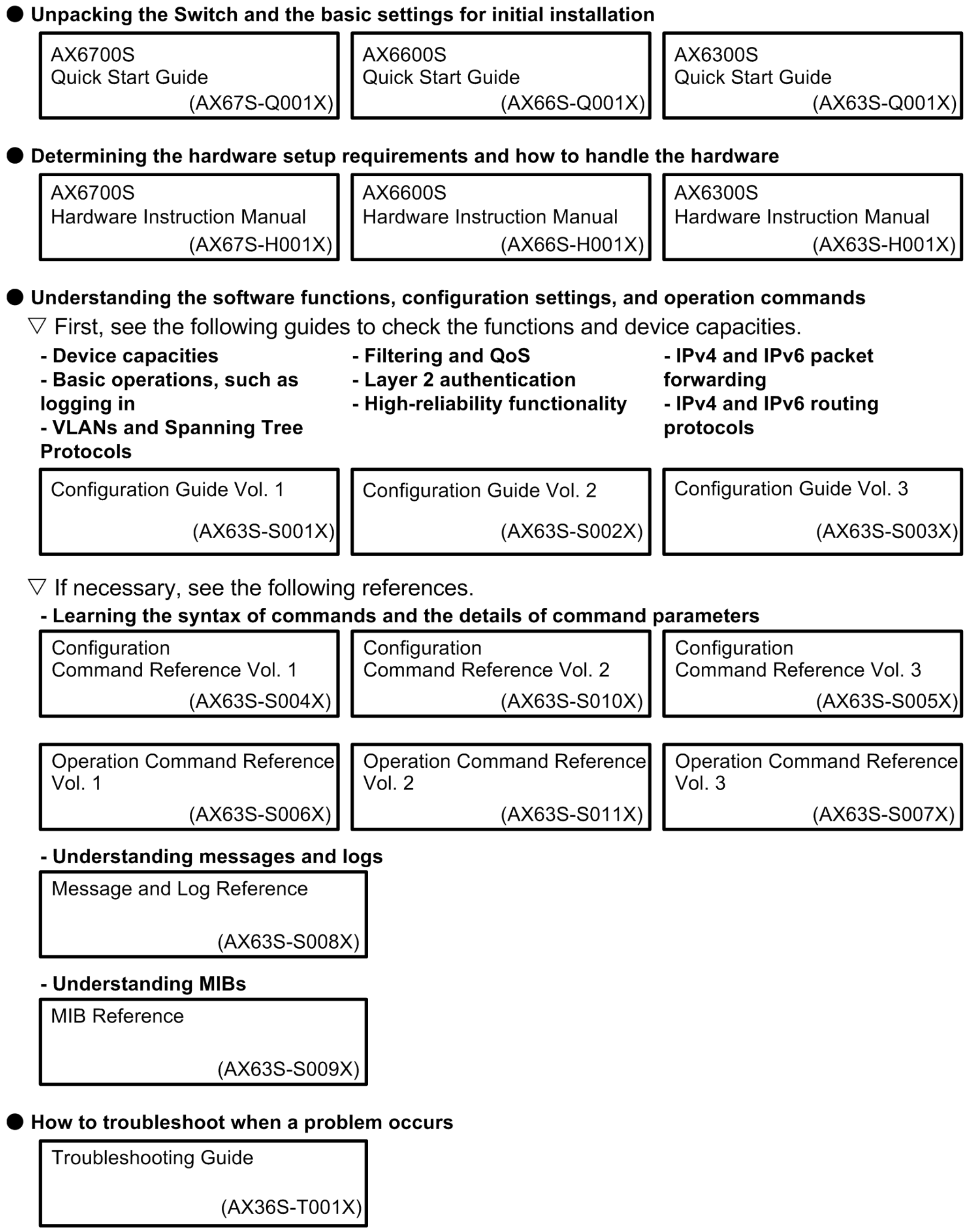
Manual URL

You can view this manual on our website at:

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

Reading sequence of the manuals

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



● **Unpacking the Switch and the basic settings for initial installation**

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

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

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

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

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

- Device capacities **- Basic operations, such as logging in** **- VLANs and Spanning Tree Protocols**	**- Filtering and QoS** **- Layer 2 authentication** **- High-reliability functionality**	**- IPv4 and IPv6 packet forwarding** **- IPv4 and IPv6 routing protocols**
Configuration Guide Vol. 1 (AX63S-S001X)	Configuration Guide Vol. 2 (AX63S-S002X)	Configuration Guide Vol. 3 (AX63S-S003X)

▽ If necessary, see the following references.

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

Configuration Command Reference Vol. 1 (AX63S-S004X)	Configuration Command Reference Vol. 2 (AX63S-S010X)	Configuration Command Reference Vol. 3 (AX63S-S005X)
Operation Command Reference Vol. 1 (AX63S-S006X)	Operation Command Reference Vol. 2 (AX63S-S011X)	Operation Command Reference Vol. 3 (AX63S-S007X)

- Understanding messages and logs

Message and Log Reference
(AX63S-S008X)

- Understanding MIBs

MIB Reference
(AX63S-S009X)

● **How to troubleshoot when a problem occurs**

Troubleshooting Guide
(AX36S-T001X)

Conventions: The terms "Switch" and "switch"

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

AX6700S series switch

AX6600S series switch

AX6300S series switch

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

Abbreviations used in the manual

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BCU	Basic Control Unit
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second (can also appear as bps)
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
BSU	Basic Switching Unit
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
CSU	Control and Switching Unit
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission

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

PS	Power Supply
PSNP	Partial Sequence Numbers PDU
PSP	Packet Switching Processor
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RGQ	Rate Guaranteed Queueing
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SOP	System Operational Panel
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
uRPF	unicast Reverse Path Forwarding
VAA	VLAN Access Agent
VLAN	Virtual LAN
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WGQ	Weighted Guaranteed Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

Conventions: KB, MB, GB, and TB

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

Contents

PART 3: Network Interfaces

PART 4: Layer 2 Switching

PART 5: Configuration Error Messages

Chapter

1. Reading the Manual

Command description format
Command mode list
Specifiable values for parameters

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. The name of a sub-mode of a configuration command mode corresponds to the name displayed on the command prompt.

Parameters

Describes in detail the parameters that can be set by the command. The default value and the values that can be specified for each parameter are described.

Default behavior

If there are default values for parameters, or a default behavior when a command is not entered, related information is provided here.

Impact on communication

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

When the change is applied

Describes whether changes to values for configuration information in memory are immediately effective, or whether they take effect only after temporarily stopping operation, such as by restarting the switch.

Notes

Provides cautionary information on using the command.

Related commands

Describes the commands that must be set in order to use the applicable command.

Command mode list

The following table lists the command modes.

Table 1-1: Command mode list

#	Prompt displayed for the command mode	Description	Command for mode transition
1	(config)	Global configuration mode	# enable # configure
2	(config-line)	Configures remote login and console.	(config)# line vty (config)# line console
3	(config-if)	Configures an interface.	(config)# interface
4	(config-if-range)	Configures multiple interfaces.	(config)# interface range
5	(config-vlan)	Configures VLAN.	(config)# vlan
6	(config-mst)	Configures Multiple Spanning Tree	(config)# spanning-tree mst configuration
7	(config-axrp)	Configures the Ring Protocol.	(config)# axrp
8	(config-gsrp)	Configures GSRP.	(config)# gsrp
9	(config-adv-acl)	Configures an Advance filter.	(config)# advance access-list
10	(config-ext-nacl)	Configures an IPv4 packet filter.	(config)# ip access-list extended
11	(config-std-nacl)	Configures an IPv4 address filter.	(config)# ip access-list standard
12	(config-ipv6-acl)	Configures an IPv6 filter.	(config)# ipv6 access-list
13	(config-ext-macl)	Configures a MAC filter.	(config)# mac access-list extended
14	(config-adv-qos)	Configures Advance QoS.	(config)# advance qos-flow-list
15	(config-ip-qos)	Configures IPv4 QoS.	(config)# ip qos-flow-list
16	(config-ipv6-qos)	Configures IPv6 QoS.	(config)# ipv6 qos-flow-list
17	(config-mac-qos)	Configures MAC QoS.	(config)# mac qos-flow-list
18	(dhcp-config)	Configures DHCP	(config)# ip dhcp pool
19	(config-dhcp)	Configures IPv6 DHCP (PD).	(config)# ipv6 dhcp pool
20	(config-route-map)	Configures a route map.	(config)# route-map
21	(config-rtr-rip)	Configures RIPng.	(config)# ipv6 router rip
22	(config-router)	Configures RIP.	(config)# router rip
		Configures OSPF.	(config)# router ospf
		Configures BGP4/BGP4+.	(config)# router bgp
23	(config-rtr)	Configures OSPFv3.	(config)# ipv6 router ospf
24	(config-router-af)	Configures RIP for each VRF.	(config)# router rip (config-router)# address-family ipv4 vrf
		Configures BGP4 for each VRF. (config-router-af)(ipv4 vrf) mode	(config)# router bgp (config-router)# address-family ipv4 vrf

#	Prompt displayed for the command mode	Description	Command for mode transition
		Configures BGP4+ global network. (config-router-af)(ipv6) mode	(config)# router bgp (config-router)# address-family ipv6
		Configures BGP4+ for each VRF. (config-router-af)(ipv6 vrf) mode	(config)# router bgp (config-router)# address-family ipv6 vrf
25	(config-auto-cf)	Configures auto-config.	(config)# auto-config
26	(config-netconf)	Configures netconf.	(config)# netconf.
27	(config-view)	Configures view.	(config)# parser view
28	(config-sh-nif)	Configures shaper mode.	(config)# shaper nif
29	(config-vrf)	Configures config-vrf.	(config)# vrf definition
30	(config-ether-cfm)	Configures the domain name and MA.	(config)# ethernet cfm domain
31	(config-track-object)	Configures the policy-based routing tracking functionality.	(config)# track-object
32	(config-pol)	Configures policy-based routing list information.	(config)# policy-list
33	(config-pol-sw)	Configures policy-based switching list information.	(config)# policy-switch-list

Specifiable values for parameters

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

Table 1-2: Specifiable values for parameters

Parameter type	Description	Input example
Name	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.	ip access-list standard inbound1
Host name	For a host name, alphabetic characters can be used for the first character, and alphanumeric characters, hyphens (-), and periods (.) can be used for the second and subsequent characters.	ip host telnet-host 192.168.1.1
IPv4 address, IPv4 subnet mask	Specify these items in decimal format, separating 1-byte decimal values by a period (.).	192.168.0.14 255.255.255.0
Wildcard mask	The same input format as IPv4 addresses. The set bits in an IPv4 address represent an arbitrary value.	255.255.0.0
IPv6 address	Specify this item in hexadecimal format, separating 2-byte hexadecimal values by colons (:).	3ffe:501:811:ff03::87ff:fed0:c7e0
Specification of multiple interfaces	Set the information about multiple interfaces. Specifiable interfaces are gigabitethernet, tengigabitethernet, vlan, and port-channel. You can specify gigabitethernet and tengigabitethernet at the same time, but cannot specify any other interfaces at the same time. The following are the input formats: • For gigabitethernet interface range gigabitethernet <*nif no.*>/<*port no.*> [- <*port no.*>] • For tengigabitethernet interface range tengigabitethernet <*nif no.*>/<*port no.*> [- <*port no.*>] • For vlan interface range vlan <*vlan id*> [- <*vlan id*>] • For port-channel interface range port-channel <*channel group number*> [- <*channel group number*>] You can specify no more than 16 of the above input formats, separating each by a comma (,).	interface range gigabitethernet 1/1-3 interface range gigabitethernet 1/1-3, tengigabitethernet 3/1 interface range vlan 1-100
add/remove specification	Add to or delete from the information when multiple interfaces have been specified. The add specification adds information to the current information. The remove specification deletes information from the current information.	switchport trunk allowed vlan add 100200-210 switchport trunk allowed vlan remove 100200-210

Any character string

Alphanumeric characters and special characters can be specified for parameters. Some special characters, however, cannot be used. Character codes are listed in the following table. Characters other than alphanumeric characters in the following list of character codes are special characters.

Table 1-3: 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	---	---

Notes

- To enter a question mark (`?`, or 0x3F), press **Ctrl** + **V**, and then type a question mark. You cannot copy and paste any specification string that includes a question mark.

Special characters that cannot be specified

Table 1-4: Special characters that cannot be specified

Character name	Character	Code
Double quotation mark	"	0x22
Dollar sign	$	0x24
Single quotation mark	'	0x27
Semicolon	;	0x3B
Backslash	\	0x5C
Grave accent mark	`	0x60
Left curly bracket	{	0x7B
Right curly bracket	}	0x7D

Example of specification string

access-list 10 remark "mail:xx@xx %tokyo"

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

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

Table 1-5: Range of <*nif no.*> values

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

Table 1-6: Range of <*port no.*> values [AX6700S] [AX6600S]

#	NIF type name abbreviation	Range of <*port no.*> values
1	NK1G-24T	1 to 24
2	NK1G-24S	1 to 24
3	NK1GS-8M	1 to 8
4	NK10G-4RX	1 to 4
5	NK10G-8RX	1 to 8

Table 1-7: Range of <*port no.*> values [AX6300S]

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

Range of values that can be set for <*channel group number*>

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

Table 1-8: Range of <*channel group number*> values

#	Model	Range of values
1	AX6304S/AX6604S	1 to 48
2	AX6308S/AX6608S/AX6708S	1 to 63

Range of values that can be set for <*vlan id*>

The following table lists the range of <*vlan id*> values.

Table 1-9: Range of <*vlan id*> values

#	Range of values
1	1 to 4095

How to specify <*vlan id list*> and the range of specifiable values

If <*vlan id list*> is written in the parameter input format, use a hyphen (`-`) or comma (`,`) to set multiple VLAN IDs. You can also set one VLAN ID, as when <*vlan id*> is written as the parameter input format. The range of values that can be set is the same as the range of <*vlan id*> values above. If there are large amounts of information set for <*vlan id list*>, the configuration information might be displayed over multiple lines. Conversely, if the information set in <*vlan id list*> is reduced by edits made to VLANs using `add/remove`, multiple lines of configuration information might be consolidated into one line.

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

1-3,5,10

Example of a specification displayed in multiple lines:

switchport trunk allowed vlan 100200300...

switchport trunk allowed vlan add 400500...

How to specify <*interface id list*> and the range of specifiable values

If <*interface id list*> is written in parameter input format, use a hyphen (`-`) or commas (`,`) as delimiters to specify multiple interfaces of the type gigabitethernet or tengigabitethernet. You can also specify just one interface of the type gigabitethernet or tengigabitethernet. The following are the input formats for gigabitethernet and tengigabitethernet interfaces:

- For gigabitethernet

  gigabitethernet <*nif no.*>`/`<*port no.*> `[-` <*port no.*>`]`

- For tengigabitethernet

  tengigabitethernet <*nif no.*>`/`<*port no.*> `[-` <*port no.*>`]`

The ranges of specifiable values for <*nif no.*> and <*port no.*> in <*nif no.*>`/`<*port no.*> `[-` <*port no.*>`]` are the same as the ranges of <*nif no.*> and <*port no.*> values in the above tables.

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

gigabitethernet 1/1-2,gigabitethernet 1/5,tengigabitethernet 3/1

Range of values that can be set for <*vrf id*> [OP-NPAR]

The following table lists the range of <*vrf id*> values.

Table 1-10: Range of <*vrf id*> values

#	VRF operation mode	Range of values
1	Not specified	Not configurable
2	axrp-enable axrp-enable-ipv4-ipv6	2 to 64
3	l2protocol-disable l2protocol-disable-ipv4-ipv6	2 to 250
4	gsrp-enable-ipv4-ipv6	2 to 125

Chapter

2. Connecting from an Operation Terminal

ftp-server
line console
line vty
speed
transport input

ftp-server

Permits access from remote operation terminals by using FTP. To permit or deny a remote operation terminal's access to the Switch, enter `config-line` mode, create a common access list that is used to restrict both Telnet and FTP access, and specify the IPv4 or IPv6 address of the remote operation terminal in the access list.

Syntax

To set information:

ftp-server

ftp-server vrf {<*vrf id*> | all}

To delete information:

no ftp-server

no ftp-server vrf {<*vrf id*> | all}

Input mode

`(config)`

Parameters

vrf {<*vrf id*> | all} [OP-NPAR]

<*vrf id*>

Accepts access from specified VRFs. The global network is excluded.

When VRFs that permit access are individually specified, a maximum of four entries can be specified per device.

all

Accepts access from all VRFs including the global network.

1. Default value when this parameter is omitted:

   Accepts access from the global network.

2. Range of values:

   Specify `all` for <*vrf id*>.

   Specify a VRF ID for <*vrf id*>.

   For details, see *Specifiable values for parameters*.

Default behavior

Does not allow remote FTP access.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When `config-line` mode is used to specify an access list for the Switch, the access list can be used to control (permit or deny) FTP log-in access to the Switch from remote operation terminals whose IPv4 or IPv6 addresses are specified in the access list.

2. If the `vrf all` parameter is specified, the global network or VRFs cannot be individually specified. [OP-NPAR]
3. If VRFs that permit access are individually specified, the maximum number of VRF IDs that can be specified by using this command and the `transport input` command is four. [OP-NPAR]

Related commands

line vty

ip access-group

ipv6 access-class

transport input

line console

Entering this command changes the mode to `config-line` mode, which permits settings related to the specified CONSOLE (RS232C) port.

Syntax

To set information:

line console 0

To delete information:

no line console

Input mode

`(config)`

Parameters

None

Default behavior

The console can be connected to a CONSOLE (RS232C) port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

speed

line vty

Permits Telnet remote access to a switch. This command is also used to limit the number of remote users that can be simultaneously logged in to the switch.

Configuration with this command enables remote access using the Telnet protocol from any remote operation terminal to be accepted. To restrict access, see *8.1.7 Setting the IP addresses of remote operation terminals permitted to log in* in the manual *Configuration Guide Vol. 1 For Version 11.7* to set ip access-group, ipv6 access-class, or transport input.

Syntax

To set information:

line vty 0 <*number*>

To delete information:

no line vty

Input mode

```
(config)
```

Parameters

<*number*>

Sets the number of users who are able to log in simultaneously.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 15 (The number of users who can log in can be set to any value from 1 to 16).

Default behavior

Does not accept remote access that uses the Telnet protocol.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Configuration with this command enables remote access using the Telnet protocol from any remote operation terminal to be accepted. To restrict access, see *8.1.7 Setting the IP addresses of remote operation terminals permitted to log in* in the manual *Configuration Guide Vol. 1 For Version 11.7* to set ip access-group, ipv6 access-class, or transport input.
2. If you change the maximum number of concurrent users, current user sessions will not be terminated. The change does not close the sessions of users who are currently logged in.

Related commands

transport input

ip access-group

ipv6 access-class

speed

Sets the communication speed of the CONSOLE (RS232C) port. If a user is already logged in from CONSOLE (RS232C) when the setting is changed, the communication speed is changed after the user logs out. If the communication speed is changed from a remote operation terminal while user login authentication from CONSOLE (RS232C) is in progress, authentication might fail.

Syntax

To set or change information:

speed <*number*>

To delete information:

no speed

Input mode

```
(config-line)
```

Parameters

<*number*>

Sets the communication speed for CONSOLE (RS232C) in bit/s.

1. Default value when this parameter is omitted:

   Sets the communication speed of CONSOLE (RS232C) to 9600 bit/s.

2. Range of values:

   1200, 2400, 4800, 9600, 19200

Default behavior

The communication speed of CONSOLE (RS232C) is 9600 bit/s.

Impact on communication

None

When the change is applied

If a user is already logged in from CONSOLE (RS232C) when the setting is changed, the communication speed is changed after the user logs out.

Notes

1. If a user is already logged in from CONSOLE (RS232C) when the setting is changed, the communication speed is changed after the user logs out. If the communication speed is changed from a remote operation terminal while user login authentication from CONSOLE (RS232C) is in progress, authentication might fail.

Related commands

line console

transport input

Restricts access from remote operation terminals based on protocol.

Syntax

To set or change information:

transport input {telnet | all | none}

transport input vrf {<*vrf id*> | all} {telnet | all | none}

To delete information:

no transport input

no transport input vrf {<*vrf id*> | all}

Input mode

```
(config-line)
```

Parameters

vrf {<*vrf id*> | all} [OP-NPAR]

<*vrf id*>

Accepts access from specified VRFs. The global network is excluded.

When VRFs that permit access are individually specified, a maximum of four entries can be specified per device.

all

Accepts access from all VRFs including the global network.

1. Default value when this parameter is omitted:

   Accepts access from the global network.

2. Range of values:

   Specify `all` for <*vrf id*>.

   Specify a VRF ID for <*vrf id*>.

   For details, see *Specifiable values for parameters*.

{telnet | all | none}

telnet

Accepts remote access that uses the Telnet protocol.

all

Accepts remote access using any protocol (currently only Telnet is supported).

Only the Telnet protocol supports access from VRFs. [OP-NPAR]

none

Does not accept remote access using any protocol.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `telnet`, `all`, or `none`.

Default behavior

Accepts remote access that uses the Telnet protocol from the global network.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To permit or restrict FTP connections, use the `ftp-server` command in global configuration mode.
2. If the `vrf all` parameter is specified, the global network or VRFs cannot be individually specified. [OP-NPAR]
3. If VRFs that permit access are individually specified, the maximum number of VRF IDs that can be specified by using this command and the `ftp-server` command is four. [OP-NPAR]

Related commands

line vty

ftp-server

ip access-group

ipv6 access-class

Chapter

3. Editing and Working with Configurations

end
quit (exit)
save (write)
show
status
top

end

Ends configuration command mode and returns you to administrator mode.

Syntax

end

Input mode

`Configuration command mode`

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

None

Response messages

The following table describes the response messages for the `end` command.

Table 3-1: Response messages for the end command

Message	Description
Unsaved changes found! Do you exit "configure" without save ? (y/n):	You are trying to finish editing a configuration without saving changes. Enter `y` to finish editing. If you do so, the configuration changes that you made will be lost. Enter `n` to cancel the `end` command. If necessary, use the `save` command to save the edited configuration.

Notes

1. You can use the `end` command to temporarily exit the configuration command mode without saving configuration file changes to internal flash memory. If you do so, the editing process of the configuration file will still be incomplete, so save the file after you finish making changes.
2. After editing the running configuration in RAM, if you execute the `end` command without saving the changes to internal flash memory, the startup configuration file in internal flash memory and the running configuration in RAM will not be the same. For this reason, if you enter configuration command mode again and then enter the `end` command, the same confirmation message will be displayed even if you have not made any new changes to the configuration file.
3. Do not press **Ctrl** + **C** to interrupt processing while the `end` command is being executed. If the processing is interrupted, configuration command mode does not end. Subsequent execution of a configuration command might cause the error message `Logical inconsistency occurred.` to be output. If this message is output, use the `end` command to end configuration command mode.

Related commands

None

quit (exit)

Reverts to an earlier mode. If you are in global configuration mode, this command ends configuration command mode and returns you to administrator mode. If you are editing data in a level-2 or level-3 detailed configuration command mode, you are returned one level higher.

For details about operations in user mode and administrator mode, see the manual *Operation Command Reference*.

Syntax

quit or exit

Input mode

`Configuration command mode, User mode, and administrator mode`

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

None

Response messages

The following table describes the response messages for the `quit (exit)` command.

Table 3-2: Response messages for the quit (exit) command

Message	Description
Unsaved changes found! Do you exit "configure" without save ? (y/n):	You are trying to finish editing a configuration without saving changes. Enter `y` to finish editing. If you do so, the configuration changes that you made will be lost. Enter `n` to cancel the `quit (exit)` command. If necessary, use the `save` command to save the edited configuration.

Notes

Note the following if you use the `quit (exit)` command in configuration command mode:

1. You can use the `quit (exit)` command to temporarily exit the configuration command mode without saving configuration file changes to internal flash memory. If you do so, the editing process of the configuration file will still be incomplete, so save the file after you finish making changes.
2. After editing the running configuration in RAM, if you execute the `quit (exit)` command without saving the changes to internal flash memory, the startup configuration file in internal flash memory and the running configuration in RAM will not be the same. For this reason, if you enter configuration command mode again and then enter the `quit (exit)` command, the same confirmation message will be displayed even if you have not made any new changes to the configuration file.
3. Do not press **Ctrl** + **C** to interrupt processing while the `quit (exit)` command is being executed. If the processing is interrupted, configuration command mode does not end. Subsequent execution of a configuration command might cause the error message `Logical`

`inconsistency occurred.` to be output. If this message is output, use the `end` command to end configuration command mode.

Related commands

None

save (write)

Saves the edited configuration to the startup configuration file or to a backup configuration file.

Syntax

save [<*file name*>] [debug]

write [<*file name*>] [debug]

Input mode

`Configuration command mode`

Parameters

<*file name*>

Specifies the name of the configuration file to be saved. This file will be the backup configuration file.

- Specifying a local configuration file

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

- Specify a remotely-stored configuration file.

  Specify a remote file name in either of the following URL formats:

- FTP

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

- TFTP

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

1. Default value when this parameter is omitted:

   The startup configuration file (`startup-config`) is overwritten by the configuration you have been editing.

debug

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

If the error `Data transfer failed.` occurs while attempting to access a remote file, re-execute the command with the debug parameter specified to display detailed error messages, such as server responses.

Default behavior

None

Impact on communication

None

When the change is applied

None

Response messages

The following table describes the response messages for the `save` command.

Table 3-3: Response messages for the save command

Message	Description
Configuration file already exist. Configuration file save to <*file name*>? (y/n):	This message notifies you that the specified file already exists, and asks you to confirm whether you want to execute the `save` command and overwrite it. Enter `y` to execute the `save` command. Enter `n` to cancel this operation.
Configuration file save to <*file name*>? (y/n):	This message confirms whether you want to execute the `save` command for the specified file. Enter `y` to execute the `save` command. Enter `n` to cancel this operation.

Notes

1. Saving the configuration file does not exit configuration command mode. To finish editing and exit configuration command mode, use the `exit` command or `end` command.
2. If you do not have permission to write the configuration file to the save destination, your edits are not saved to the file. To save edits to a file on a remote server, your remote server access permissions must be changed to allow you to write to the remote server.
3. You can use the `status` command to check if the configuration has been changed but not saved.
4. If there is insufficient free capacity in internal flash memory, changed configurations cannot be saved. Use the `show flash` operation command to check the free capacity in the user area. Saving a new startup configuration file (`/config/system.cnf`) requires free capacity equivalent to the size of the existing startup configuration file (`/config/system.cnf`) plus the size of the configuration you are editing. About 2 MB of free capacity is required for a maximum-size configuration file.

Related commands

None

show

Displays the configuration being edited.

Syntax

show [<*command*> [<*parameter*>]]

Input mode

`Configuration command mode`

Parameters

<*command*>

Specifies a configuration command.

<*parameter*>

Specifies parameters such as <*vlan id*> or <*access list name*> to limit the displayed items.

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

1. If there are many items in the configuration, the command might take time to execute.
2. If the configuration is edited, the `copy` command is executed, or NIF insertion is performed 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.

Related commands

None

status

Displays the status of the configuration being edited.

Syntax

status

Input mode

`Configuration command mode`

Parameters

None

Displayed information

The table below describes the items displayed for the `status` command.

Table 3-4: Response messages for the status command

Title		Displayed information
File name		The file being edited is displayed. Because only running-config can be edited, running-config is displayed.
Last modified time		The last-modified time and the person who updated the file are displayed. Depending on the edit status, the following information is displayed: The file contains initial installation defaults, and the file has not been changed: Not modified The file has not been edited since the switch was started: <*Date*> by <*User*> (not modified) The file has been edited and changed but not saved using the `save` command: <*Date*> by <*User*> (not saved) The file has been edited (changed) and changes saved using the `save` command: <*Date*> by <*User*> (saved)
Buffer	Total	Displays the total amount of storage that is available, including the configuration file that is currently being edited.
	Available	Displays the amount of storage remaining for use by the configuration file that is currently being edited. This remaining space is also displayed as a percentage of the total amount.
	Fragments	The amount of currently-edited configuration file space that is unavailable -- for example, because it is fragmented (items have been deleted, but the area has not been reclaimed) -- is displayed. This unavailable capacity is also displayed as a percentage of the total amount.
Login user		The names of users currently logged in to the switch, and their login times are displayed. `edit` is displayed next to users who are editing the configuration.

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

1. If the remaining capacity becomes very small, it might not be sufficient to execute some configuration commands.
2. Before and after a switch is restarted, the last-modified time displayed on the first line might be slightly inaccurate.

Related commands

None

top

Returns you from a level-2 or level-3 configuration command mode to global configuration mode (level 1).

Syntax

top

Input mode

`Configuration command mode`

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

None

Related commands

None

Chapter

4. Management Port

description

Sets supplementary information. Use this command to create a note related to the management port. You can check the note via ifDescr (SNMP MIB) if this command is set.

Syntax

To set or change information:

description <*Strings*>

To delete information:

no description

Input mode

```
(config-if)
```

Parameters

<*Strings*>

Sets supplementary information for the management port.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

NULL

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

interface mgmt

duplex

Sets the management port mode to `duplex`.

Syntax

To set or change information:

duplex {half | full |auto}

To delete information:

no duplex

Input mode

`(config-if)`

Parameters

{ half | full | auto }

Sets the management port mode to `duplex`.

half

Sets the line to half duplex (fixed) mode.

full

Sets the line to full duplex (fixed) mode.

auto

Determines the duplex mode by auto-negotiation.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

`auto` is set for the `speed` and `duplex` commands.

Impact on communication

If any management port settings are changed by using this command while the management port is up, the port first goes down and then comes up again.

Accordingly, the following might occur:

- If management port communication is in progress, it is stopped.
- Dynamic ARP entries and dynamic NDP entries generated for the management port are deleted.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If `auto` or a parameter containing `auto` is set for `speed` or `duplex`, auto-negotiation is performed.
2. If you do not want to use auto-negotiation, you must set `full` or `half` for `duplex` and `10` or

`100` for `speed`.

Related commands

interface mgmt

speed

interface mgmt

Moves to the management port level.

Syntax

To set or change information:

interface mgmt 0

To delete information:

no interface mgmt 0

Input mode

```
(config)
```

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A management port cannot be used if an IP address is not set for the port.
2. Configuring (enabling) the management port does not count towards the capacity limit (maximum number of interfaces). For the maximum number of interfaces, see *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*.

Related commands

None

ip routing

Performs IPv4 Layer 3 forwarding for a management port.

Syntax

To set or change information:

```
ip routing
```

To delete information:

```
no ip routing
```

Input mode

`(config-if)`

Parameters

None

Default behavior

IPv4 Layer 3 forwarding is not performed on a management port.

To perform IPv4 Layer 3 forwarding on a management port, specify `ip routing`.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Note that if a large volume of management port packets are forwarded, CPU usage rises, which might affect other communications and operations.

Related commands

interface mgmt

ipv6 routing

Performs IPv6 Layer 3 forwarding for a management port.

Syntax

To set or change information:

ipv6 routing

To delete information:

no ipv6 routing

Input mode

```
(config-if)
```

Parameters

None

Default behavior

IPv6 Layer 3 forwarding is not performed on a management port.

To perform IPv6 Layer 3 forwarding on a management port, specify `ipv6 routing`.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Note that if a large volume of management port packets are forwarded, CPU usage rises, which might affect other communications and operations.

Related commands

interface mgmt

shutdown

Sets the management port to the shutdown state.

Syntax

To set or change information:

```
shutdown
```

To delete information:

```
no shutdown
```

Input mode

`(config-if)`

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command can be set from the SNMP manager by using an SNMP SetRequest operation. If this command is set by using an SNMP SetRequest operation, the setting is applied to the configuration.

Related commands

interface mgmt

speed

Sets the line speed of a management port.

Syntax

To set or change information:

speed { 10 | 100 | auto | auto { 10 | 100 | 10 100 }}

To delete information:

no speed

Input mode

`(config-if)`

Parameters

{ 10 | 100 | auto | auto { 10 | 100 | 10 100 }}

Sets the line speed of a management port.

10

Sets the line speed to 10 Mbps.

100

Sets the line speed to 100 Mbps.

auto

Sets the line speed to auto-negotiation.

auto { 10 | 100 | 10 100 }

Auto-negotiation is performed at the specified line speed. This setting prevents the line speed negotiation from selecting a lower-than-expected speed, resulting in high line usage. If negotiation at the specified line speed does not succeed, the link status does not transition to link-up status.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

`auto` is set for the `speed` and `duplex` commands.

Impact on communication

If any management port settings are changed by using this command while the management port is up, the port first goes down and then comes up again.

Accordingly, the following might occur:

- If communication is in progress on the management port, it will be aborted.
- Dynamic ARP entries and dynamic NDP entries generated for the management port are deleted.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If `auto` or a parameter containing `auto` is set for `speed` or `duplex`, auto-negotiation is performed.
2. If you do not want to use auto-negotiation, you must set `10` or `100` for `speed` and `full` or `half` for `duplex`.

Related commands

interface mgmt

duplex

Chapter

5. Dial-up IP Connection

interface async
ip address (AUX)
peer default ip address

interface async

Sets items about AUX ports.

Entering this command transfers to `config-if` mode and permits AUX ports settings to be specified.

Syntax

To set information:

```
interface async 1
```

To delete information:

```
no interface async
```

Input mode

`(config)`

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

ip address (AUX)

peer default ip address

ip address (AUX)

Sets an IPv4 address for an AUX port.

Syntax

To set or change information:

ip address <*ip address*> <*subnet mask*>

To delete information:

no ip address

Input mode

`(config-if)`

Parameters

<*ip address*>

Specifies the local IPv4 address of an AUX port.

<*subnet mask*>

Specifies the subnet mask.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   128.0.0.0 to 255.255.255.255 (bits must be contiguous)

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed. Note, however, that if this command is used to make changes during dial-up IP connection, the changes will take effect from the next connection.

Notes

1. For a dial-up IP connection, both `peer default ip address` and `ip address (AUX)` must be set.

Related commands

interface async

peer default ip address

peer default ip address

Specifies the destination address of an AUX port.

Syntax

To set or change information:

peer default ip address <*ip address*>

To delete information:

no peer default ip address

Input mode

`(config-if)`

Parameters

<*ip address*>

Specifies the destination address of an AUX port.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed. Note, however, that if this command is used to make changes during dial-up IP connection, the changes will take effect from the next connection.

Notes

1. For a dial-up IP connection, both `peer default ip address` and `ip address (AUX)` must be set.

Related commands

interface async

ip address (AUX)

Chapter

6. Login Security and RADIUS or TACACS+

aaa accounting commands
aaa accounting exec
aaa authentication enable
aaa authentication enable attribute-user-per-method
aaa authentication enable end-by-reject
aaa authentication login
aaa authentication login console
aaa authentication login end-by-reject
aaa authorization commands
aaa authorization commands console
banner
commands exec
ip access-group
ipv6 access-class
parser view
radius-server host
radius-server key
radius-server retransmit
radius-server timeout
tacacs-server host
tacacs-server key
tacacs-server timeout
username

aaa accounting commands

Logs accounting information when commands are used.

Syntax

To set or change information:

aaa accounting commands { 15 | 0-15 } default { start-stop | stop-only } [broadcast] group tacacs+

To delete information:

no aaa accounting commands

Input mode

`(config)`

Parameters

{ 15 | 0-15 }

Specifies the command level for accounting.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   15: Only configuration commands are subject to accounting.

   0 to 15: Both operation commands and configuration commands are subject to accounting.

{start-stop | stop-only}

Specifies the trigger of accounting for commands.

start-stop

Sends a start instruction before a command is executed and a stop instruction after the command is executed.

stop-only

Sends a stop instruction before a command is executed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `start-stop` or `stop-only`

broadcast

If this parameter is specified, accounting information is sent in turn to all servers (a maximum of four) set by the `tacacs-server host` command, and continues regardless of success or failure in sending information or receiving acknowledgements from any of the servers.

1. Default value when this parameter is omitted:

   Accounting information will be repeatedly sent in turn to a maximum of four servers until it is successfully sent to, and acknowledgements are received from, the servers.

group tacacs+

The TACACS+ server is used as the accounting server.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

tacacs-server host

aaa accounting exec

Enables accounting of login and logout.

Syntax

To set or change information:

aaa accounting exec default { start-stop | stop-only } [broadcast] { group radius | group tacacs+ }

To delete information:

no aaa accounting exec

Input mode

`(config)`

Parameters

{start-stop | stop-only}

Sets the trigger for accounting.

start-stop

Sends a start instruction at login and a stop instruction at logout.

stop-only

Sends a stop instruction at logout only.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `start-stop` or `stop-only`

broadcast

If this parameter is specified, accounting information is sent in turn to all servers (a maximum of four) set by the `radius-server host` or `tacacs-server host` command, and continues regardless of success or failure in sending information or receiving acknowledgements from any of the servers.

1. Default value when this parameter is omitted:

   Accounting information will be repeatedly sent in turn to a maximum of four servers until it is successfully sent to, and acknowledgements are received from, the servers.

{group radius | group tacacs+}

Sets the type of an accounting server.

group radius

The RADIUS server is used as the accounting server.

group tacacs+

The TACACS+ server is used as the accounting server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

`group radius` or `group tacacs+`

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

radius-server host

tacacs-server host

aaa authentication enable

Specifies the authentication method to be used when changing to administrator mode (`enable` command). If the first specified authentication method fails, the second specified method is used for authentication. You can change how authentication works when the first method failed by using the `aaa authentication enable end-by-reject` command.

Syntax

To set or change information:

aaa authentication enable default <*method*> [<*method*> [<*method*>]]

To delete information:

no aaa authentication enable

Input mode

`(config)`

Parameters

default <*method*> [<*method*> [<*method*>]]

Specifies the authentication method to be used when changing to administrator mode (`enable` command) for <*method*>.

Specify any of the parameters below for <*method*>. You cannot set the same <*method*> more than once.

group radius

RADIUS authentication is used.

group tacacs+

TACACS+ authentication is used.

enable

Local password authentication is used.

Default behavior

Local password authentication is performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the `group radius` parameter or the `group tacacs+` parameter is specified, you cannot switch to administrator mode if communication with a RADIUS or TACACS+ server is impossible or authentication fails. Therefore, we recommend that you specify the `enable` parameter at the same time.

Related commands

aaa authentication enable attribute-user-per-method

aaa authentication enable end-by-reject

radius-server

tacacs-server

aaa authentication enable attribute-user-per-method

Based on each authentication method, change the user name attribute to be used for authentication when changing to administrator mode (`enable` command) as follows:

- For RADIUS authentication, `$enab15$` is sent as the User-Name attribute.
- For TACACS+ authentication, the login user name is sent as the User attribute.

Syntax

To set information:

aaa authentication enable attribute-user-per-method

To delete information:

no aaa authentication enable attribute-user-per-method

Input mode

`(config)`

Parameters

None

Default behavior

"admin" is sent as the User-Name attribute when changing to administrator mode (`enable` command).

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Use this command to suit your RADIUS or TACACS+ server.

Related commands

aaa authentication enable

aaa authentication enable end-by-reject

Terminates authentication if an attempt to change to administrator mode (by the `enable` command) is denied. If the authentication fails due to an abnormality, such as an inability to communicate, the next authentication method specified by the `aaa authentication enable` command is used to perform authentication.

Syntax

To set information:

aaa authentication enable end-by-reject

To delete information:

no aaa authentication enable end-by-reject

Input mode

`(config)`

Parameters

None

Default behavior

If authentication fails, regardless of the reason for failure, the next authentication method specified by the `aaa authentication enable` command is used to perform authentication.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is only valid for authentication methods specified by the `aaa authentication enable` command.

Related commands

aaa authentication enable

aaa authentication login

Specifies the authentication method to be used at login. If the first specified authentication method fails, the second specified method is used for authentication. You can change how authentication works when the first method failed by using the `aaa authentication login end-by-reject` command.

Syntax

To set or change information:

aaa authentication login default <*method*> [<*method*> [<*method*>]]

To delete information:

no aaa authentication login

Input mode

`(config)`

Parameters

default <*method*> [<*method*> [<*method*>]]

Specifies the authentication method to be used at login for <*method*>.

Specify any of the parameters below for <*method*>. You cannot set the same <*method*> more than once.

group radius

RADIUS authentication is used.

group tacacs+

TACACS+ authentication is used.

local

Local password authentication is used.

Default behavior

Local password authentication is performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the `group radius` parameter or the `group tacacs+` parameter is specified, you cannot log in to the Switch if communication with a RADIUS or TACACS+ server is impossible or authentication fails. Therefore, we recommend that you specify the `local` parameter at the same time.

Related commands

aaa authentication login console

aaa authentication login end-by-reject

radius-server host

tacacs-server host

aaa authentication login console

Applies the authentication method specified by the `aaa authentication login` command when the user logs in from the console (RS232C) or AUX port.

Syntax

To set information:

aaa authentication login console

To delete information:

no aaa authentication login console

Input mode

`(config)`

Parameters

None

Default behavior

Local password authentication is used when a user logs in from the console (RS232C) or AUX port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To perform RADIUS or TACACS+ authentication, you must set the `aaa authentication login` command at the same time.
2. When the `local` parameter is not specified as the authentication method by the `aaa authentication login` command, and the `aaa authentication login console` command is set, the user cannot log in from the console (RS232C) and AUX if communication with a RADIUS or TACACS+ server is impossible, authentication fails, or the user logs in from a standby system.

Related commands

aaa authentication login

aaa authentication login end-by-reject

aaa authentication login end-by-reject

Terminates authentication if login authentication is denied. If the authentication fails due to an abnormality, such as an inability to communicate, the next authentication method specified by the `aaa authentication login` command is used to perform authentication.

Syntax

To set information:

aaa authentication login end-by-reject

To delete information:

no aaa authentication login end-by-reject

Input mode

`(config)`

Parameters

None

Default behavior

If authentication fails, regardless of the reason for failure, the next authentication method specified by the `aaa authentication login` command is used to perform authentication.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is only valid for authentication methods specified by the `aaa authentication login` command.

Related commands

aaa authentication login

aaa authorization commands

This command is specified to perform command authorization by using a RADIUS server, TACACS+ server, or by using local (configuration-based) authorization.

Note that, after successful login, you will not be authorized to execute any commands except `logout`, `exit`, `quit`, `disable`, `end`, `set terminal`, `show whoami`, and `who am i` if any of the following applies:

- If the command class or the command list cannot be obtained as a vendor-specific attribute or an attribute value when authentication is performed on a RADIUS server or a TACACS+ server
- If the user name and the associated command class (`username view-class`) or command lists (`username view`, `parser view`, or `commands exec`) are not configured when authentication is performed using a local password

Syntax

To set or change information:

aaa authorization commands default <*method*> [<*method*> [<*method*>]]

To delete information:

no aaa authorization commands

Input mode

`(config)`

Parameters

default <*method*> [<*method*> [<*method*>]]

For <*method*>, specifies the method to be used for command authorization.

Specify any of the parameters below for <*method*>. You cannot set the same <*method*> more than once.

group radius

Command authorization is performed by a RADIUS server.

group tacacs+

Command authorization is performed by a TACACS+ server.

local

Local command authorization is performed.

Default behavior

Command authorization is not performed.

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

1. With this setting, when authentication is performed on the RADIUS server or TACACS+ server specified by the `aaa authentication login` command, or by using a local password,

this authorizes the use of command class or command list related commands. The `aaa authorization commands console` command alone is not sufficient for command authorization. You also need to have used the `aaa authentication login` command in advance.

2. Note that, after successful login, you will not be authorized to execute any commands except `logout`, `exit`, `quit`, `disable`, `end`, `set terminal`, `show whoami`, and `who am i` if any of the following applies:

    - If the command class or the command list cannot be obtained as a vendor-specific attribute or an attribute value when authentication is performed on a RADIUS server or a TACACS+ server
    - If the user name and the associated command class (`username view-class`) or command list (`username view`) are not configured when authentication is performed using a local password

Related commands

radius-server host

tacacs-server host

aaa authentication login

aaa authorization commands console

parser view

commands exec

username

aaa authorization commands console

Authorizes the commands specified by the `aaa authorization commands` command when the user logs in from the console (RS232C) or AUX port.

Syntax

To set information:

aaa authorization commands console

To delete information:

no aaa authorization commands console

Input mode

`(config)`

Parameters

None

Default behavior

Authorization of commands is not required when a user logs in from the console (RS232C) or AUX port.

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

1. The `aaa authorization commands console` command alone is not sufficient for command authorization. You also need to set the `aaa authorization commands` command.
2. With this setting, if a user logs in from the console (RS232C) or AUX port, command authorization is used to restrict the commands that can be executed.

Related commands

aaa authorization commands

banner

Sets the messages to be displayed before and after a user logs in. Depending on the specified parameters, messages can be displayed before or after a user login via Telnet, console, or FTP. A separate message can be set for FTP access.

The following table describes how the login message is displayed according to parameter settings.

Table 6-1: List of operations according to parameter settings

Description		Operation	
login(motd)	**login-ftp(motd-ftp)**	**Message displayed for Telnet or console access**	**Message displayed for FTP access**
Message A is set.	Not set	Message A is displayed.	Message A is displayed.
Message A is set.	The `disable` parameter is set.	Message A is displayed.	Not displayed.
Message A is set.	Message B is set.	Message A is displayed.	Message B is displayed.
Not set	Message B is set.	Not displayed.	Message B is displayed.
Not set (initial state)	Not set (initial state)	Not displayed.	Not displayed.

Syntax

To set or change information:

banner login { {encode "<*encoded message*>"} | plain-text }

banner login-ftp { {encode "<*encoded message*>"} | plain-text | disable }

banner motd { {encode "<*encoded message*>"} | plain-text }

banner motd-ftp { {encode "<*encoded message*>"} | plain-text | disable }

To delete information:

no banner [{motd | motd-ftp | login | login-ftp }]

Input mode

`(config)`

Parameters

login

Sets the message to be displayed before a user logs in via Telnet, console, or FTP.

plain-text

Enter the login message as a plain-text string. After the command is entered, the following message appears and you can enter a string in lines.

```
--- Press CTRL+D or only '.' on last line ---
```

At this point, enter the string you want to display for the login message. At the end of the string, press the **Ctrl** + **D** keys or enter a period (.) to close the input window.

Entries are automatically set in the `encode` parameter configuration. Any login message that was set previously is deleted. If, after inputting the login message, you want to check an image of how the login screen will look in text format, use the `show banner {motd | motd-ftp | login | login-ftp } plain-text` command to do so.

1. Default value when this parameter is omitted:

   No login messages are displayed.

2. Range of values:

   A string consisting of a maximum of 720 alphanumeric characters

3. Note on using this parameter:

   When entering login messages, check the screen settings for the client so that you do not use characters that cannot be displayed on the client. Otherwise, when the `show banner {motd | motd-ftp | login | login-ftp } plain-text` command is executed or a client is connected, the prompt might be garbled and the screen display might freeze. If you want to cancel login message setting while entering the login message, press the **CTRL**+ **C** keys to abort this. If you enter far more characters than the maximum number of characters permitted in a line, you may find that no further keyboard input (including the **CTRL**+ **D** keys or a line break) is accepted. If this happens, use the **Backspace** key to delete entered characters and then re-enter them, or use the **CTRL**+ **C** keys to abort.

   While entering a message, if you find that the previous character in a single line is not deleted when you press the **Backspace** key, change the setting of the **Backspace** key of the terminal so that the BS control code (ASCII 0x08 ^H) is sent. Note that the **Backspace** key does not affect characters in other than the current line.

encode "<*encoded message*>"

Enter a Base64-encoded string as a login message. Any login message that was set previously is deleted. Normally this is used to encode a message that was entered with the `plain-text` parameter. If you want to check a text-format image of what the login screen message will look like, use the `show banner {motd | motd-ftp | login | login-ftp } plain-text` command.

1. Default value when this parameter is omitted:

   No login messages are displayed.

2. Range of values:

   Enter a Base64-encoded string enclosed in double-quotation marks (") (a maximum of 960 characters).

3. Note on using this parameter:

   When entering login messages, check the screen settings for the client so that you do not use characters that cannot be displayed on the client. Otherwise, when the `show banner {motd | motd-ftp | login | login-ftp } plain-text` command is executed, or a client is connected, the prompt might be garbled and the screen display might freeze.

login-ftp

Individually sets or disables the message to be displayed before a user logs in through FTP access. For FTP access, this setting has precedence over the login setting.

plain-text

Enter the login message as a plain-text string. For details, see the *plain-text* section under the *login* parameter above.

encode "<*encoded message*>"

Enter a Base64-encoded string as a login message. For details, see the *encode* section under the *login* parameter above.

disable

Does not display a login message for FTP access even when the `login` parameter is set.

motd

Sets the message to be displayed after a user logs in through Telnet, console, or FTP access.

plain-text

Enter the login message as a plain-text string. For details, see the *plain-text* section under the *login* parameter above.

encode "<*encoded message*>"

Enter a Base64-encoded string as a login message. For details, see the *encode* section under the *login* parameter above.

motd-ftp

Individually sets or disables a message to be displayed after a user logs in through FTP access. For FTP access, this setting has precedence over the `motd` setting.

plain-text

Enter the login message as a plain-text string. For details, see the *plain-text* section under the *login* parameter above.

encode "<*encoded message*>"

Enter a Base64-encoded string as a login message.

For details, see the *encode* section under the *login* parameter above.

disable

Does not display a login message for FTP access even when the `motd` parameter is set.

Default behavior

No login messages are displayed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When setting a login message, if a client log-in prompt is unnecessary (for example: when no password is required, and the user name is automatically passed by the client), the login message and the post-authentication screen are displayed in turn.

   When entering a login message, check the screen setting for the client so that you do not use characters that cannot be displayed on the client. Otherwise, when the `show banner {motd | motd-ftp | login | login-ftp } plain-text` command is executed or a client is connected, the prompt might be garbled and the screen display might freeze.

Related commands

None

commands exec

Adds a command string to a command list used when local command authorization is enabled.

A maximum of 40 commands, including permitted and restricted commands, can be set in a command list.

Syntax

To set information:

commands exec {include | exclude} all <*command*>

To delete information:

no commands exec {include | exclude} all <*command*>

Input mode

`(config-view)`

Parameters

{include | exclude}

Restricts use of the specified command string.

Command strings for which the `include` parameter is specified are configured as permitted commands. Command strings for which the `exclude` parameter is specified are configured as restricted commands.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `include` or `exclude`

all <*command*>

Specifies a command string to be added to the command list.

The Switch judges whether the initial character string of the command entered by the user matches any of the command strings specified in the command lists (match beginning).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 50 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

   In addition, commas (,) cannot be used in this parameter.

Default behavior

None

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

1. A maximum of 40 commands, including permitted and restricted commands, can be set in a command list. A string consisting of a maximum of 50 characters can be set as a command string.

Related commands

aaa authorization commands

parser view

username

ip access-group

Sets an access list that specifies the IPv4 addresses of remote operation terminals for which remote login to the Switch is permitted or denied. This setting is common to all types of remote access (Telnet or FTP).

No more than 128 entries, spread over multiple lines, including access list entries set by using `ip access-group` and `ipv6 access-class`, can be set.

Syntax

To set information:

ip access-group {<*access list number*>|<*access list name*>} [vrf {<*vrf id*>| all}] in

To delete information:

no ip access-group {<*access list number*>|<*access list name*>} [vrf {<*vrf id*>| all}]

Input mode

`(config-line)`

Parameters

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

Specifies the ID for an IPv4 address filter access list (an ID for `ip access-list standard` or an IPv4 address filter specific access list ID for an `access-list`).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*access list number*>, specify values from 1 to 99, or from 1300 to 1999 (in decimal).

   For <*access list name*>, specify a name that is no more than 31 characters.

   For details, see *Specifiable values for parameters*.

vrf {<*vrf id*> | all} [OP-NPAR]

Applies an access list to access from VRF.

<*vrf id*>

Applies an access list to access from the specified VRF.

all

Applies an access list to access from all VRFs including the global network.

1. Default value when this parameter is omitted:

   Applies an access list to access from the global network.

2. Range of values:

   Specify `all` for <*vrf id*>.

   Specify a VRF ID for <*vrf id*>.

   For details, see *Specifiable values for parameters*.

Default behavior

Access, using IPv4 addresses, is permitted from all remote operation terminals.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This setting is common to all types of remote access (Telnet or FTP).
2. To allow FTP connections, set `ftp-server`.
3. When `ip access-group` is not set, access using IPv4 addresses is permitted from all remote operation terminals.
4. Changing the access-permitted IPv4 addresses does not close the sessions of users who have already logged in. The change is applied to users who attempt to log in remotely after the change.
5. An access list which is specified for `vrf all` is applied after the access list set for the global network or each `vrf` *<vrf id>* is applied.

Related commands

line vty

ftp-server

transport input

ipv6 access-class

access-list

ip access-list standard

ipv6 access-class

Sets an access list that specifies the IPv6 addresses of remote operation terminals for which remote login to the Switch is permitted or denied. This setting is common to all types of remote access (Telnet or FTP).

No more than 128 entries, spread over multiple lines, including access list entries set by using `ip access-group` and `ipv6 access-class`, can be set.

Syntax

To set information:

ipv6 access-class <*access list name*> [vrf {<*vrf id*>| all}] in

To delete information:

no ipv6 access-class <*access list name*> [vrf {<*vrf id*>| all}]

Input mode

`(config-line)`

Parameters

<*access list name*>

Specifies an IPv6 filter access-list ID (identifier for `ipv6 access-list`).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   For details, see *Specifiable values for parameters*.

vrf {<*vrf id*> | all} [OP-NPAR]

Applies an access list to access from VRF.

<*vrf id*>

Applies an access list to access from the specified VRF.

all

Applies an access list to access from all VRFs including the global network.

1. Default value when this parameter is omitted:

   Applies an access list to access from the global network.

2. Range of values:

   Specify `all` for <*vrf id*>.

   Specify a VRF ID for <*vrf id*>.

   For details, see *Specifiable values for parameters*.

Default behavior

Access using IPv6 addresses is permitted from all remote operation terminals.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This setting is common to all types of remote access (Telnet or FTP).
2. To allow FTP connections, set `ftp-server`.
3. When `ipv6 access-class` is not set, access using IPv6 addresses is permitted from all remote operation terminals.
4. Changing the access-permitted IPv6 addresses does not close the sessions of users who have already logged in. The change is applied to users who attempt to log in remotely after the change.
5. An access list which is specified for `vrf all` is applied after the access list set for the global network or each `vrf` <*vrf id*> is applied.

Related commands

line vty

ftp-server

transport input

ip access-group

ipv6 access-list

parser view

Generates a command list used when local command authorization is enabled. Entering this command switches to `config-view` mode in which information about the command list can be set.

A maximum of 20 command lists can be generated per device.

Syntax

To set information:

parser view <*view name*>

To delete information:

no parser view <*view name*>

Input mode

```
(config)
```

Parameters

<*view name*>

Specifies the name of a command list to be generated.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   An alphabetical character can be specified for the first character of such name, and alphanumeric characters, hyphens (-), underscores (_), and periods (.) can be specified for the subsequent characters.

   For details, see *Name* of the *Parameter type* column in the *Specifiable values for parameters* table.

Default behavior

None

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

1. A maximum of 20 command lists can be generated per device.

Related commands

aaa authorization commands

commands exec

username

radius-server host

Configures the RADIUS server used for authentication, authorization, and accounting purposes.

Syntax

To set or change information:

radius-server host {<*ipv4 address*> | <*ipv6 address*> [interface <*interface type*> <*interface number*>] |<*host name*>} [auth-port <*port*>] [acct-port <*port*>] [timeout <*seconds*>] [retransmit <*retries*>] [key <*string*>] [{auth-only | acct-only}]

To delete information:

no radius-server host {<*ipv4 address*> | <*ipv6 address*> [interface <*interface type*> <*interface number*>] |<*host name*>}

Input mode

`(config)`

Parameters

{<*ipv4 address*> | <*ipv6 address*> [interface <*interface type*> <*interface number*>] | <*host name*>}

<*ipv4 address*>

Specifies the IPv4 address of the RADIUS server in dot notation.

<*ipv6 address*> [interface <*interface type*> <*interface number*>]

Specifies the IPv6 address of the RADIUS server in colon notation.

Specify the `interface` parameter only when a link-local address is specified.

For <*interface type*> <*interface number*>, the following values can be specified:

- vlan <*vlan id*>

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

- mgmt `0`

<*host name*>

Specifies the host name of the RADIUS server with 64 or fewer characters.

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   An IPv4 address, an IPv6 address, or a host name can be specified.

   When an IPv6 link-local address is specified, specify the interface at the same time.

key <*string*>

Specifies the RADIUS key used for encryption or for authentication of communication with the RADIUS server. The same RADIUS key must be set for the client and the RADIUS server.

1. Default value when this parameter is omitted:

   The RADIUS key set by using `radius-server key` is used. If no key is set, the RADIUS server is disabled.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

auth-port <*port*>

Specifies the RADIUS server port number.

1. Default value when this parameter is omitted:

   Port number 1812 is used.

2. Range of values:

   1 to 65535

acct-port <*port*>

Specifies the port number for RADIUS server accounting.

1. Default value when this parameter is omitted:

   Port number 1813 is used.

2. Range of values:

   1 to 65535

{auth-only | acct-only}

Restricts use of the specified RADIUS server. It can be used only for the specified purpose. A RADIUS server specified with the `auth-only` option is used as a server dedicated to authentication. A RADIUS server specified with the `acct-only` option is used as a server dedicated to accounting.

1. Default value when this parameter is omitted:

   The RADIUS server can be used for all purposes (authentication and accounting).

2. Range of values:

   None

retransmit <*retries*>

Specifies the number of times an authentication request is resent to the RADIUS server.

1. Default value when this parameter is omitted:

   The number of times configured by using `radius-server retransmit` is used. If no period is set, the initial value is 3.

2. Range of values:

   0 to 15

timeout <*seconds*>

Specifies the timeout period (in seconds) for a response from the RADIUS server.

1. Default value when this parameter is omitted:

   The period configured by using `radius-server timeout` is used. If no period is set, the initial value is 5.

2. Range of values:

   1 to 30

Default behavior

Because the RADIUS server is not configured, no RADIUS communication is performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A maximum of four RADIUS servers can be specified per device.
2. When multiple RADIUS servers are specified, the RADIUS server that is first in the configuration file listing is the first server used for authentication.
3. If the `key` parameter is omitted and the `radius-server key` command is not set, the RADIUS server is disabled.

Related commands

radius-server key

radius-server retransmit

radius-server timeout

aaa authentication login

aaa authorization commands

aaa accounting exec

radius-server key

Sets the default RADIUS server key for authentication, authorization, and accounting purposes.

Syntax

To set or change information:

radius-server key <*string*>

To delete information:

no radius-server key

Input mode

`(config)`

Parameters

<*string*>

Specifies the RADIUS key used for encryption or for authentication of communication with the RADIUS server. The same RADIUS key must be set for the client and the RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The `key` setting for the `radius-server host` command has precedence over the setting for the `radius-server key` command.

Related commands

radius-server host

radius-server retransmit

radius-server timeout

aaa authentication login

aaa authorization commands

aaa accounting exec

radius-server retransmit

Sets the default number of retransmissions to a RADIUS server used for authentication, authorization, and accounting purposes.

Syntax

To set or change information:

radius-server retransmit <*retries*>

To delete information:

no radius-server retransmit

Input mode

`(config)`

Parameters

<*retries*>

Specifies the number of times an authentication request is resent to the RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 15

Default behavior

The default value for the number of times an authentication request is retransmitted to a RADIUS server is 3.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The `retransmit` setting for the `radius-server host` command has precedence over the setting for the `radius-server retransmit` command.

Related commands

radius-server host

radius-server key

radius-server timeout

aaa authentication login

aaa authorization commands

aaa accounting exec

radius-server timeout

Sets a response timeout value for a RADIUS server used for authentication, authorization, and accounting purposes.

Syntax

To set or change information:

radius-server timeout <*seconds*>

To delete information:

no radius-server timeout

Input mode

`(config)`

Parameters

<*seconds*>

Specifies the timeout period in seconds for a response from the RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 30

Default behavior

The default response timeout value for the RADIUS server is 5 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The `timeout` setting for the `radius-server host` command has precedence over the setting for the `radius-server timeout` command.

Related commands

radius-server host

radius-server key

radius-server retransmit

aaa authentication login

aaa authorization commands

aaa accounting exec

tacacs-server host

Configures the TACACS+ server used for authentication or authorization.

Syntax

To set or change information:

tacacs-server host {<*host name*> | <*ip address*>} [key <*string*>] [port <*port*>] [timeout <*seconds*>] [{auth-only | acct-only}]

To delete information:

no tacacs-server host {<*host name*> | <*ip address*>}

Input mode

`(config)`

Parameters

{<*host name*> | <*ip address*>}

Specifies the IPv4 address or the host name of the TACACS+ server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   An IPv4 address (in dot notation) or a host name can be specified.

   Specify the host name with 64 or fewer characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

key <*string*>

Specifies the shared private key used for encryption or authentication of communication with the TACACS+ server. The same shared private key must be set for the client and the TACACS+ server.

1. Default value when this parameter is omitted:

   The shared private key configured by using `tacacs-server key` is used. If the key is not configured, communication with the TACACS+ server is not encrypted.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

port <*port*>

Specifies the TCP port number for TACACS+ server authentication.

1. Default value when this parameter is omitted:

   Port number 49 is used.

2. Range of values:

   1 to 65535

timeout <*seconds*>

Sets the timeout period (in seconds) for a response from the TACACS+ server.

1. Default value when this parameter is omitted:

   The period configured by using `tacacs-server timeout` is used. If no period is set, the initial value is 5.

2. Range of values:

   1 to 30

{auth-only | acct-only}

Restricts use of the specified TACACS+ server. It can be used only for the specified purpose.

A TACACS+ server specified with the `auth-only` parameter is used as a server dedicated to authentication. A TACACS+ server specified with the `acct-only` parameter is used as a server dedicated to accounting.

1. Default value when this parameter is omitted:

   The TACACS+ server can be used for all purposes (authentication and accounting).

2. Range of values:

   None

Default behavior

Because the TACACS+ server is not configured, no TACACS+ communication is performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A maximum of four TACACS+ servers can be specified per device.
2. When multiple TACACS+ servers are specified, the TACACS+ server that is first in the configuration file listing is the first server used for authentication.

Related commands

tacacs-server key

tacacs-server timeout

aaa authentication login

aaa authorization commands

aaa accounting exec

aaa accounting commands

tacacs-server key

Sets the default shared private key of a TACACS+ server used for authentication or authorization purposes.

Syntax

To set or change information:

tacacs-server key <*string*>

To delete information:

no tacacs-server key

Input mode

`(config)`

Parameters

<*string*>

Specifies the shared private key used for encryption or authentication of communication with the TACACS+ server. The same shared private key must be set for the client and the TACACS+ server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The `key` setting specific to the `tacacs-server host` command has precedence over the setting for the `tacacs-server key` command.

Related commands

tacacs-server host

tacacs-server timeout

aaa authentication login

aaa authorization commands

aaa accounting exec

aaa accounting commands

tacacs-server timeout

Sets the default response timeout value for a TACACS+ server used for authentication or authorization purpose.

Syntax

To set or change information:

tacacs-server timeout <*seconds*>

To delete information:

no tacacs-server timeout

Input mode

`(config)`

Parameters

<*seconds*>

Specifies the timeout period in seconds for a response from the TACACS+ server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 30

Default behavior

The default response timeout value for the TACACS+ server is 5 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The `timeout` setting specific to the `tacacs-server host` command has precedence over the setting of the `tacacs-server timeout` command.

Related commands

tacacs-server host

tacacs-server key

aaa authentication login

aaa authorization commands

aaa accounting exec

aaa accounting commands

username

For a specified user, sets the command list or command class permitted by local command authorization. In addition, this command also specifies the auto logout period for each user, paging, and help message display operation.

A maximum of 20 users can be specified per device.

Syntax

To set or change information:

username <*user name*> exec-timeout <*minutes*>

username <*user name*> terminal-pager {enable | disable}

username <*user name*> terminal-help {all | no-utility}

username <*user name*> view <*view name*>

username <*user name*> view-class {root | allcommand | noconfig | nomanage | noenable}

To delete information:

no username <*user name*>

no username <*user name*> exec-timeout

no username <*user name*> terminal-pager

no username <*user name*> terminal-help

no username <*user name*> view

no username <*user name*> view-class

Input mode

`(config)`

Parameters

<*user name*>

Specifies the name of the user to be set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the user name with 16 or fewer characters (the first character must be alphabetic and the subsequent characters must be alphanumeric).

   For `exec-timeout`, `terminal-pager`, or `terminal-help` you can specify `default_user`, and the settings apply to all users. When `default_user` is specified, the settings apply only to users who are not specified using a specific user name.

exec-timeout <*minutes*>

Specifies the auto-logout time (in minutes) of the specified user. If 0 is specified, auto-logout does not apply. This setting is loaded when a user logs in, and has precedence over settings configured by using the `set exec-timeout` operation command before the user logs in.

1. Default value when this parameter is omitted:

   60

2. Range of values:

0 to 60

terminal-pager {enable | disable}

Specifies whether to enable paging (messaging) of the specified user. This setting is loaded when a user logs in, and has precedence over the settings configured by using the `set terminal pager` operation command before the user logs in.

enable

Paging is performed.

disable

Paging is not performed.

1. Default value when this parameter is omitted:

   enable

2. Range of values:

   `enable` or `disable`

terminal-help {all | no-utility}

For the specified user, specifies what type of operation command help messages can be displayed. This setting is loaded when a user logs in, and has precedence over the settings configured by using the `set terminal help` operation command before the user logs in.

all

Enables help messages for all permissible operation commands to be displayed.

no-utility

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

1. Default value when this parameter is omitted:

   all

2. Range of values:

   `all` or `no-utility`

view <*view name*>

Specifies a command list generated by the `parser view` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   An alphabetical character can be specified for the first character of such name, and alphanumeric characters, hyphens (-), underscores (_), and periods (.) can be specified for the subsequent characters.

   For details, see *Name* of the *Parameter type* column in the *Specifiable values for parameters* table.

view-class {root | allcommand | noconfig | nomanage | noenable}

Specifies a command class to be assigned to a user.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

   Specifies any one of `root`, `allcommand`, `noconfig`, `nomanage`, and `noenable` command classes that have been defined in advance on the Switch.

   For details, see *Table 8-11 Command classes* in the manual *Configuration Guide Vol. 1 For Version 11.7*.

Default behavior

None

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

1. A maximum of 20 users including `default_user` can be set per device.
2. When `default_user` is specified, the settings apply only to users who are not specified using a specific user name. For example, when 0 is set as the `exec-timeout` value for `default_user`, if the `terminal-pager` or `terminal-help` parameter is set for the user name `staff`, the setting to be applied to user `staff` is 60, and this is set as the initial value when the `exec-timeout` parameter is omitted.
3. For users with (username command) parameter settings for at least one of `exec-timeout`, `terminal-pager`, and `terminal-help` (which is all users if `default_user` is set with this command), these (username command) parameter settings override settings made by the `set exec-timeout`, `set terminal pager`, and `set terminal help` operation commands, and the initial default value applies if the parameter was not specified. In this case, operation for each command can be changed temporarily just for the current log-in session by using the `set exec-timeout`, `set terminal pager`, or `set terminal help` operation commands after the user has logged in.
4. If all of the username command `exec-timeout`, `terminal-pager`, and `terminal-help` settings for a certain user are deleted by using this command with "no" ("no username"), the parameter values revert to the values set by the `set exec-timeout`, `set terminal pager`, or `set terminal help` operation commands (or to the default values if they were not set by these commands) -- they revert to the values that they had before the username command was used to set them.

Related commands

aaa authorization commands

parser view

commands exec

Chapter

7. Time Settings and NTP

clock timezone
ntp access-group
ntp authenticate
ntp authentication-key
ntp broadcast
ntp broadcast client
ntp broadcastdelay
ntp master
ntp peer
ntp server
ntp trusted-key

clock timezone

Sets the time zone.

The Switch maintains the date and time internally in Coordinated Universal Time (UTC). This clock timezone setting affects only time set using the `set clock` command, and the time displayed by using an operation command.

Syntax

To set or change information:

clock timezone <*zone name*> <*hours offset*> [<*minutes offset*>]

To delete information:

no clock timezone

Input mode

`(config)`

Parameters

<*zone name*>

Specifies the name used to identify a time zone.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   A maximum of seven alphanumeric characters

<*hours offset*>

Specifies the offset from UTC in hours as a decimal integer.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   -12 to -1, 0, and 1 to 12 (hours)

<*minutes offset*>

Specifies the offset from UTC in minutes as a decimal integer.

1. Default value when this parameter is omitted:

   0

2. Range of values:

   0 to 59 (minutes)

Default behavior

UTC is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

set clock

show clock

show logging

ntp access-group

Creates an access group that can be permitted or denied access to NTP services by means of an IPv4 address filter. This command allows you to set a maximum of 740 filtering condition entries for an access list.

Syntax

To set information:

ntp access-group {query-only | serve-only | serve | peer} {<*access list number*> | <*access list name*>} [vrf <*vrf id*>]

To delete information:

no ntp access-group {query-only | serve-only | serve | peer} [vrf <*vrf id*>]

Input mode

`(config)`

Parameters

{query-only | serve-only | serve | peer}

Sets the mode in which an NTP services are used.

query-only

Only NTP control queries are permitted.

serve-only

NTP control queries and NTP broadcast messages are not permitted.

serve

NTP broadcast messages are not permitted.

peer

All accesses to NTP services are permitted.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `query-only`, `serve-only`, `serve`, or `peer`

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

Specifies the number or the name of an access list that specifies IPv4 addresses which are permitted or denied access to the NTP service.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*access list number*>, specify values from 1 to 99, or from 1300 to 1999 (in decimal).

   For <*access list name*>, specify a name that is no more than 31 characters.

   For details, see *Specifiable values for parameters*.

vrf <*vrf id*> [OP-NPAR]

Specifies VRF to which an IPv4 address filter is applied.

1. Default value when this parameter is omitted:

   An IPv4 address filter is applied to the global network.

2. Range of values:

   For <*vrf id*>, specify a VRF ID.

   For details, see *Specifiable values for parameters*.

Default behavior

All accesses to NTP services are permitted.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed if `ntp peer`, `ntp server`, `ntp master`, or `ntp broadcast client` is set and an IPv4 address filter is set.

Notes

1. Access lists specified by this command are not subject to implicit discard entries.
2. In a VRF instance or a global network, if at least one access group is created, any accesses with a source IP address that does not match the specified access list are denied.
3. When the source IP address matches access lists for multiple access types, access type keywords are applied according to the following priority:

   `peer` -> `serve` -> `serve-only` -> `query-only`

Related commands

ntp peer

ntp server

access-list

ip access-list

ntp authenticate

Enables the NTP authentication functionality.

Syntax

To set information:

```
ntp authenticate
```

To delete information:

```
no ntp authenticate
```

Input mode

`(config)`

Parameters

None

Default behavior

The NTP authentication functionality is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed if `ntp peer`, `ntp server`, `ntp master`, or `ntp broadcast client` is set.

Notes

None

Related commands

ntp authentication-key

ntp trusted-key

ntp authentication-key

Sets an authentication key. This command can set a maximum of 10 authentication key entries.

Syntax

To set or change information:

ntp authentication-key <*key id*> md5 <*value*>

To delete information:

no ntp authentication-key <*key id*>

Input mode

`(config)`

Parameters

<*key id*>

Specifies the key number in decimal.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

md5 <*value*>

Specifies a value to be assigned to an authentication key.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   A maximum of 30 ASCII characters

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed if `ntp peer`, `ntp server`, `ntp master`, or `ntp broadcast client` is set.

Notes

1. For some destination devices, the range of available authentication keys might be less than 32 bits. In this case, set the value of a key to use to a value within the valid range of the destination device.
2. Do not specify 65536 or a larger value as the key number.

Related commands

ntp peer

ntp server

ntp master

ntp authenticate

ntp trusted-key

ntp broadcast client

ntp broadcast

Broadcasts NTP packets to each interface and synchronizes other devices with the Switch.

This command can be used together with the `ntp peer` and `ntp server` commands to specify a maximum of 10 entries in total.

Syntax

To set or change information:

ntp broadcast [version <*number*>] [key <*key id*>]

To delete information:

no ntp broadcast

Input mode

`(config-if)`

Parameters

version <*number*>

Specifies the NTP version number.

1. Default value when this parameter is omitted:

   Version 4 is specified by default. If you prefer to use the default value, do not set this parameter.

2. Range of values:

   1, 2, or 3

key <*key id*>

Specifies the authentication key for access. Specify `key` as the number (in decimal) set for `authentication-key`.

1. Default value when this parameter is omitted:

   No authentication keys are specified.

2. Range of values:

   1 to 65535

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed if `ntp peer`, `ntp server`, `ntp master`, or `ntp broadcast client` is set.

Notes

1. This functionality can use IPv4 only.
2. If no IPv4 addresses are set for an interface, no NTP broadcast packets are sent.
3. To change IPv4 address settings of an interface, delete the `ntp broadcast` setting first.

4. Do not specify 65536 or a larger value as the key number.

Related commands

ntp broadcast client

ntp authentication-key

ntp broadcast client

Specifies the setting for accepting NTP broadcast messages from devices on the connected subnet. This setting enables the Switch to receive NTP broadcast messages from other switches and synchronize its time with that of other switches. When this command is omitted, no NTP broadcast messages are accepted.

Syntax

To set information:

```
ntp broadcast client
```

To delete information:

```
no ntp broadcast client
```

Input mode

`(config)`

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you adjust the Switch's clock when scheduled power saving is in use, the adjustment might not be reflected in the schedule until the length of the time that has been adjusted (or up to 30 minutes) lapses. [AX6700S] [AX6600S]

Related commands

ntp broadcast

ntp broadcastdelay

Specifies the estimated latency (time delay) between the NTP broadcast server sending time information and the Switch.

Syntax

To set or change information:

ntp broadcastdelay <*micro seconds*>

To delete information:

no ntp broadcastdelay

Input mode

`(config)`

Parameters

<*micro seconds*>

Specifies a delay time. The time is set as a decimal integer in microseconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 999999

Default behavior

4000 microseconds are set as the delay time of the NTP broadcast server.

Impact on communication

None

When the change is applied

When the `ntp broadcast client` command is set, the change takes effect immediately after the setting value is changed.

Notes

None

Related commands

ntp broadcast client

ntp master

Designates the switch as a local time server. Perform this setting if a reference NTP server cannot be accessed from the network to which the Switch is normally connected.

Syntax

To set or change information:

ntp master [<*stratum*>]

To delete information:

no ntp master

Input mode

```
(config)
```

Parameters

<*stratum*>

Specifies the stratum value in decimal.

1. Default value when this parameter is omitted:

   8

2. Range of values:

   1 to 15

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you use the Switch as an NTP server, and 10 or more clients are to be synchronized, synchronization might be temporarily disabled. Although the Switch functionality is not affected even if the number of clients to be synchronized exceeds 10, consider your environment when deciding the number of clients.
2. If 16 or a larger value is set as the stratum value, the Switch assumes that the stratum value is 15.

Related commands

ntp peer

ntp server

ntp peer

Configures NTP server symmetric active/passive mode. In symmetric active/passive mode, the time of the Switch can be synchronized with that of other switches, and vice versa.

This command can be used together with the `ntp broadcast` and `ntp server` commands to specify a maximum of 10 entries in total.

Syntax

To set or change information:

ntp peer [vrf <*vrf id*>] <*ip address*> [version <*number*>] [key <*key id*>] [prefer]

To delete information:

no ntp peer [vrf <*vrf id*>] <*ip address*>

Input mode

`(config)`

Parameters

vrf <*vrf id*> [OP-NPAR]

Specifies the VRF of an NTP time source (time reference) Switch or an NTP client Switch.

1. Default value when this parameter is omitted:

   Belongs to the global network.

2. Range of values:

   For <*vrf id*>, specify a VRF ID.

   For details, see *Specifiable values for parameters*.

<*ip address*>

Specifies the IPv4 address of an NTP time source (time reference) Switch or an NTP client Switch.

version <*number*>

Specifies the NTP version number.

1. Default value when this parameter is omitted:

   Version 4 is specified by default. If you prefer to use the default value, do not set this parameter.

2. Range of values:

   1, 2, or 3

key <*key id*>

Specifies the authentication key for access. Specify `key` as the number (in decimal) set for `authentication-key`.

1. Default value when this parameter is omitted:

   No authentication keys are specified.

2. Range of values:

   1 to 65535

prefer

When multiple time reference source switches are specified, a switch with the `prefer` parameter specified takes priority.

1. Default value when this parameter is omitted:

   No priorities are set.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If there is a 1000 second (about 16 minute) or longer difference between the time of a time reference source (server) switch and the time of this (client) Switch, the specified switch time is treated as invalid (not reconcilable) and it is not synchronized. If the time of the time-reference synchronization-source switch is correct, use the `set clock` operation command to synchronize the time of this Switch to the time of the time-reference synchronization-source switch.
2. In a configuration where this Switch references multiple time-reference synchronization-source switches, if there is a 16 second or longer time difference between the time references, synchronization of this Switch (that references the other switches) will succeed, but any switches that reference this switch will not be synchronized. Make sure the time of specified time-reference synchronization-source switches is correct.
3. If the Switch and other switches are configured in symmetric active/passive mode, it might take a very long time to synchronize these switches. If this happens, we recommend that you reduce the number of switches in the configuration.
4. When a switch references multiple time-reference synchronization-source switches, if the time of a high-priority synchronization-source switch moves outside of the synchronization range (a 1000 second or longer time difference), other synchronization-source switches will be used as the time reference. If this situation is not fixed, synchronization with the other switches might also be lost. You can change the settings to manually disable the synchronization-source designation of the switch whose time has moved out of the valid range. Another solution in this case is to manually reset the time of such a switch to the correct value, and synchronization will be recovered.
5. If the IP address of a switch is configured as that of its loopback interface, use the IP address of the loopback interface as the source IP address for sending NTP packets. Therefore, if you set the Switch as the synchronization source or destination, specify the IP address of the loopback interface as the IP address of the Switch. When adding, changing, or deleting the IP address of the loopback interface, use the `restart ntp` operation command to re-initialize the ntp program.
6. If you adjust the Switch's clock when scheduled power saving is in use, the adjustment might not be reflected in the schedule until the length of the time that has been adjusted (or up to 30 minutes) lapses. [AX6700S] [AX6600S]
7. Do not specify 65536 or a larger value as the key number.

Related commands

ntp server

ntp authentication-key

ntp server

Configures client/server mode and specifies client mode for an NTP server. As a result, the time of this Switch is synchronized to that of a time server. The time of this Switch can be synchronized to that of another switch, but the time of another switch cannot be synchronized to that of this Switch.

This command can be used together with the `ntp broadcast` and `ntp peer` commands to specify a maximum of 10 entries in total.

Syntax

To set or change information:

ntp server [vrf <*vrf id*>] <*ip address*> [version <*number*>] [key <*key id*>] [prefer]

To delete information:

no ntp server [vrf <*vrf id*>] <*ip address*>

Input mode

`(config)`

Parameters

vrf <*vrf id*> [OP-NPAR]

Specifies VRF to which a Switch whose time is to be synchronized belongs.

1. Default value when this parameter is omitted:

   Belongs to the global network.

2. Range of values:

   For <*vrf id*>, specify a VRF ID.

   For details, see *Specifiable values for parameters*.

<*ip address*>

Specifies the IPv4 address of a Switch whose time is to be synchronized.

version <*number*>

Specifies the NTP version number.

1. Default value when this parameter is omitted:

   Version 4 is specified by default. If you prefer to use the default value, do not set this parameter.

2. Range of values:

   1, 2, or 3

key <*key id*>

Specifies the authentication key for access. Specify `key` as the number (in decimal) set for `authentication-key`.

1. Default value when this parameter is omitted:

   No authentication keys are specified.

2. Range of values:

   1 to 65535

prefer

When multiple time reference source switches are specified, a switch with the `prefer` parameter specified takes priority.

1. Default value when this parameter is omitted:

   No priorities are set.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If there is a 1000 second (about 16 minute) or longer difference between the time of a time reference source (server) switch and the time of this (client) Switch, the specified switch time is treated as invalid (not reconcilable) and it is not synchronized. If the time of the time-reference synchronization-source switch is correct, use the `set clock` operation command to synchronize the time of this Switch to the time of the time-reference synchronization-source switch.
2. In a configuration where this Switch references multiple time-reference synchronization-source switches, if there is a 16 second or longer time difference between the time references, synchronization of this Switch (that references the other switches) will succeed, but any switches that reference this switch will not be synchronized. Make sure the time of specified time-reference synchronization-source switches is correct.
3. If the IP address of a switch is configured as that of its loopback interface, use the IP address of the loopback interface as the source IP address for sending NTP packets. Therefore, if you set the Switch as the synchronization source or destination, specify the IP address of the loopback interface as the IP address of the Switch. When adding, changing, or deleting the IP address of the loopback interface, use the `restart ntp` operation command to re-initialize the ntp program.
4. If you adjust the Switch's clock when scheduled power saving is in use, the adjustment might not be reflected in the schedule until the length of the time that has been adjusted (or up to 30 minutes) lapses. [AX6700S] [AX6600S]
5. Do not specify 65536 or a larger value as the key number.

Related commands

ntp peer

ntp authentication-key

ntp trusted-key

Sets a security key number to perform authentication for security purposes when synchronizing with other switches. By default, the key to be used for authentication is not set. This command can be used to set a maximum of 10 key number entries.

Syntax

To set information:

ntp trusted-key <*key id*>

To delete information:

no ntp trusted-key <*key id*>

Input mode

`(config)`

Parameters

<*key id*>

Specifies the key number to be used for authentication. For this key, the number (in decimal) set by using `authentication-key` is specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed if `ntp peer`, `ntp server`, `ntp master`, or `ntp broadcast client` is set.

Notes

1. Do not specify 65536 or a larger value as the key number.

Related commands

ntp authenticate

ntp authentication-key

Chapter

8. Host Names and DNS

ip domain lookup

Enables or disables the DNS resolver functionality.

Syntax

To set information:

```
no ip domain lookup
```

To delete information:

```
ip domain lookup
```

Input mode

`(config)`

Parameters

None

Default behavior

The DNS resolver functionality is enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

hostname

ip domain name

ip name-server

ping

traceroute

telnet

ip domain name

Sets the domain name to be used by the DNS resolver.

Syntax

To set or change information:

ip domain name <*domain name*>

To delete information:

no ip domain name

Input mode

`(config)`

Parameters

<*domain name*>

Sets the domain name for the Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   No more than 63 alphanumeric characters, periods (.), and hyphens (-) can be used.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

If `no ip domain lookup` is set, the change is applied to operation after `ip domain lookup` is entered.

Notes

1. Only one domain name can be set for the Switch.

Related commands

hostname

ip name-server

ip domain lookup

ip domain reverse-lookup

Disables or enables the reverse lookup functionality (functionality for using an IP address to search for a host name) of the DNS resolver functionality.

Syntax

To set information:

```
no ip domain reverse-lookup
```

To delete information:

```
ip domain reverse-lookup
```

Input mode

`(config)`

Parameters

None

Default behavior

When the DNS resolver functionality is enabled, the reverse lookup functionality is also enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the DNS resolver functionality is disabled, it does not operate regardless of this setting.
2. If the reverse lookup functionality of the DNS resolver functionality is disabled by this setting, a host name might not be displayed for the `traceroute` or the `show ntp associations` operation commands.

Related commands

ip domain lookup

ip domain name

ip name-server

traceroute

show ntp association

ip host

Sets host name information mapped to an IPv4 address. This command can configure a maximum of 20 entries.

Syntax

To set or change information:

ip host <*name*> <*ip address*>

To delete information:

no ip host <*name*>

Input mode

`(config)`

Parameters

<*name*>

Specifies a host name to be assigned to an IPv4 address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specifies a host name with no more than 63 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

<*ip address*>

Specifies the IPv4 address of a switch for which a host name is set in dot notation.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. `localhost` cannot be set as a host name.
2. `127.*.*.*` cannot be set as an IPv4 address.
3. A class D or class E IPv4 address cannot be set.
4. Host names are not case sensitive.
5. If the same host name is specified for the `ip host` command and the `ipv6 host` command, the `ip host` command takes priority.

Related commands

ping

traceroute

telnet

ip name-server

Sets the name server referenced by the DNS resolver. A maximum of three name servers can be specified. If multiple name servers are specified, inquiries to the name servers are performed in the order in which they were set. Because the DNS resolver functionality is enabled by default, it works as soon as the name server has been set.

Syntax

To set information:

ip name-server <*ip address*>

To delete information:

no ip name-server <*ip address*>

Input mode

`(config)`

Parameters

<*ip address*>

Specifies the IPv4 address of a name server in dot notation.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

If `no ip domain lookup` is set, the change is applied to operation after `ip domain lookup` is entered.

Notes

1. Set the IP address (`ip name-server`) of the DNS server correctly. If the IP address of a DNS server is not set correctly, it might take time until a communication failure with the DNS server is detected when a host name is referenced, and operation might be affected (Example: It takes time until the login prompt appears when a remote connection is established from another switch to the Switch via Telnet).

   One way to check the DNS server status is to use the `nslookup` command as shown below.

   ```
   nslookup -retry=1 <name of host to be referenced> [<IP address of DNS server>]
   ```

   If the IP address of a DNS server is correct, information about the specified host is displayed as shown below.

   ```
   Server: <host name of DNS server>
   Address: <IP address of DNS server>
   Name: <name of specified host>
   Address: <IP address of specified host>
   ```

   If the IP address of the DNS server is not correct, the following is displayed:

   ```
   *** Can't find server name for address <IP address of DNS server>: Timed out
   ```

2. `127.*.*.*` cannot be specified as an IP address.
3. Class D and class E addresses cannot be set as IP addresses.
4. AAAA query information cannot be referenced by using IPv6. AAAA query information is referenced by IPv4.

Related commands

ip domain name

ip domain lookup

ipv6 host

Sets host name information mapped to an IPv6 address. This command can configure a maximum of 20 entries.

Syntax

To set or change information:

ipv6 host <*name*> <*ipv6 address*>

To delete information:

no ipv6 host <*name*>

Input mode

`(config)`

Parameters

<*name*>

Specifies a host name to be assigned to an IPv6 address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specifies a host name with no more than 63 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

<*ipv6 address*>

Specifies the IPv6 address of a switch for which a host name is set in colon notation.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. `localhost` cannot be set as a host name.
2. Host names are not case sensitive.
3. If the same host name is specified for the `ipv6 host` command and the `ip host` command, the `ip host` command takes priority.

Related commands

ping ipv6

traceroute ipv6

telnet

Chapter

9. Device Management

fldm prefer

Sets the flow distribution pattern for filtering and the QoS functionality, and whether to specify flow detection extended mode.

This command changes the distribution pattern for the maximum number of entries in a hardware table for a switch. By changing the allocation pattern according to the operating mode, you can collect hardware resource information in the necessary tables and use it.

Because this command is used to configure the basic operating conditions of the hardware, make sure you set this command during the first stage of actual operation. We recommend that you do not make any changes during operation.

Syntax

To set or change information:

fldm prefer default {standard | standard-advance}

fldm prefer {default | filter-only | qos-only | filter | qos} {extended | extended-advance}

Input mode

```
(config)
```

Parameters

default

For the standard flow distribution pattern, sets the equal-distribution pattern for the filter and Qos.

For details about the flow distribution pattern, see *Configuration Guide Vol. 1 For Version 11.7*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

{standard | standard-advance}

For the standard flow distribution pattern, sets whether to specify flow detection extended mode.

standard

Sets the standard flow distribution pattern. Flow detection extended mode is not set.

standard-advance

Sets the standard flow distribution pattern, and then sets flow detection extended mode.

For details about the flow detection extended mode, see *Configuration Guide Vol. 2 For Version 11.7*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

For AX6700S series switches:

The following table shows the BSU types that can use this parameter.

Table 9-1: Use of standard and standard-advance as determined by BSU type

BSU type	Whether standard or standard-advance can be used
BSU-LA	Y
BSU-LB	N

Legend Y: Can be used; N: Cannot be used

For AX6600S series switches:

The following table shows the CSU types that can use this parameter.

Table 9-2: Use of standard and standard-advance as determined by CSU type

CSU type	Whether standard or standard-advance can be used
CSU-1A	Y
CSU-1B	N

Legend Y: Can be used; N: Cannot be used

For AX6300S series switches:

The following table shows the MSU types that can use this parameter.

Table 9-3: Use of standard and standard-advance as determined by MSU type

MSU type	Whether standard or standard-advance can be used
MSU-1A and MSU-1A1	Y
MSU-1B and MSU-1B1	N

Legend Y: Can be used; N: Cannot be used

{default | filter-only | qos-only | filter | qos }

Specifies the advanced flow distribution pattern.

default

Sets the equal-distribution pattern for the filter and QoS.

filter-only

Sets the distribution pattern only for the filter.

qos -only

Sets the distribution pattern only for QoS.

filter

Sets the filter-oriented distribution pattern.

qos

Sets the QoS-oriented distribution pattern.

For details about the flow distribution pattern, see *Configuration Guide Vol. 1 For Version 11.7*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

{extended | extended-advance}

For the advanced flow distribution pattern, sets whether to specify flow detection extended mode.

extended

Sets the advanced flow distribution pattern. Flow detection extended mode is not set.

extended-advance

Sets the advanced flow distribution pattern and then sets the flow detection extended mode.

For details about the flow detection extended mode, see *Configuration Guide Vol. 2 For Version 11.7*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

For AX6700S series switches:

The following table shows the BSU types that can use this parameter.

Table 9-4: Use of extended and extended-advance as determined by BSU type

BSU type	Whether extended or extended-advance can be used
BSU-LA	N
BSU-LB	Y

Legend Y: Can be used; N: Cannot be used

For AX6600S series switches:

The following table shows the CSU types that can use this parameter.

Table 9-5: Use of extended and extended-advance as determined by CSU type

CSU type	Whether extended or extended-advance can be used
CSU-1A	N
CSU-1B	Y

Legend Y: Can be used; N: Cannot be used

For AX6300S series switches:

The following table shows the MSU types that can use this parameter.

Table 9-6: Use of extended and extended-advance as determined by MSU type

MSU type	Whether extended or extended-advance can be used
MSU-1A and MSU-1A1	N
MSU-1B and MSU-1B1	Y

Legend Y: Can be used; N: Cannot be used

Default behavior

For AX6700S series switches:

A distribution pattern from the following table is set according to the BSU type at initial startup.

Table 9-7: Distribution patterns at initial startup time, as determined by BSU type

BSU type	Distribution pattern
BSU-LA	default standard
BSU-LB	default extended

For AX6600S series switches:

A distribution pattern from the following table is set according to the CSU type at initial startup.

Table 9-8: Distribution patterns at initial startup time, as determined by CSU type

CSU type	Distribution pattern
CSU-1A	default standard
CSU-1B	default extended

For AX6300S series switches:

A distribution pattern from the following table is set according to the MSU type at initial startup.

Table 9-9: Distribution patterns at initial startup time, as determined by MSU type

MSU type	Distribution pattern
MSU-1A and MSU-1A1	default standard
MSU-1B and MSU-1B1	default extended

Impact on communication

For AX6700S series switches:

Because BSU must restart, communication via the Switch stops until the startup process completes.

For AX6600S and AX6300S series switches:

Because PSP must restart, communication via the Switch stops until the startup process completes.

When the change is applied

For AX6700S series switches:

After the setting value is changed, if you enter `y` for a yes or no confirmation message and BSU restarts automatically, the change is applied.

For AX6600S and AX6300S series switches:

After the setting value is changed, if you enter `y` for a yes or no confirmation message and PSP restarts automatically, the change is applied.

Notes

1. Flow detection extended mode can be specified when MAC mode is not specified.
2. To change the flow distribution pattern, the number of configured entries must be within the number of configured entries after the change.
3. Note that BSU does not start if you set a parameter that cannot be used by the BSU type.
4. Note that CSU does not operate properly if you set a parameter that cannot be used by the CSU type.
5. Note that MSU does not operate properly if you set a parameter that cannot be used by the MSU type.
6. Depending on whether or not DHCP snooping is set, the number of specifiable filter entries varies. For details, see *Configuration Guide Vol. 1 For Version 11.7*.

Related commands

None

fwdm prefer

Sets the distribution pattern for the maximum number of entries per switch for the IPv4 unicast active route, IPv4 multicast route, IPv6 unicast active route, IPv6 multicast route, MAC address entries, ARP entries, and NDP entries. With this setting, operation can be performed with a set number of entries for each operation mode.

Because this command is used to configure the basic operating conditions of the Switch, make sure you set this command before starting actual operation.

Syntax

To set or change information:

fwdm prefer {default | ipv4-uni | ipv4-ipv6-uni | vlan} {standard | extended}

Input mode

`(config)`

Parameters

{default | ipv4-uni | ipv4-ipv6-uni | vlan}

Sets the distribution pattern for the IPv4 unicast active route, IPv4 multicast route, IPv6 unicast active route, IPv6 multicast route, MAC address entries, ARP entries, and NDP entries.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

{standard | extended}

Specifies the type of BSU, CSU, or MSU.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

For AX6700S series switches:

The following table shows the BSU types that can use this parameter.

Table 9-10: Specifiable parameters as determined by BSU type

BSU type	Parameter
BSU-LA	standard
BSU-LB	extended

For AX6600S series switches:

The following table shows the CSU types that can use this parameter.

Table 9-11: Specifiable parameters as determined by CSU type

CSU type	Parameter
CSU-1A	standard
CSU-1B	extended

For AX6300S series switches:

The following table shows the MSU types that can use this parameter.

Table 9-12: Specifiable parameters as determined by MSU type

MSU type	Parameter
MSU-1A and MSU-1A1	standard
MSU-1B and MSU-1B1	extended

The following table shows distribution patterns for combinations of parameters.

Table 9-13: Distribution pattern for standard

Distribution pattern	Number of entries that can be set						
	IPv4 unicast active route	IPv4 multicast route	IPv6 unicast active route	IPv6 multicast route	MAC address entries	ARP entries	NDP entries
default	32768	4000	16384	1000	24576	12288	12288
ipv4-uni	65536	0	0	0	24576	12288	0
ipv4-ipv6-uni	32768	0	32768	0	24576	12288	12288
vlan	8192	0	8192	0	49152	8192	8192

Table 9-14: Distribution pattern for extended

Distribution pattern	Number of entries that can be set						
	IPv4 unicast active route	IPv4 multicast route	IPv6 unicast active route	IPv6 multicast route	MAC address entries	ARP entries	NDP entries
default	65536	8000	32768	8000	65536	24576	24576
ipv4-uni	212992	0	0	0	24576	24576	0
ipv4-ipv6-uni	106496	0	106496	0	24576	24576	24576
vlan	8192	0	8192	0	122880	8192	8192

Default behavior

For AX6700S series switches:

A distribution pattern from the following table is set according to the BSU type at initial startup.

Table 9-15: Distribution patterns at initial startup time, as determined by BSU type

BSU type	Distribution pattern
BSU-LA	default standard
BSU-LB	default extended

For AX6600S series switches:

A distribution pattern from the following table is set according to the CSU type at initial startup.

Table 9-16: Distribution patterns at initial startup time, as determined by CSU type

CSU type	Distribution pattern
CSU-1A	default standard
CSU-1B	default extended

For AX6300S series switches:

A distribution pattern from the following table is set according to the MSU type at initial startup.

Table 9-17: Distribution patterns at initial startup time, as determined by MSU type

MSU type	Distribution pattern
MSU-1A and MSU-1A1	default standard
MSU-1B and MSU-1B1	default extended

Impact on communication

For AX6700S series switches:

Because BSU must restart, communication via the Switch stops until the startup process completes.

For AX6600S and AX6300S series switches:

Because PSP must restart, communication via the Switch stops until the startup process completes.

When the change is applied

For AX6700S series switches:

After the setting value is changed, if you enter `y` for a yes or no confirmation message and BSU restarts automatically, the change is applied.

For AX6600S and AX6300S series switches:

After the setting value is changed, if you enter `y` for a yes or no confirmation message and PSP restarts automatically, the change is applied.

Notes

1. When using this parameter, some protocols (functionalities) might have no entries depending on the distribution pattern you set (for example, IPv4 multicast route for `ipv4-ipv6-uni`, or IPv6 multicast route). In this case, communication is not possible, even if such protocols (functionalities) are configured.
2. Note that BSU does not start if you set a parameter that cannot be used by the BSU type.

3. Note that CSU does not operate properly if you set a parameter that cannot be used by the CSU type.
4. Note that MSU does not operate properly if you set a parameter that cannot be used by the MSU type.

Related commands

None

system fan mode

Sets the operating mode of the fan.

Syntax

To set or change information:

system fan mode <*mode*>

To delete information:

no system fan mode

Input mode

```
(config)
```

Parameters

<*mode*>

Specify operating mode 1 or 2 for the fan.

1: Low-noise setting

2: Low-temperature setting

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 and 2

Default behavior

1: The low-noise setting is specified.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

system hardware-mode

This command changes the hardware mode of a switch according to the functionality it uses. Because this command is used to configure the basic operating conditions of the hardware, make sure you set this command during the first stage of actual operation. We recommend that you do not make any changes during operation.

Syntax

To set information:

system hardware-mode access-log

To delete information:

no system hardware-mode

Input mode

`(config)`

Parameters

access-log

Sets access list logging-compatible hardware mode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The following functionality cannot be used.

- Access list logging

Impact on communication

If `access-log` is specified for the parameter, communication via the Switch stops temporarily until the hardware mode finishes applying.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

system recovery

When a failure occurs in a switch, no recovery is performed for the failed part, which will remain stopped after the failure occurs. The parts below are covered by this functionality.

- For AX6700S series switches:

  BCUs, BSUs, and NIFs. The applicable BSUs and NIFs are turned off.
- For AX6600S series switches:

  CSUs and NIFs. The applicable NIFs are turned off.
- For AX6300S series switches:

  MSUs and NIFs. The applicable NIFs are turned off.

Syntax

To set information:

no system recovery

To delete information:

system recovery

Input mode

`(config)`

Parameters

None

Default behavior

Recovery is performed and failed parts are re-initialized.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Because the status LEDs for the applicable BSUs and NIFs are turned off, use the following commands to diagnose failure locations:
   - `show system` command
   - `show nif` command
2. If failures are found in a BSU or NIF, the power for the applicable board is not turned off even if the `system recovery` command is set. To turn off the power, execute the `no power enable` command or the `inactivate` command. Note that the board is not recovered by these commands.

Related commands

None

system temperature-warning-level

Outputs an operation message when the intake temperature of the switch exceeds the specified temperature.

Syntax

To set information:

system temperature-warning-level <*temperature*>

To delete information:

no system temperature-warning-level

Input mode

`(config)`

Parameters

<*temperature*>

Specify the intake air temperature (in Celsius) for the switch.

You can specify the temperature in degrees Celsius.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   25 to 40

Default behavior

An operation message is not output when the specified temperature is exceeded.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

If the intake temperature of the switch has already exceeded the specified temperature, an operation message is immediately output.

Related commands

None

Chapter

10. BSU/NIF Management

power enable
system nif-hdc restart
system nif-hdc software-bundle

power enable

Disables a BSU or NIF board. Also turns off the board's power.

Syntax

To set information:

no power enable {bsu <*bsu no.*> | nif <*nif no.*>} [AX6700S]

no power enable nif <*nif no.*> [AX6600S] [AX6300S]

To delete information:

power enable {bsu <*bsu no.*> | nif <*nif no.*>} [AX6700S]

power enable nif <*nif no.*> [AX6600S] [AX6300S]

Input mode

`(config)`

Parameters

bsu <*bsu no.*> [AX6700S]

Specifies the BSU number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3

nif <*nif no.*>

Specifies a NIF number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

A BSU or NIF board operates in the status other than disable. For details about operating status of BSUs, see the description for the `show system` operation command. For details about the status of NIFs, see the description for the `show nif` operation command.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When a Switch is operating in a redundant configuration and the standby BSU is in cold standby status, if this configuration is set for the active BSU, the BSU status is changed to inactive. However, communication continues until the standby BSU becomes active. [AX6700S]
2. When the scheduled power saving functionality is in operation, the device operates according

to the configuration of the `schedule-power-control shutdown` command. [AX6700S] [AX6600S]

Related commands

None

system nif-hdc restart

Sets NIF control software (HDC: Hardware Dependent Code) so that it is not updated automatically during a system switchover. When updating HDC, execute the `inactivate` and `activate` operation commands for the applicable NIF, and then restart the Switch.

Syntax

To set information:

no system nif-hdc restart

To delete information:

system nif-hdc restart

Input mode

`(config)`

Parameters

None

Default behavior

HDC for NIFs is updated automatically.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is set or deleted, HDC for the applicable NIF is not updated and the Switch is not restarted. To update HDC, execute the `inactivate` and `activate` operation commands for the applicable NIF, and then restart the Switch.

Related commands

system nif-hdc software-bundle

system nif-hdc software-bundle

When switching systems, if NIF is in the active status, and if the version of the NIF control software (HDC: Hardware Dependent Code) is later than the bundled HDC, the software is not updated to the bundled HDC and operation continues.

Syntax

To set information:

no system nif-hdc software-bundle

To delete information:

system nif-hdc software-bundle

Input mode

`(config)`

Parameters

None

Default behavior

HDC is updated to the bundled HDC.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is set or deleted, HDC for the applicable NIF is not updated and the Switch is not restarted. To update HDC, execute the `inactivate` and `activate` operation commands for the applicable NIF, and then restart the Switch.

Related commands

system nif-hdc restart

Chapter

11. Power Saving Functionality

adaptive-power-control decrease-traffic-debounce [AX6700S] [AX6600S]

Specifies the monitoring interval before the traffic-based power saving functionality is turned on.

Syntax

To set or change information:

adaptive-power-control decrease-traffic-debounce <*minutes*>

To delete information:

no adaptive-power-control decrease-traffic-debounce

Input mode

```
(config)
```

Parameters

<*minutes*>

Specifies in minutes the monitoring interval before the traffic-based power saving functionality is turned on.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   60 to 360 (minutes)

Default behavior

60 (minutes) is set as the monitoring interval before the traffic-based power saving functionality is turned on.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

adaptive-power-control enable

adaptive-power-control enable [AX6700S] [AX6600S]

Enables the traffic-based power saving functionality.

Syntax

To set information:

adaptive-power-control enable

To delete information:

no adaptive-power-control enable

Input mode

`(config)`

Parameters

None

Default behavior

Disables the traffic-based power saving functionality.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command can be set when `redundancy bsu-load-balancing smac`, `redundancy bsu-mode fixed`, `redundancy standby-bsu cold`, `schedule-power-control time-range`, and `power-control mode1` are not set.

Related commands

None

adaptive-power-control increase-traffic-debounce [AX6700S] [AX6600S]

Specifies the monitoring interval before the traffic-based power saving functionality is turned off.

Syntax

To set or change information:

adaptive-power-control increase-traffic-debounce <*minutes*>

To delete information:

no adaptive-power-control increase-traffic-debounce

Input mode

```
(config)
```

Parameters

<*minutes*>

Specifies in minutes the monitoring interval before the traffic-based power saving functionality is turned off.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 360 (minutes)

Default behavior

1 (minute) is set as the monitoring interval before the traffic-based power saving functionality is turned off.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

adaptive-power-control enable

adaptive-power-control max-bsu [AX6700S]

Sets the number of BSUs to be used when the traffic-based power saving functionality is in use.

Syntax

To set or change information:

adaptive-power-control max-bsu <*max bsu*>

To delete information:

no adaptive-power-control max-bsu

Input mode

`(config)`

Parameters

<*max bsu*>

Sets the number of active BSUs. If a larger value is set, packet forwarding performance is improved.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3

Default behavior

Only one BSU is set to active and the others to standby.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

adaptive-power-control enable

adaptive-power-control max-psp [AX6600S]

Sets the number of PSPs to be used when the traffic-based power saving functionality is in use.

Syntax

To set or change information:

adaptive-power-control max-psp <*max psp*>

To delete information:

no adaptive-power-control max-psp

Input mode

```
(config)
```

Parameters

<*max psp*>

Sets the number of active PSPs. If a larger value is set for the number of PSPs, packet forwarding performance is improved.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 2

Default behavior

Sets one PSP to standby and the other to active.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

adaptive-power-control enable

adaptive-power-control mode [AX6700S] [AX6600S]

Sets the power control mode when the traffic-based power saving functionality is in use. BSU/PSP power control allows you to reduce the power required for forwarding packets.

If the number of operating BSUs/PSPs is one, the power control mode for BSU/PSP is not changed. When changing the power control mode for BSU/PSPs while using the traffic-based power saving functionality, set the number of BSUs/PSPs to two or a larger value.

Syntax

To set or change information:

adaptive-power-control mode {normal | mode2}

To delete information:

no adaptive-power-control mode

Input mode

```
(config)
```

Parameters

{normal | mode2}

normal

Operates with normal power consumption.

mode2

- For AX6700S series switches:

  Operates with lower BSU power consumption.
- For AX6600S series switches:

  Operates with lower PSP power consumption.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.
2. Range of values:

   normal, mode2

Default behavior

For AX6700S series switches:

Operates with lower BSU power consumption.

For AX6600S series switches:

Operates with lower PSP power consumption.

Impact on communication

Depending on the operating status of the power saving functionality, communication is affected as described in the following table.

Table 11-1: Effect on user communication

Operating status when settings or changes are made	Number of BSUs/ PSPs	Impact on communication
Traffic-based power saving functionality is disabled.	1 to 3	None
Traffic-based power saving functionality is enabled.	1	A BSU or PSP is re-initialized and communication stops until the startup process completes.
	2 to 3	None#

#: When the number of operating BSUs/PSPs is two or more, but no standby BSUs/PSPs exist, if the power control mode is changed, the BSUs/PSPs operate at a reduced switching capacity. As a result, communication might temporarily stop.

When the change is applied

For AX6700S series switches:

After the setting value is changed, if you enter `y` for a yes or no confirmation message, the changes are applied. After a yes or no confirmation message, if the BSU and the NIF must be restarted, they restart automatically and the changes are applied.

For AX6600S series switches:

After the setting value is changed, if you enter `y` for a yes or no confirmation message, the changes are applied. After a yes or no confirmation message, if the PSP and the NIF must be restarted, they restart automatically and the changes are applied.

Notes

None

Related commands

adaptive-power-control enable

adaptive-power-control port-led [AX6700S] [AX6600S]

Sets LED operation of a port when traffic-based power saving functionality is in use.

Syntax

To set or change information:

adaptive-power-control port-led {enable | disable}

To delete information:

no adaptive-power-control port-led

Input mode

```
(config)
```

Parameters

{enable | disable}

enable

Turns on the port LED according to the operating status.

disable

Turns off the port LED regardless of the operating status. If a key on the system operation panel of the active system is used, the port LED temporarily turns on according to the operating status. If no keys are used for 60 seconds, the LED turns off.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   enable, disable

Default behavior

Turns off the port LED regardless of the operating status.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

adaptive-power-control enable

adaptive-power-control standby-bsu [AX6700S]

Sets the operating mode for the standby BSU when traffic-based power saving functionality is in use.

Syntax

To set or change information:

```
adaptive-power-control standby-bsu {hot | cold2}
```

To delete information:

```
no adaptive-power-control standby-bsu
```

Input mode

`(config)`

Parameters

{hot | cold2}

hot

Powers on the standby BSU, and switches between the active and standby BSUs if a failure occurs.

cold2

Fully powering off the standby BSU allows you to reduce its power consumption to almost zero. If a failure occurs in an active BSU, the standby BSU starts automatically, and the BSUs are switched. Note that the switching takes time because the standby BSU is started when the switching occurs.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   hot, cold2

Default behavior

Fully turns off the standby BSU, but starts the BSU and switches systems if a failure occurs.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

adaptive-power-control enable

adaptive-power-control standby-psp [AX6600S]

Sets the operating mode for the standby PSP when the traffic-based power saving functionality is in use.

Syntax

To set or change information:

```
adaptive-power-control standby-psp {hot | cold2}
```

To delete information:

```
no adaptive-power-control standby-psp
```

Input mode

```
(config)
```

Parameters

{hot | cold2}

hot

Turns on the power of the standby PSP, and switches systems immediately if a failure occurs.

cold2

Fully powering off the standby PSP allows you to reduce its power consumption to almost zero. If a failure occurs in an active PSP, the standby PSP starts automatically, and the PSPs are switched. Note that the switching takes time because the standby PSP is started when the switching occurs.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   hot, cold2

Default behavior

Fully turns off the standby PSP, but starts the PSP and switches systems if a failure occurs.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

adaptive-power-control enable

power-control [AX6700S] [AX6600S]

Specifies power control related settings of the Switch. BSU/PSP, or BSU/PSP and NIF power control allows you to reduce the power required for forwarding packets.

Syntax

To set or change information:

power-control [mode {normal | mode1 | mode2}]

To delete information:

no power-control

Input mode

(config)

Parameters

mode {normal | mode1 | mode2}

normal

Operates with normal power consumption.

mode1

- For AX6700S series switches:

  Operates with lower BSU and NIF power consumption.
- For AX6600S series switches:

  Operates with lower PSP and NIF power consumption.

mode2

- For AX6700S series switches:

  Operates with lower BSU power consumption.
- For AX6600S series switches:

  Operates with lower PSP power consumption.

1. Default value when this parameter is omitted:

   mode1
2. Range of values:

   normal, mode1, mode2

Default behavior

Operates with normal power consumption.

Impact on communication

The following table shows impacts on communication when parameters `mode2` and `normal` are set or changed according to the operating status of the power saving functionality.

Table 11-2: Effect on user communication

Operating status when settings or changes are made	Number of BSUs/ PSPs	Impact on communication
The power saving functionality is being executed. • The power saving functionality is performed during a scheduled time range. • The traffic-based power saving functionality is performed.	1 to 3	None
None of the above power saving functionalities are performed.	1	A BSU or PSP is re-initialized and communication stops until the startup process completes.
	2 to 3	None#

#: When the number of operating BSUs/PSPs is two or more, but no standby BSUs/PSPs exist, if the power control mode is changed, the BSUs/PSPs operate at a reduced switching capacity. As a result, communication might temporarily stop.

If the `mode1` parameter and other parameters (`mode2` or `normal`) are set or changed, regardless of the number of BSUs/PSPs and the operating status, all BSUs/PSPs and NIFs are re-initialized and communication stops until the startup process completes.

When the change is applied

For AX6700S series switches:

After the setting value is changed, if you enter `y` for a yes or no confirmation message, the changes are applied. After a yes or no confirmation message, if the BSU and the NIF must be restarted, they restart automatically and the changes are applied.

For AX6600S series switches:

After the setting value is changed, if you enter `y` for a yes or no confirmation message, the changes are applied. After a yes or no confirmation message, if the PSP and the NIF must be restarted, they restart automatically and the changes are applied.

Notes

1. This command can be set when `redundancy bsu-load-balancing smac` and `redundancy bsu-mode fixed` are not set. [AX6700S]
2. The `mode1` parameter can be set when `adaptive-power-control enable` is not set.
3. When the scheduled power saving functionality is in use, the Switch operates according to the configuration of the `schedule-power-control mode` command.
4. When the traffic-based power saving functionality is in use, the Switch operates according to the configuration of the `adaptive-power-control mode` command.

Related commands

None

power-control [AX6300S]

Specifies power control related settings of the Switch. PSP and NIF power control allows you to reduce the power required for forwarding packets. For details, see *13. Power Saving Functionality* in the manual *Configuration Guide Vol. 1 For Version 11.7*.

Syntax

To set information:

power-control

To delete information:

no power-control

Input mode

```
(config)
```

Parameters

None

Default behavior

Operates with normal power consumption.

Impact on communication

Communications that pass through the Switch stop while the Switch is restarting.

When the change is applied

If you set this parameter, make sure you save the configuration and restart the Switch. The new setting values do not take effect until the Switch is restarted.

Notes

1. After the setting is changed, before restarting the Switch, do not perform the following operations:
   - Restarting a NIF
   - Updating software
   - Restarting or additionally starting the standby MSU

Related commands

None

schedule-power-control max-bsu [AX6700S]

Sets the number of BSUs to be used when scheduled power saving functionality is in use.

Syntax

To set or change information:

schedule-power-control max-bsu <*max bsu*>

To delete information:

no schedule-power-control max-bsu

Input mode

`(config)`

Parameters

<*max bsu*>

Sets the number of active BSUs. If a larger value is set, packet forwarding performance is improved.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3

Default behavior

Only one BSU is set to active and the others to standby.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command can be set when `redundancy bsu-load-balancing smac`, `redundancy bsu-mode fixed`, and `redundancy standby-bsu cold` are not set.

Related commands

schedule-power-control time-range

schedule-power-control max-psp [AX6600S]

Sets the number of PSPs to be used when scheduled power saving functionality is in use.

Syntax

To set or change information:

schedule-power-control max-psp <*max psp*>

To delete information:

no schedule-power-control max-psp

Input mode

```
(config)
```

Parameters

<*max psp*>

Sets the number of active PSPs. If a larger value is set for the number of PSPs, packet forwarding performance is improved.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 2

Default behavior

Sets one PSP to standby and the other to active.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

schedule-power-control time-range

schedule-power-control mode [AX6700S] [AX6600S]

Sets power control mode when the scheduled power saving functionality is in use. BSU/PSP, or BSU/PSP and NIF power control allows you to reduce the power required for forwarding packets.

When the number of operating BSUs/PSPs is one, the power control mode for the BSU/PSP is not changed even if a scheduled start or end time is reached. When changing the power control mode for BSU/PSPs while using the scheduled power saving functionality, set the number of BSUs/PSPs to two or a larger value.

Syntax

To set or change information:

schedule-power-control mode {normal | mode1 | mode2}

To delete information:

no schedule-power-control mode

Input mode

```
(config)
```

Parameters

{normal | mode1 | mode2}

normal

Operates with normal power consumption.

mode1

- For AX6700S series switches:

  Operates with lower BSU and NIF power consumption.
- For AX6600S series switches:

  Operates with lower PSP and NIF power consumption.

mode2

- For AX6700S series switches:

  Operates with lower BSU power consumption.
- For AX6600S series switches:

  Operates with lower PSP power consumption.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.
2. Range of values:

   normal, mode1, mode2

Default behavior

For AX6700S series switches:

Operates with lower BSU power consumption.

For AX6600S series switches:

Operates with lower PSP power consumption.

Impact on communication

The following table shows impacts on communication when parameters `mode2` and `normal` are set or changed according to the operating status of the power saving functionality.

Table 11-3: Effect on user communication

Operating status when settings or changes are made	Number of BSUs/PSPs	Impact on communication
The power saving functionality is not performed. (Normal time range)	1 to 3	None
The power saving functionality is being executed. (Scheduled time range)	1	A BSU or PSP is re-initialized and communication stops until the startup process completes.
	2 to 3	None#

#: When the number of operating BSUs/PSPs is two or more, but no standby BSUs/PSPs exist, if the power control mode is changed, the BSUs/PSPs operate at a reduced switching capacity. As a result, communication might temporarily stop.

If the `mode1` parameter and other parameters (`mode2` or `normal`) are set or changed, regardless of the number of BSUs/PSPs and the operating status, all BSUs/PSPs and NIFs are re-initialized and communication stops until the startup process completes.

When the change is applied

For AX6700S series switches:

After the setting value is changed, if you enter `y` for a yes or no confirmation message, the changes are applied. After a yes or no confirmation message, if the BSU and the NIF must be restarted, they restart automatically and the changes are applied.

For AX6600S series switches:

After the setting value is changed, if you enter `y` for a yes or no confirmation message, the changes are applied. After a yes or no confirmation message, if the PSP and the NIF must be restarted, they restart automatically and the changes are applied.

Notes

1. This command can be set when `redundancy bsu-load-balancing smac`, `redundancy bsu-mode fixed`, and `redundancy standby-bsu cold` are not set. [AX6700S]

Related commands

schedule-power-control time-range

schedule-power-control port-led [AX6700S] [AX6600S]

Sets LED operation of a port when scheduled power saving functionality is in use.

Syntax

To set or change information:

schedule-power-control port-led {enable | disable}

To delete information:

no schedule-power-control port-led

Input mode

```
(config)
```

Parameters

{enable | disable}

enable

Turns on the port LED according to the operating status.

disable

Turns off the port LED regardless of the operating status. If a key on the system operation panel of the active system is used, the port LED temporarily turns on according to the operating status. If no keys are used for 60 seconds, the LED turns off.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   enable, disable

Default behavior

Turns off the port LED regardless of the operating status.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

schedule-power-control time-range

schedule-power-control redundancy nif-group max-standby-nif [AX6700S] [AX6600S]

When the NIF redundancy group is specified and scheduled power saving functionality is in use, sets the maximum number of standby NIFs in the group.

Syntax

To set or change information:

schedule-power-control redundancy nif-group <*nif group no.*> max-standby-nif <*max standby nif*>

To delete information:

no schedule-power-control redundancy nif-group <*nif group no.*> max-standby-nif

Input mode

`(config)`

Parameters

<*nif group no.*>

Specifies a NIF redundancy group number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4

<*max standby nif*>

Specifies the maximum number of standby NIFs in a NIF redundancy group. If the number of active NIFs in a NIF redundancy group exceeds the number specified by this command, this sets the specified number of NIFs to standby. The procedure for selecting NIFs to be set to standby is as follows:

- Lower priority NIFs set by the `redundancy nif-group nif priority` command
- If the priority is the same, a NIF with a larger NIF number

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 1

Default behavior

Sets only one NIF in a NIF redundancy group to active, and the other NIFs to standby.

Impact on communication

If the active NIF is placed in the standby status by the NIF redundancy control functionality, communication using the standby NIF stops.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

schedule-power-control time-range

redundancy nif-group nif priority

schedule-power-control shutdown [AX6700S] [AX6600S]

Sets a NIF or a port that is disabled when scheduled power saving functionality is in use.

Disabling the port turns off the power, reducing the amount of power consumption.

Syntax

To set information:

schedule-power-control shutdown nif <*nif no.*>

schedule-power-control shutdown interface <*interface id list*>

To change information:

schedule-power-control shutdown interface [{add | remove}] <*interface id list*>

To delete information:

no schedule-power-control shutdown nif <*nif no.*>

no schedule-power-control shutdown interface

Input mode

```
(config)
```

Parameters

nif <*nif no.*>

Specifies a NIF number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

interface <*interface id list*>

Specifies the port to be disabled in list format.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

interface [{add | remove}] <*interface id list*>

add

Adds ports to be disabled to the list.

remove

Removes ports to be disabled from the list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

A NIF or a port operates in the status other than `disable`.

For the NIF status, see the `show nif` operation command. For the port status, see the `show interfaces` operation command.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you want to disable a NIF all the time regardless of the schedule, you must set the `no power enable` command and the `schedule-power-control shutdown` command. If you want to disable a port all the time, you must set the `shutdown` command and the `schedule-power-control shutdown` command.
2. If a NIF that accommodates a port set for `shutdown interface` is replaced with another type of NIF, the settings for `shutdown interface` are deleted.

   When a port list is specified for `shutdown interface`, if the above port exists in the list, all settings for `shutdown interface` are deleted.
3. If you use a comma (,) to set `shutdown interface` for multiple Gigabit Ethernet interface lists and 10-Gigabit Ethernet interface lists, `shutdown interface` can be set for a maximum of 24 lists. If the number of lists exceeds 24, an error occurs.

Related commands

schedule-power-control time-range

schedule-power-control standby-bsu [AX6700S]

Sets the operating mode for the standby BSU when scheduled power saving functionality is in use.

Syntax

To set or change information:

schedule-power-control standby-bsu {hot | cold2}

To delete information:

no schedule-power-control standby-bsu

Input mode

`(config)`

Parameters

{hot | cold2}

hot

Powers on the standby BSU, and switches between the active and standby BSUs if a failure occurs.

cold2

Fully powering off the standby BSU allows you to reduce its power consumption to almost zero. If a failure occurs in an active BSU, the standby BSU starts automatically, and the BSUs are switched. Note that the switching takes time because the standby BSU is started when the switching occurs.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   hot, cold2

Default behavior

Fully turns off the standby BSU, but starts the BSU and switches systems if a failure occurs.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command can be set when `redundancy bsu-load-balancing smac`, `redundancy bsu-mode fixed`, and `redundancy  standby-bsu cold` are not set.

Related commands

schedule-power-control time-range

schedule-power-control standby-psp [AX6600S]

Sets the operating mode for standby PSP when scheduled power saving functionality is in use.

Syntax

To set or change information:

```
schedule-power-control standby-psp {hot | cold2}
```

To delete information:

```
no schedule-power-control standby-psp
```

Input mode

`(config)`

Parameters

{hot | cold2}

hot

Turns on the power of the standby PSP, and switches systems immediately if a failure occurs.

cold2

Fully powering off the standby PSP allows you to reduce its power consumption to almost zero. If a failure occurs in an active PSP, the standby PSP starts automatically, and the PSPs are switched. Note that the switching takes time because the standby PSP is started when the switching occurs.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   hot, cold2

Default behavior

Fully turns off the standby PSP, but starts the PSP and switches systems if a failure occurs.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

schedule-power-control time-range

schedule-power-control time-range [AX6700S] [AX6600S]

Specifies the execution time of scheduled power saving functionality.

Syntax

To set or change information:

schedule-power-control time-range <*entry number*> {execution time} action {enable | disable}

Execution time

- When a date is specified:

  date start-time <*yymmdd*> <*hhmm*> end-time <*yymmdd*> <*hhmm*>

- When a day of the week is specified:

  weekly start-time {sun | mon | tue | wed | thu | fri | sat} <*hhmm*> end-time {sun | mon | tue | wed | thu | fri | sat} <*hhmm*>

- When daily is specified:

  everyday start-time <*hhmm*> end-time <*hhmm*>

To delete information:

no schedule-power-control time-range <*entry number*>

Input mode

`(config)`

Parameters

<*entry number*>

Specifies the identifier used to identify the time of execution.

This identifier is used to reference the time of execution.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 50

■ Execution time parameters

{date | weekly | everyday}

Specifies the type of execution time to be specified.

date

Specify a date.

weekly

Specify a day of the week.

everyday

Specify a daily execution time.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   date, weekly, everyday

start-time <*yymmdd*> <*hhmm*>

Specifies the start date and time.

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.

hh

Specify the hour (00 to 23).

mm

Specify the minute (00 to 59).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a date for <*yymmdd*>, and a time for <*hhmm*>. The range of values is from 0:00 on January 1, 2000, to 23:59 on January 17, 2038.

end-time <*yymmdd*> <*hhmm*>

Specifies the end date and time.

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.

hh

Specify the hour (00 to 23).

mm

Specify the minute (00 to 59).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a date for <*yymmdd*>, and a time for <*hhmm*>. The range of values is from 0:00 on January 1, 2000, to 23:59 on January 17, 2038.

start-time {sun | mon | tue | wed | thu | fri | sat} <*hhmm*>

Specifies the start day of the week and the time.

sun

Sets Sunday.

mon

Sets Monday.

tue

Sets Tuesday.

wed

Sets Wednesday.

thu

Sets Thursday.

fri

Sets Friday.

sat

Sets Saturday.

hh

Specify the hour (00 to 23).

mm

Specify the minute (00 to 59).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Select sun, mon, tue, wed, thu, fri, or sat, and specify a time for <*hhmm*>.

end-time {sun | mon | tue | wed | thu | fri | sat} <*hhmm*>

Specifies the end day of the week and the time.

sun

Sets Sunday.

mon

Sets Monday.

tue

Sets Tuesday.

wed

Sets Wednesday.

thu

Sets Thursday.

fri

Sets Friday.

sat

Sets Saturday.

hh

Specify the hour (00 to 23).

mm

Specify the minute (00 to 59).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Select sun, mon, tue, wed, thu, fri, or sat, and specify a time for <*hhmm*>.

start-time <*hhmm*>

Specifies the start time.

hh

Specify the hour (00 to 23).

mm

Specify the minute (00 to 59).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a time for <*hhmm*>.

end-time <*hhmm*>

Specifies the end time.

hh

Specify the hour (00 to 23).

mm

Specify the minute (00 to 59).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a time for <*hhmm*>.

action {enable | disable}

Specifies the power control behavior for the execution time.

enable

Enables the setting specified by using a configuration command for the scheduled power saving functionality for the time of execution set by using this command.

disable

Disables the setting specified by using a configuration command for the scheduled power saving functionality for the time of execution set by using this command. Thereafter, the following configuration command settings are enabled:

- For AX6700S series switches:

  power-control, redundancy max-bsu, redundancy standby-bsu, system port-led, power enable, shutdown

- For AX6600S series switches:

  power-control, redundancy max-psp, redundancy standby-psp, system port-led, power enable, shutdown

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   enable, disable

Default behavior

None

Impact on communication

When the specified time of execution begins and ends, BSUs/PSPs and NIFs are re-initialized and communication via the Switch might stop until the startup process completes.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The following restrictions are applied when the time of execution is set:

   - Difference between the start and the end of the time of execution to be set is 0 minutes, or 30 minutes and more.
   - For any two execution times, a difference between the start times is 0 minutes, or 30 minutes or more.
   - For any two execution times, a difference between the end times is 0 minutes, or 30 minutes or more.
   - For any two execution times, a difference between the start time and the end time is 0 minute, or 30 minutes or more.

2. This command can be set when `redundancy bsu-load-balancing smac`, `redundancy bsu-mode fixed`, `redundancy standby-bsu cold`, and `adaptive-power-control enable` are not set. [AX6700S]

Related commands

None

system port-led

On NIFs installed in a Switch, sets the LED operation of all ports.

Syntax

To set or change information:

system port-led {enable | disable}

To delete information:

no system port-led

Input mode

```
(config)
```

Parameters

{enable | disable}

enable

Turns on the port LED according to the operating status.

disable

Turns off the port LED regardless of the operating status. If a key on the system operation panel of the active system is used, the port LED temporarily turns on according to the operating status. If no keys are used for 60 seconds, the LED turns off.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   enable, disable

Default behavior

Turns on the port LED according to the operating status.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the scheduled power saving functionality is in use, the Switch operates according to the configuration of the `schedule-power-control port-led` command. [AX6700S] [AX6600S]
2. When the traffic-based power saving functionality is in use, the Switch operates according to the configuration of the `adaptive-power-control port-led` command. [AX6700S] [AX6600S]

Related commands

None

Chapter

12. Ethernet

bandwidth
description
duplex
flowcontrol
frame-error-notice
interface gigabitethernet
interface tengigabitethernet
link debounce
link up-debounce
mdix auto
media-type [AX6700S] [AX6600S]
mtu
shutdown
speed
system mtu

bandwidth

Assigns the bandwidth of a line. This setting is used for calculating the line usage rate on a network monitoring device.

Syntax

To set or change information:

bandwidth <*kbit/s*>

To delete information:

no bandwidth

Input mode

`(config-if)`

Parameters

<*kbit/s*>

Assigns the line bandwidth in kbit/s.

This setting is used for the `ifSpeed/ifHighSpeed` (SNMP MIB) value of the applicable port, and has no impact on communication.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10000000

   Do not specify a value that exceeds the line speed of the applicable port.

Default behavior

The line speed of the applicable port becomes the bandwidth.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

description

Sets supplementary information. This command can be used as a comment about the port. Note that when this command is set, information can be checked by using the `show interfaces` or `ifDescr` (SNMP MIB) operation command.

Syntax

To set or change information:

description <*string*>

To delete information:

no description

Input mode

`(config-if)`

Parameters

<*string*>

Sets supplementary information for an Ethernet interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

`null` is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

duplex

Sets the duplex mode of a port.

Syntax

To set or change information:

duplex {half | full |auto}

To delete information:

no duplex

Input mode

```
(config-if)
```

Parameters

{half | full |auto}

Sets the connection mode of a port to half duplex (fixed), full-duplex (fixed), or auto-negotiation.

The table below shows the combinations of line types and specifiable parameters. `auto` is set if a non-specifiable parameter is specified.

Table 12-1: Specifiable parameters

Line type	Specifiable parameters
10BASE-T/ 100BASE-TX/ 1000BASE-T	`auto` (when `speed auto`, `auto 10`, `auto 100`, `auto 1000`, `auto 10 100`, or `auto 10 100 1000` is specified) `half` (when `speed 10` or `speed 100` is specified) `full` (when `speed 10` or `speed 100` is specified)
1000BASE-X	`auto` (when `speed auto` or `auto 1000` is specified) `full` (when `speed 1000` is specified)

half

Sets the port to half duplex (fixed) mode.

full

Sets the port to full duplex (fixed) mode.

auto

Determines the duplex mode by auto-negotiation.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   half, full, auto

Default behavior

`auto` is set.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. Thereafter, the port restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If `auto` or a parameter containing `auto` is specified for `speed` or `duplex`, auto-negotiation is performed.
2. For 1000BASE-X, if you do not want to use auto-negotiation, you must specify `1000` for `speed` and `full` for `duplex`. If `auto` or `auto 1000` is specified for `speed`, `full` is set for `duplex` as a result of the auto-negotiation.
3. For 10GBASE-R, `duplex` and `speed` cannot be specified.
4. For a port that can be switched between 10BASE-T, 100BASE-TX, 1000BASE-T and 1000BASE-X, if `media-type` is changed, `speed` and `duplex` for the configuration file is not changed, but if the value is not specifiable for the port after the switch, auto-negotiation is performed. [AX6700S] [AX6600S]
5. For 10BASE-T and 100BASE-TX on the NK1GS-8M and NH1GS-6M, `half` cannot be specified. For details, see 10BASE-T, 100BASE-TX, and 1000BASE-T connection specifications in *15.4 Description of the 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces* in the manual *Configuration Guide Vol. 1 For Version 11.7.*

Related commands

speed

flowcontrol

Sets flow control.

Syntax

To set or change information:

flowcontrol send {desired | on | off}

flowcontrol receive {desired | on | off}

To delete information:

no flowcontrol send

no flowcontrol receive

Input mode

```
(config-if)
```

Parameters

send {desired | on | off}

Specifies the operation for sending flow-control pause packets. Specify the same settings as those for the operation for receiving flow-control pause packets at the destination.

desired

If fixed mode is specified, pause packets are sent. If the auto-negotiation functionality is specified, whether pause packets are sent is determined through communication with the connected device.

on

Pause packets are sent.

off

Pause packets are not sent.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   send desired, send on, send off

receive {desired | on | off}

Sets the operation for receiving flow-control pause packets. Specify the same settings as those for the operation for sending flow-control pause packets at the destination.

desired

If fixed mode is set, pause packets are received. If the auto-negotiation functionality is specified, whether pause packets are received is determined through communication with the connected device.

on

Pause packets are received.

off

Pause packets are not received.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   receive desired, receive on, receive off

Default behavior

Behavior varies depending on the line type.

- For 10BASE-T, 100BASE-TX, or 1000BASE-T:

  Receive operation is `off` but send operation is `desired`.

- For 1000BASE-X:

  Receive operation is `off` but send operation is `desired`.

- For 10GBASE-R:

  Receive operation is `on` but send operation is `off`.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. Thereafter, the port restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

frame-error-notice

Sets the condition for sending a notification when a frame reception error or a frame sending error occurs. A frame reception error or a frame sending error indicates that a frame is discarded due to a failure in receiving or sending a frame, which is caused by a minor error. The cause of the failure is collected as statistics. If the number of error occurrences or the error occurrence rate over 30 seconds exceeds the value set by using this command, the error occurrences are reported. The settings of this command are applied to all ports of the Switch, and the sending side and the receiving side have the same settings.

If this configuration is not set, the error occurrences are reported when 15 or more errors occur in a 30-second interval.

The following table shows the list of statistical items that correspond to frame reception and frame sending errors.

Table 12-2: List of statistical items

#	Statistical item	
	Receiving	**Sending**
1	• CRC errors • Fragments • Jabber • Overrun • Underrun/Overrun • Symbol errors • Short frames • Long frames	• Late collision • Excessive collisions • Carrier sense lost • Excessive deferral • Underrun • Underrun/Overrun

If an error occurrence is reported, a log entry is displayed and a private trap is issued. For details about the log, see *Message and Log Reference For Version Ver. 11.7*. For details about private traps, see *MIB Reference For Version 11.7*.

Syntax

To set or change information:

frame-error-notice [error-frames <*frames*>] [error-rate <*rate*>] [{ one-time-display | everytime-display | off }]

Note: At least one parameter must be specified.

To delete information:

no frame-error-notice

Input mode

`(config)`

Parameters

error-frames <*frames*>

Sets, as the error notification condition, the threshold for the number of error occurrences (number of error frames).

1. Default value when this parameter is omitted:

   15

2. Range of values:

1 to 446400000

error-rate <*rate*>

Specifies, as the error notification condition, the threshold for the error occurrence rate as a percentage (%). The error occurrence rate is calculated as the rate of the number of error frames against the total number of frames. The fractional portion of the rate is truncated, and then it is compared with the set value. Note that if this parameter is omitted, the error occurrence rate is not regarded as a notification condition.

1. Default value when this parameter is omitted:

   The error occurrence rate is not regarded as a notification condition.

2. Range of values:

   1 to 100

The notification condition varies depending on whether the `error-frames` parameter and/or the `error-rate` parameter are set. The following table shows the error notification conditions depending on whether each parameter is set.

Table 12-3: List of error notification conditions

#	Parameter		Receiving/sending	Error notification condition
	error-frames	**error-rate**		
1	Omitted	Omitted	Receiving	The number of reception error frames is 15 or more
2			Sending	The number of sending error frames is 15 or more
3		Yes	Receiving	The rate of reception error frames against the total number of reception frames is equal to or greater than the value set for <*rate*>. This setting does not regard the number of error occurrences as a notification condition.
4			Sending	The rate of sending error frames against the total number of sending frames is equal to or greater than the value set for <*rate*>. This setting does not regard the number of error occurrences as a notification condition.
5	Yes	Omitted	Receiving	The number of reception error frames is equal to or greater than the value set for <*frames*>. This setting does not regard the error occurrence rate as a notification condition.
6			Sending	The number of sending error frames is equal to or greater than the value set for <*frames*>. This setting does not regard the error occurrence rate as a notification condition.
7		Yes	Receiving	The number of reception error frames is equal to or greater than the value set for <*frames*>, and the rate of reception error frames against the total number of reception frames is equal to or greater than the value set for <*rate*>.

#	Parameter		Receiving/sending	Error notification condition
	error-frames	error-rate		
8			Sending	The number of sending error frames is equal to or greater than the value set for <*frames*>, and the rate of sending error frames against the total number of sending frames is equal to or greater than the value set for <*rate*>.

{ everytime-display | one-time-display | off }

Specifies whether to display a log entry when an error occurrence is reported. If a large number of errors occur continuously, this setting can prevent the log file from being filled with this log entry. Note that this parameter has no impact on private traps. Use the `snmp-server host` command to specify whether to issue a private trap. For details, see *snmp-server host* in the manual *Configuration Command Reference Vol. 2 For Version 11.7.*

everytime-display

Displays a log entry every time an error occurrence is reported.

one-time-display

Displays a log entry only when an error occurrence is reported for the first time. No log entries are displayed for subsequent errors. Note, however, that if the applicable port is restarted, a log entry is displayed when the first error occurrence after the restart is reported.

off

No log entries are displayed.

1. Default value when this parameter is omitted:

   one-time-display

2. Range of values:

   `everytime-display`, `one-time-display`, or `off`

Default behavior

When 15 or more errors occur in a 30-second time interval, the error occurrences are reported. Displays a log entry only when an error occurrence is reported for the first time. No log entries are displayed for subsequent errors. Note, however, that if the applicable port is restarted, a log entry is displayed when the first error occurrence after the restart is reported.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you use this command to set the configuration, you must specify at least one parameter.
2. Entering this command disables the settings specified until then. If you want to inherit the old settings, use this command to specify the applicable parameter again.

Related commands

snmp-server host

interface gigabitethernet

Sets items related to 10BASE-T, 100BASE-TX, 1000BASE-T, and 1000BASE-X. Entering this command switches to `config-if` mode, in which information about the relevant port can be set.

Syntax

To set information:

interface gigabitethernet <*nif no.*>/<*port no.*>

To delete information:

no interface gigabitethernet <*nif no.*>/<*port no.*>

Input mode

`(config)`

Parameters

<*nif no.*>/<*port no.*>

Specifies the NIF number and the port number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The port name is `geth` + <*NIF number*> +/+ <*port number*>.

   For example, the name of the 1/1 port will be `geth1/1`.

2. This command can delete ports on which no NIFs are installed. This command cannot delete ports on which a NIF is installed.

Related commands

None

interface tengigabitethernet

Sets 10GBASE-R-related items. Entering this command switches to `config-if` mode, in which information about the relevant port can be set.

Syntax

To set information:

interface tengigabitethernet <*nif no.*>/<*port no.*>

To delete information:

no interface tengigabitethernet <*nif no.*>/<*port no.*>

Input mode

`(config)`

Parameters

<*nif no.*>/<*port no.*>

Specifies the NIF number and the port number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The port name is `tengeth` + <*NIF number*> +/+ <*port number*>.

   For example, the name of the 1/1 port will be `tengeth1/1`.

2. This command can delete ports on which no NIFs are installed. This command cannot delete ports on which a NIF is installed.

Related commands

None

link debounce

Sets the link-down detection time after a link failure is detected until the actual link-down occurs. When a large value is set, temporary link-downs will not be detected, thereby preventing instability of the link.

Syntax

To set or change information:

link debounce [time <*mili seconds*>]

To delete information:

no link debounce

Input mode

```
(config-if)
```

Parameters

time <*mili seconds*>

Sets the debounce timer value in milliseconds.

1. Default value when this parameter is omitted:

   3000 milliseconds

2. Range of values:

   Multiples of 100 from 0 to 10000

Default behavior

10BASE-T, 100BASE-TX, and 1000BASE-T: Operates at 2000 milliseconds.

1000BASE-X, and 10GBASE-R: Operates at 0 milliseconds.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. Thereafter, the port restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the link is stable even when a link-down detection timer is not set, do not set the timer.
2. If a value smaller than the default value (2000 milliseconds) is set for 10BASE-T, 100BASE-TX, or 1000BASE-T, the link might become unstable.

Related commands

None

link up-debounce

Sets the link-up detection time after a link failure is detected until the actual link-up occurs. When a large value is set, a temporary link-up will not be detected, thereby preventing instability of the network status.

Syntax

To set or change information:

link up-debounce time <*mili seconds*>

To delete information:

no link up-debounce

Input mode

```
(config-if)
```

Parameters

time <*mili seconds*>

Sets the debounce timer value when a link-up state occurs, in milliseconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Multiples of 100 from 0 to 10000

Default behavior

When the line speed is fixed, the operating value is 1000 milliseconds. When the line speed is set to auto-negotiation, the operating value is 0 seconds.

Impact on communication

If this command is set for a line in use, the line goes down and communication stops temporarily. Thereafter, the line restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The larger the value you set for the link-up detection timer, the more time it takes until communication is restored after a link failure has been corrected. If you want this time to be short, do not set a link-up detection timer.
2. If you set a value smaller than the default value, the link might become unstable.

Related commands

duplex

link debounce

speed

mdix auto

Sets the automatic MDIX functionality of the port to be used. When `no mdix auto` is specified, the automatic MDIX functionality is disabled and the port is fixed to MDI-X.

Syntax

To set information:

no mdix auto

To delete information:

mdix auto

Input mode

`(config-if)`

Parameters

None

Default behavior

During auto-negotiation, MDI and MDI-X are switched automatically.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is enabled during auto-negotiation.
2. For 1000BASE-X, this command is disabled.
3. For 10GBASE-R, this command cannot be specified.
4. If `media-type` is `sfp`, this command is disabled. [AX6700S] [AX6600S]

Related commands

media-type [AX6700S] [AX6600S]

speed

media-type [AX6700S] [AX6600S]

Selects a port used in a selectable port that can be used either as a 10BASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X port.

Syntax

To set or change information:

media-type {rj45 | sfp}

To delete information:

no media-type

Input mode

`(config-if)`

Parameters

{rj45 | sfp}

Selects a port used in a selectable port that can be used either as a 10BASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X port.

rj45

An RJ45 port is used.

sfp

An SFP port is used.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `rj45` or `sfp`

Default behavior

Sets `sfp` (an SFP port is used).

Impact on communication

If this command is specified for a port in use, the port goes down, but the specified port restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command cannot be set for a port other than a selectable port that can be used as a 10BASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X port.

Related commands

None

mtu

Sets the MTU for ports. With this configuration, jumbo frames can be used to improve the throughput of data transfers. As a result, the usability of a network and devices connected to the network improves.

Syntax

To set or change information:

mtu <*length*>

To delete information:

no mtu

Input mode

`(config-if)`

Parameters

<*length*>

Sets the MTU of ports in octets. The MTU is the maximum length of the data section# for frames in Ethernet V2 format.

#: For details about the frame format, see *15.1.3 Control on the MAC and LLC sublayers* in the manual *Configuration Guide Vol. 1 For Version 11.7*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1500 to 9578

Default behavior

The following initial values are set.

Table 12-4: Initial MTU values for ports

Presence of the system mtu command	Initial value
Set	Setting value for `system mtu`
Not set	1500

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The table below describes the MTU of the applicable port and the length of frames that can be sent or received (the maximum length of frames in Ethernet V2 format#, excluding the FCS).

   #: For details about the frame format, see *15.1.3 Control on the MAC and LLC sublayers* in the manual *Configuration Guide Vol. 1 For Version 11.7*.

Table 12-5: MTU and the length of frames that can be sent or received

Line type	mtu setting	system mtu setting	Length of a frame that can be sent or received (in octets)	Port MTU (in octets)
10BASE-T (full and half-duplex), 100BASE-TX (half-duplex)	Not related	Not related	1518	1500
All other cases	Set	Not related	M1[#1]+18	M1[#1]
	Not set	Set	M2[#2]+18	M2[#2]
		Not set	1518	1500

#1: The value set by using the `mtu` command of `interface`.

#2: The value set by using the `system mtu` command.

2. Use the same MTU value for the ports belonging to the VLAN. If the MTU is different, the following operation is performed:
    - For L2 forwarding, if the MTU of the output port is smaller than the MTU of the input port, and the length of the frames to be forwarded exceeds the maximum length of frames that can be sent on the output port, frames can be sent from the output port.
    - For L3 forwarding, MTU for a VLAN interface varies depending on the port MTU and the IP MTU setting, as described in the following table.

Table 12-6: MTU for a VLAN interface

MTU setting	IP MTU setting	MTU of a VLAN interface (in octets)
Omitted	Omitted	1500
	Set	min (1500, L2[#1])
Set	Omitted	L1[#2]
	Set	min (L1[#2], L2[#1])

#1: IP MTU value

#2: Port MTU value (if values differ among ports, the minimum value is used).

3. For two row VLAN tags in VLAN tunneling, the frame length will be <*IP packet length*> + 22 octets. If an IP packet of 1500 octets is sent from a port with two-row VLAN tags, set a value equal to or larger than 1504 for `mtu`.
4. NIFs listed in the table below have limitations on the jumbo frame length to be supported. When using jumbo frames in these NIFs, set the MTU configuration for a port to a value equal to or less than the value indicated in the table below. In addition, the MTU of all ports that are handled in the same VLAN as the corresponding port in the device must be set to a value equal to or smaller than the value listed in the table below.

Table 12-7: Upper limit of jumbo frame length (not including FCS) and upper limit of MTU length

NIF abbreviation	Upper limit of jumbo frame length (not including FCS)	Upper limit of MTU length
NK1GS-8M	2000	1982
NH1G-16S	4092	4074
NH1G-48T	4092	4074

NIF abbreviation	Upper limit of jumbo frame length (not including FCS)	Upper limit of MTU length
NH1GS-6M	2000	1982

Related commands

None

shutdown

Places the port in the shutdown state. The command also turns off the port's power.

Syntax

To set information:

shutdown

To delete information:

no shutdown

Input mode

`(config-if)`

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command can be set from the SNMP manager by using an SNMP SetRequest operation. If this command is set by using an SNMP SetRequest operation, the setting is applied to the configuration.
2. When the scheduled power saving functionality is in operation, the device operates according to the configuration of the `schedule-power-control shutdown` command. [AX6700S] [AX6600S]

Related commands

None

speed

Sets the port speed.

Syntax

To set or change information:

speed { 10 | 100 | 1000 | auto | auto {10 | 100 | 1000 | 10 100 | 10 100 1000} }

To delete information:

no speed

Input mode

`(config-if)`

Parameters

{ 10 | 100 | 1000 | auto | auto {10 | 100 | 1000 | 10 100 | 10 100 1000} }

Sets the line speed.

The table below shows the combinations of line types and specifiable parameters. `auto` is set if a non-specifiable parameter is specified.

Table 12-8: Specifiable parameters

Line type	Specifiable parameters
10BASE-T/ 100BASE-TX/ 1000BASE-T	10 100 auto auto 10 auto 100 auto 1000 auto 10 100 auto 10 100 1000
1000BASE-X	1000 auto auto 1000

10

Sets the line speed to 10 Mbit/s.

100

Sets the line speed to 100 Mbit/s.

1000

Sets the line speed to 1000 Mbit/s.

auto

Sets the line speed to auto-negotiation.

auto {10 | 100 | 1000 | 10 100 | 10 100 1000}

Auto-negotiation is performed at the specified line speed. This setting prevents the line speed from operating at an unexpected speed, so the line usage rate is prevented from increasing. If negotiation at the specified line speed does not succeed, the link status does not transition to link-up status.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   10, 100, 1000, auto, auto {10 | 100 | 1000 | 10 100 | 10 100 1000}

Default behavior

`auto` is set.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. Thereafter, the port restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If `auto` or a parameter containing `auto` is specified for `speed` or `duplex`, auto-negotiation is performed.
2. If auto-negotiation is not used for 10BASE-T, 100BASE-TX, or 1000BASE-T, you must set `speed` to `10` or `100`, and set `duplex` to `full` or `half`.
3. For 1000BASE-X, if auto-negotiation is not used, you must set `speed` to `1000` and `duplex` to `full`.
4. For 10GBASE-R, `duplex` and `speed` cannot be specified.
5. For a port that can be switched between 10BASE-T, 100BASE-TX, 1000BASE-T and 1000BASE-X, if `media-type` is changed, `speed` and `duplex` for the configuration file is not changed, but if the value is not specifiable for the port after the switch, auto-negotiation is performed. [AX6700S] [AX6600S]

Related commands

duplex

system mtu

Sets the MTU of all ports. With this configuration, jumbo frames can be used to improve the throughput of data transfers. As a result, the usability of a network and devices connected to the network improves.

Syntax

To set or change information:

system mtu *<length>*

To delete information:

no system mtu

Input mode

```
(config)
```

Parameters

<length>

Sets the MTU of all ports in octets. The MTU is the maximum length of the data section# for frames in Ethernet V2 format.

#: For details about the frame format, see *15.1.3 Control on the MAC and LLC sublayers* in the manual *Configuration Guide Vol. 1 For Version 11.7*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1500 to 9578

Default behavior

The MTU of all ports is set to 1500.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The table below describes the port MTU and the length of a frame that can be sent or received (the maximum length of a frame in Ethernet V2 format#, excluding the FCS).

   #: For details about the frame format, see *15.1.3 Control on the MAC and LLC sublayers* in the manual *Configuration Guide Vol. 1 For Version 11.7*.

Table 12-9: MTU and the length of frames that can be sent or received

Line type	mtu setting	system mtu setting	Length of a frame that can be sent or received (in octets)	Port MTU (in octets)
10BASE-T (full and half-duplex), 100BASE-TX (half-duplex)	Not related	Not related	1518	1500

Line type	mtu setting	system mtu setting	Length of a frame that can be sent or received (in octets)	Port MTU (in octets)
All other cases	Set	Not related	M1[#1]+18	M1[#1]
	Not set	Set	M2[#2]+18	M2[#2]
		Not set	1518	1500

#1: The value set by using the `mtu` command of `interface`.

#2: The value set by using the `system mtu` command.

2. For two row VLAN tags in VLAN tunneling, the frame length will be <*IP packet length*> +22 octets. If an IP packet of 1500 octets is sent from a port with two-row VLAN tags, set `system mtu` so that the port mtu value is set to a value larger than 1504 or set mtu on the port.
3. NIFs listed in the table below have limitations on the jumbo frame length to be supported. When using jumbo frames in these NIFs, set the MTU configuration for a port to a value equal to or less than the value indicated in the table below. In addition, the MTU of all ports that are handled in the same VLAN as the corresponding port in the device must be set to a value equal to or smaller than the value listed in the table below.

Table 12-10: Upper limit of jumbo frame length (not including FCS) and upper limit of MTU length

NIF abbreviation	Upper limit of jumbo frame length (not including FCS)	Upper limit of MTU length
NK1GS-8M	2000	1982
NH1G-16S	4092	4074
NH1G-48T	4092	4074
NH1GS-6M	2000	1982

Related commands

None

Chapter

13. Link Aggregation

channel-group lacp system-priority

Sets the LACP system priority of the applicable channel group for link aggregation.

Syntax

To set or change information:

channel-group lacp system-priority <*priority*>

To delete information:

no channel-group lacp system-priority

Input mode

```
(config-if)
```

Parameters

<*priority*>

Sets the LACP system priority. The lower the value, the higher the priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

The setting of the `lacp system-priority` command is used.

Impact on communication

If a priority is set for an active channel group, the channel group goes down, and then restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.
2. If you set a restriction on the number of detached ports (`max-detach-port`) to connect a Switch to a device from other manufacturers, set a higher LACP system priority level for the Switch.
3. If the LACP system priority is changed, the status of all ports registered for the channel group changes to `Blocking` (communication interrupted).

Related commands

interface port-channel

channel-group max-detach-port

channel-group load-balance

Specifies the method of link aggregation used for load balancing.

Syntax

To set or change information:

channel-group load-balance {mac-ip-port | vlan}

To delete information:

no channel-group load-balance

Input mode

`(config-if)`

Parameters

{mac-ip-port | vlan}

mac-ip-port

Determines link aggregation based on information contained in received frames.

vlan

Determines link aggregation separately for each VLAN that is sending frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `mac-ip-port` or `vlan`

Default behavior

Determines link aggregation based on information contained in received frames.

Impact on communication

If this setting is specified for an active port, communication temporarily stops.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

channel-group max-active-port

Sets the maximum number of active ports that will be used for link aggregation in the applicable channel group.

Syntax

To set information:

channel-group max-active-port <*number*> [no-link-down]

To change information:

channel-group max-active-port <*number*>

channel-group max-active-port <*number*> no-link-down

To delete information:

no channel-group max-active-port

Input mode

`(config-if)`

Parameters

<*number*>

Specifies the maximum number of ports that will be used for link aggregation in a channel group. If the number of ports that are actually used in a channel group exceeds the value specified by this command, only the specified maximum number of ports are used, and the standby link functionality is applied to the rest of the ports.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 16

no-link-down

To use the standby link functionality in a link-not-down mode, specify this parameter. Otherwise, standby links switch to the link-down status. The conditions for selecting which links are standby links are as follows:

- Select ports that have been assigned lower priority by using the `lacp port-priority` command.
- If the priority is the same, select the port with the larger NIF number and larger port number.

1. Default value when this parameter is omitted:

   Standby links switch to link-down status.

2. Range of values:

   None

Default behavior

The maximum number is 16.

Impact on communication

The ports that are in use might be changed by the standby link functionality, and communication might stop temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when static link aggregation is used.
2. If you specify the `max-active-port` command, match its settings to the settings of the `max-active-port` and `lacp port-priority` commands on the destination device.
3. Ports in standby link mode cannot be changed directly between the link-down and no-link-down statuses. To change the status, delete this parameter, and then set this parameter again. To change the number of ports in a link-not-down mode, you must specify the `no-link-down` parameter.
4. If this command is set and a port in link-down status is selected as a standby link, only the log entries that indicate detachment are displayed. Log entries indicating aggregation for the ports are not displayed.

Related commands

interface port-channel

channel-group lacp system-priority

lacp system-priority

lacp port-priority

channel-group max-detach-port

Limits the maximum number of detached ports in the applicable link aggregation channel group.

Syntax

To set or change information:

channel-group max-detach-port <*number*>

To delete information:

no channel-group max-detach-port

Input mode

`(config-if)`

Parameters

<*number*>

Specifies the maximum number of ports that can be detached from a channel group used for link aggregation for reasons such as a link down. When 0 is specified, no ports can be detached. Therefore, if a link goes down, the whole channel group goes down.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 or 15

Default behavior

15 is set as the limit on the maximum number of detached ports.

Impact on communication

Channel groups might go down due to a limit on the number of detached ports.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.
2. If you specify the `max-detach-port` command, match its settings to the settings of the destination device.
3. If `0` is entered for the `max-detach-port` command, the effect is the same as when `15` is entered for the `max-detach-port` command in on mode (this is the default when nothing is entered for `max-detach-port`).
4. If you set a restriction on the number of detached ports (`max-detach-port`) to connect a Switch to a device from other manufacturers, set a higher LACP system priority level for the Switch.
5. If you change the value for <*number*> to `0`, all ports registered for the channel group change to `Blocking` (communication interrupted) while some ports registered in the channel group for the applicable link aggregation are degraded.

Related commands

interface port-channel

channel-group mode

channel-group lacp system-priority

lacp system-priority

channel-group mode

Creates a channel group for link aggregation.

Syntax

To set information:

channel-group <*channel group number*> mode { on | { active | passive } }

To change information:

channel-group <*channel group number*> mode { active | passive }

To delete information:

no channel-group

Input mode

```
(config-if)
```

Parameters

<*channel group number*>

Specifies the channel group number for link aggregation.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

mode { on | { active | passive } }

Specifies the mode for link aggregation.

on

Static link aggregation is performed.

active

LACP-based link aggregation is performed, and LACPDUs are always sent irrespective of the remote device.

passive

LACP-based link aggregation is performed, but LACPDUs are sent only when an LACPDU from the remote device is received.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `on`, `active`, or `passive`

Default behavior

None

Impact on communication

If this setting is specified for an active port, communication temporarily stops.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To change static link aggregation to LACP-based link aggregation, or vice versa, delete this command, change the mode, and then set the command again.
2. When `channel-group mode` is set, the `port-channel` setting of the specified channel group is automatically generated. If `port-channel` has already been set, no specific operation is required.
3. If the `port-channel` setting of the specified channel group number already exists when you set this command, you must either specify the same setting for the applicable interface and the port channel interface with the specified channel group number or else not set a common configuration command for the applicable interface. For details, see *16.2.4 Configuring a port channel interface* in the manual *Configuration Guide Vol. 1 For Version 11.7*.
4. To delete this command, do so after performing either of the following:
   - In Ethernet interface configuration mode, set `shutdown`.
   - Use the power saving functionality's `schedule-power-control shutdown` command to disable the port. [AX6700S] [AX6600S]
5. Deleting this command does not delete the `port-channel` configuration (deleting all ports in a channel group does not delete the `port-channel` configuration). When deleting a channel group, you must delete the `port-channel` configuration manually.

Related commands

interface gigabitethernet

interface tengigabitethernet

channel-group multi-speed

Sets mixed-speed mode. If this command is set, ports with different transmission speeds can be used simultaneously in a channel group for link aggregation.

Syntax

To set information:

```
channel-group multi-speed
```

To delete information:

```
no channel-group multi-speed
```

Input mode

```
(config-if)
```

Parameters

None

Default behavior

None

Impact on communication

The ports that are in use might be changed by the standby link functionality, and communication might stop temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When frames are sent, ports are allocated irrespective of the port transmission speed

Related commands

interface port-channel

channel-group periodic-timer

Specifies the interval for sending LACPDUs.

Syntax

To set or change information:

channel-group periodic-timer { long | short }

To delete information:

no channel-group periodic-timer

Input mode

`(config-if)`

Parameters

{ long | short }

Specifies the interval at which the remote device sends LACPDUs to a Switch.

`long`: 30 seconds

`short`: 1 second

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `long` or `short`

Default behavior

`long` (30 seconds) is set as the sending interval.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.

Related commands

interface port-channel

channel-group mode

description

Sets supplementary information.

Syntax

To set or change information:

description <*string*>

To delete information:

no description

Input mode

```
(config-if)
```

Parameters

<*string*>

Sets supplementary information for the applicable channel group used for link aggregation. Use this command to create and attach a note to the interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

`NULL` is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

interface port-channel

Sets an item related to a port channel interface. Entering this command switches to `config-if` mode, which allows you to use configuration commands to specify the channel group number. A port channel interface is automatically generated when the `channel-group mode` command is set.

Syntax

To set information:

interface port-channel <*channel group number*>

To delete information:

no interface port-channel <*channel group number*>

Input mode

`(config)`

Parameters

<*channel group number*>

Specifies the channel group number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you want to delete this command, do so after executing the `shutdown` command for all ports in the applicable channel group.

Related commands

interface gigabitethernet

interface tengigabitethernet

interface range

lacp port-priority

Sets the port priority.

Syntax

To set or change information:

lacp port-priority <*priority*>

To delete information:

no lacp port-priority

Input mode

`(config-if)`

Parameters

<*priority*>

Specifies the port priority. The lower the value, the higher the priority.

When `on` is specified for the `channel-group mode` command

This parameter is used with the `max-active-port` command to select the standby links.

When `active` or `passive` is set for the `channel-group mode` command

This parameter applies to port priority for the LACP protocol.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

Default behavior

`128` is set as the port priority.

Impact on communication

If you specify the port priority for an active port by setting `channel-group mode` to `active` or `passive`, communication is temporarily interrupted. If you specify port priority for active ports by setting `channel-group mode` to `on`, ports that are use might be changed by the standby link functionality, and communication might temporarily stop.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you specify the `max-active-port` command, match its settings to the settings of `max-active-port` for the destination device.
2. If you change <*priority*>, the status of the applicable port changes to `Blocking` (communication interrupted).

Related commands

interface gigabitethernet

interface tengigabitethernet

channel-group mode

channel-group max-active-port

lacp system-priority

Sets the effective LACP system priority for a Switch.

Syntax

To set or change information:

lacp system-priority <*priority*>

To delete information:

no lacp system-priority

Input mode

`(config)`

Parameters

<*priority*>

Sets the LACP system priority. The lower the value, the higher the priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

If the `channel-group lacp system-priority` command has been set, that setting is used. If the `channel-group lacp system-priority` command has not been set, 128 is used.

Impact on communication

If a priority is set for an active channel group, the channel group goes down, and then restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.
2. If you set a restriction on the number of detached ports (`max-detach-port`) to connect a Switch to a device from other manufacturers, set a higher LACP system priority level for the Switch.
3. If the LACP system priority is changed, the status of all ports registered for the channel group changes to `Blocking` (communication interrupted).

Related commands

channel-group max-detach-port

shutdown

Always disables the applicable channel group for link aggregation, and stops communication.

Syntax

To set information:

shutdown

To delete information:

no shutdown

Input mode

```
(config-if)
```

Parameters

None

Default behavior

None

Impact on communication

If a priority is specified for an active channel group, the channel group goes down.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command can be set from the SNMP manager by using an SNMP SetRequest operation. If this command is set by using an SNMP SetRequest operation, the setting is applied to the configuration.

Related commands

None

Chapter

14. MAC Address Table

mac-address-table aging-time

Sets the aging conditions for MAC address table entries.

Syntax

To set or change information:

mac-address-table aging-time <*seconds*> [vlan <*vlan id*>]

To delete information:

no mac-address-table aging-time [vlan <*vlan id*>]

Input mode

```
(config)
```

Parameters

<*seconds*>

Sets the aging time in seconds. If `0` is specified, aging is not performed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0, 10 to 1000000 (seconds)

vlan <*vlan id*>

Specifies the VLAN ID of the VLAN of which aging time is set.

1. Default value when this parameter is omitted:

   Sets the same aging time for all VLANs.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

300 seconds is set as the aging time.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you set this without designating a specific VLAN, the setting applies to all VLANs. If you specify VLAN-specific settings and a setting without a specific VLAN designation simultaneously, the timer values of VLAN-specific settings takes precedence. For other VLANs which are not specifically designated, the timer value for the setting without a specific VLAN designation applies.
2. If only settings with specific VLAN designations are specified, the default aging time for VLANs without a specific VLAN designation is 300 seconds.
3. Settings made using VLAN-specific designations are not deleted by deleting the non-VLAN-specific setting. You must specify an individual VLAN to delete its

VLAN-specific settings.

Related commands

None

mac-address-table learning

Suppresses dynamic MAC address learning. If MAC address learning is suppressed, frames which are not addressed to the local Switch or not matched to static MAC table entries are flooded to all ports.

Syntax

To set information:

no mac-address-table learning vlan <*vlan id*>

To delete information:

mac-address-table learning vlan <*vlan id*>

Input mode

`(config)`

Parameters

vlan <*vlan id*>

Specifies the VLAN ID of a VLAN for which MAC address learning is to be suppressed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

MAC address learning is not suppressed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The `no mac-address-table learning` setting has precedence over the `mac-address-table limit` setting. Because of this, VLAN frames for which MAC address learning is suppressed are relayed even when MAC address learning is suppressed by `mac-address-table limit`.
2. Suppressing MAC address learning deletes the `mac-address-table` that was being learned.
3. If there is no available space in the MAC address table, `no mac-address-table learning` cannot be set. For the capacity limit of the MAC address table, see the description of the applicable MAC address table in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the configuration entries of the functionalities that use the MAC address table.

Related commands

vlan

mac-address-table limit

Limits the number of dynamic MAC addresses learned. If the count reaches the high limit, a log messages are displayed, and MAC address learning stops. When MAC address learning stops, if SMAC receives frames that do not exist in `mac-address-table`, such frames are discarded. MAC address learning is restarted if the number of learned entries becomes smaller than the specified threshold value due to aging or the like.

Syntax

To set or change information:

mac-address-table limit { vlan <*vlan id*> | interface <*interface type*> <*interface number*>} maximum <*number*> [threshold <*number*>]

To delete information:

no mac-address-table limit { vlan <*vlan id*> | interface <*interface type*> <*interface number*>}

Input mode

`(config)`

Parameters

vlan <*vlan id*>

Specifies the VLAN ID of a VLAN for which MAC address learning is to be suppressed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

interface <*interface type*> <*interface number*>

Specifies the interface for which MAC address learning is to be limited. A physical port or channel group can be specified for the interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*interface type*> <*interface number*>, the following values can be specified:

   - gigabitethernet <*nif no.*>/<*port no.*>

   - tengigabitethernet <*nif no.*>/<*port no.*>

   For details about the valid setting range of <*nif no.*>/<*port no.*>, see *Specifiable values for parameters*.

   - port-channel <*channel group number*>

   For details about the valid setting range of <*channel group number*>, see *Specifiable values for parameters*.

maximum <*number*>

Specifies the limit value for the number of MAC addresses learned. If `0` is specified, no learned MAC address entries can be registered. Also, when `0` is specified, the `threshold` parameter cannot be set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 100000

threshold <*number*>

Specifies the threshold value for resuming learning after the learned MAC address count reaches the limit and learning stops. When the number of entries falls below the threshold value, MAC address learning is resumed. When `0` is specified for `maximum`, this parameter cannot be set.

1. Default value when this parameter is omitted:

   The same value as the limit value is used.

2. Range of values:

   A value ranging from 1 to 100000 that is equal to or smaller than the limit value.

Default behavior

MAC address learning is not limited.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Suppressing of MAC address learning by `no mac-address-table learning` has precedence over the learning limit values in this command. As a result, if MAC address learning is stopped by this command, frames of VLANs for which MAC address learning is suppressed by `no mac-address-table learning` are forwarded.
2. If the learned MAC address limit is set to a value equal to or smaller than the number of already-learned entries, already-learned entries are not deleted. To delete learned entries, wait for aging to remove them or execute the `clear mac-address-table` command.

Related commands

vlan

mac-address-table static

Sets static MAC address table information.

Syntax

To set or change information:

mac-address-table static <*mac*> vlan <*vlan id*> interface <*interface type*> <*interface number*>

To delete information:

no mac-address-table static <*mac*> vlan <*vlan id*> [interface <*interface type*> <*interface number*>]

Input mode

`(config)`

Parameters

<*mac*>

Specifies a MAC address to be registered as a static entry.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0000.0000.0000 to feff.ffff.ffff

   Note, however, that a multicast MAC address (address whose first-byte lower bit is set to 1) cannot be set.

vlan <*vlan id*>

Specifies the VLAN ID of the VLAN for static entries.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

interface <*interface type*> <*interface number*>

Specifies the output destination interface for static entries. A physical port or channel group can be specified for the interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*interface type*> <*interface number*>, the following values can be specified:

   - gigabitethernet <*nif no.*>/<*port no.*>

   - tengigabitethernet <*nif no.*>/<*port no.*>

   For details about the valid setting range of <*nif no.*>/<*port no.*>, see *Specifiable values for parameters*.

   - port-channel <*channel group number*>

For details about the valid setting range of <*channel group number*>, see *Specifiable values for parameters*.

Default behavior

No static entries are set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you set a static entry for the default VLAN (VLAN ID = 1), explicitly set `vlan 1` for the output destination interface.
2. If there is no available space in the MAC address table, `mac-address-table static` cannot be set. For the capacity limit of the MAC address table, see the description of the applicable MAC address table in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the configuration entries of the functionalities that use the MAC address table.
3. If a physical port in the channel group is specified as an output destination interface, communication might not be possible. Specify the `port-channel` parameter to set a channel group as the output destination for the static MAC address.

Related commands

vlan

Chapter

15. VLANs

down-debounce

Sets the down-determination time of a VLAN interface when no more ports that can be used for relays exist in the VLAN.

Syntax

To set or change information:

down-debounce <*seconds*>

To delete information:

no down-debounce

Input mode

`(config-if) This can be set only for VLAN interfaces.`

Parameters

<*seconds*>

Sets the down-determination time (in seconds) of a VLAN interface when no more ports that can be used for relays exist in the VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 180

Default behavior

The VLAN interface goes down immediately when it is detected that there are no longer any ports that can be used for relaying the VLAN.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If there are no more ports that can be used for relaying the VLAN in the following situations, the VLAN interface goes down immediately regardless of any setting by this command:
   - When no more ports belong to the VLAN
   - When the VLAN status is disabled by the `state` command
2. If the setting value is changed during the down-determination time of a VLAN interface, the VLAN interface goes down after the changed setting value elapses since the time when the value was changed.
3. If the setting value is deleted during the down-determination time of a VLAN interface, the interface goes down when the value is deleted.
4. If the system is switched during the down-determination time of a VLAN interface, the interface goes down when the system is switched.

Related commands

None

interface vlan

Configures a VLAN interface. Entering this command switches to `config-if` mode in which the IP address or other settings can be set for the relevant VLAN interface.

Syntax

To set information:

interface vlan <*vlan id*>

To delete information:

no interface vlan <*vlan id*>

Input mode

`(config)`

Parameters

<*vlan id*>

Specifies a VLAN ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*. Note, however, that the default VLAN (VLAN ID = 1) cannot be specified when information is deleted.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If a VLAN ID which has not yet been set is specified for <*vlan id*>, a VLAN is created. Created VLANs are port-based VLANs. For a protocol-based VLAN or MAC VLAN, the VLAN must be created beforehand by using the `vlan` command.
2. If you set information for multiple VLAN interfaces, use the `interface range` command to set <*vlan id list*>. Note that an error will occur if you specify a VLAN ID which has not been set by using the `interface range` command, and a new VLAN will not be created.
3. Specifying `no vlan` for a VLAN that was created by the `interface vlan` command deletes the VLAN. Also, specifying the `no interface vlan` command for a VLAN that was created by the `vlan` command deletes the VLAN.

Related commands

vlan

l2protocol-tunnel eap

Enables the EAPOL forwarding functionality. Sets this command for VLAN interfaces.

Syntax

To set information:

```
l2protocol-tunnel eap
```

To delete information:

```
no l2protocol-tunnel eap
```

Input mode

```
(config-if)
```

Parameters

None

Default behavior

The EAPOL forwarding functionality is invalid.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

interface vlan

l2protocol-tunnel stp

Enables the BPDU forwarding functionality. Sets this command for VLAN interfaces.

Syntax

To set information:

```
l2protocol-tunnel stp
```

To delete information:

```
no l2protocol-tunnel stp
```

Input mode

`(config-if)`

Parameters

None

Default behavior

The BPDU forwarding functionality is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

interface vlan

l2-isolation

Blocks Layer 2 forwarding within a VLAN. Only Layer 3 forwarding is permitted.

Syntax

To set information:

l2-isolation

To delete information:

no l2-isolation

Input mode

`(config)`

Parameters

None

Default behavior

Layer 2 forwarding is not blocked.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

mac-address

Sets the MAC address used to identify a MAC VLAN.

Syntax

To set information:

mac-address <*mac*>

To delete information:

no mac-address <*mac*>

Input mode

```
(config-vlan) (MAC VLAN only)
```

Parameters

<*mac*>

Specifies the MAC address setting for a MAC VLAN. This command can be set only when the applicable VLAN is a MAC VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0000.0000.0000 to feff.ffff.ffff

   The lowest bit of the first byte (the multicast bit) must not be 1.

Default behavior

No MAC address is specified.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. MAC addresses that are already assigned to another VLAN cannot be set. Delete the address, and then set it again.
2. If you specify a dynamically-set MAC address used for IEEE 802.1X, Web authentication, or an authentication VLAN, settings for those functionalities become invalid and settings for this command are enabled.
3. The maximum number of MAC addresses that can be set for a Switch is 4096.

Related commands

None

name

Sets a VLAN name.

Syntax

To set or change information:

name <*string*>

To delete information:

no name

Input mode

`(config-vlan)`

Parameters

<*string*>

Sets a VLAN name. This parameter cannot be set if <*vlan id list*> has been specified by using the `vlan` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

The initial value is `VLAN`xxxx. Note that xxxx is a four-digit numeric string, including any leading zeros, that indicates a VLAN ID.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

protocol

Sets the protocol for identifying VLANs in protocol VLANs.

Syntax

To set information:

protocol <*protocol name*>

To delete information:

no protocol <*protocol name*>

Input mode

```
(config-vlan)
```

Parameters

<*protocol name*>

Specifies the name of the protocol in a protocol-based VLAN. This command can be set only when the applicable VLAN is a protocol-based VLAN. If you want to use multiple protocols in a single VLAN, specify this command as many times as the number of protocol names.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Protocol name set by the `vlan-protocol` command.

Default behavior

No protocol is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To use a protocol VLAN with an IPv4 address or IPv6 address set, you must use this command to specify the applicable protocol.

Related commands

vlan-protocol

state

Sets the VLAN status.

Syntax

To set or change information:

state {suspend | active}

To delete information:

no state

Input mode

`(config-vlan)`

Parameters

{suspend | active}

suspend

Sets the VLAN status to `disable` and stops the sending and receiving of all frames.

active

Sets the VLAN status to `enable` and starts the sending and receiving of all frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `suspend` or `active`

Default behavior

The VLAN status is `enable`.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command can be set from the SNMP manager by using an SNMP SetRequest operation. If this command is set by using an SNMP SetRequest operation, the setting is applied to the configuration.

Related commands

None

switchport access

Sets access port information. The information you set is also applied to access VLANs of tunneling ports.

Syntax

To set or change information:

switchport access vlan <*vlan id*>

To delete information:

no switchport access vlan

Input mode

`(config-if)`

Parameters

vlan <*vlan id*>

Sets an interface to the access port for the specified VLAN (access VLAN). The access VLAN for the tunneling port is also the specified VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

In non-VLAN tunneling mode, the access port for the default VLAN (VLAN ID = 1) is used. The default behavior in VLAN tunneling mode is for switch ports to not belong to any VLAN and for communication with VLANs to be disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. In non-VLAN tunneling mode, if an untagged frame is received, it is handled by the access VLAN. If a tagged frame is received, it is discarded.
2. In VLAN tunneling mode, frames are handled by access VLANs irrespective of whether they have a VLAN tag.

Related commands

switchport mode

vlan

switchport dot1q ethertype

Sets the TPID (Tag Protocol IDentifier) value that identifies VLAN frames on a port. This command is set when you connect to a network in which a non-standard TPID value is used.

Syntax

To set or change information:

switchport dot1q ethertype <*hex*>

To delete information:

no switchport dot1q ethertype

Input mode

`(config-if)`

Parameters

<*hex*>

Sets the TPID value of a VLAN tag which is assigned by a Switch. This command sets the default value for ports.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0x8100

Default behavior

When the `vlan-dot1q-ethertype` command is set, the setting value for the command is regarded as the TPID value. When the `vlan-dot1q-ethertype` command is not set, 0x8100 is regarded as the TPID value.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For ports specified by using this command, the value specified for `vlan-dot1q-ethertype` is not applied.

Related commands

None

switchport mac

Sets MAC VLAN port information.

Syntax

To set information:

switchport mac vlan <*vlan id list*>

switchport mac native vlan <*vlan id*>

To change information:

switchport mac {vlan <*vlan id list*> | vlan add <*vlan id list*> | vlan remove <*vlan id list*> | native vlan <*vlan id*>}

To delete information:

no switchport mac vlan

no switchport mac native vlan

Input mode

`(config-if)`

Parameters

vlan <*vlan id list*>

Specifies the list of valid MAC VLANs that applies to a switch port. When this value is changed, a list of the currently-valid MAC VLANs replaces the specified list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

native vlan <*vlan id*>

Sets the VLAN that can receive frames with unregistered source MAC addresses. Frames can also be sent from the specified VLAN. Specifiable VLANs are port VLANs.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

vlan add <*vlan id list*>

Adds the currently-valid MAC VLANs for this port to the VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

vlan remove <*vlan id list*>

Removes the valid MAC VLANs for this port from the VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

Default behavior

None. If a MAC VLAN port has been set by using the `switchport mode` command with the `mac-vlan` parameter, and this command has not been set, only the default VLAN is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

If no valid MAC VLANs have been set, the port operates as an access port.

Related commands

switchport mode

vlan mac-based

switchport mode

Sets Layer 2 interface attributes.

Syntax

To set or change information:

switchport mode {access | trunk | protocol-vlan | mac-vlan | dot1q-tunnel }

To delete information:

no switchport mode {access | trunk | protocol-vlan | mac-vlan | dot1q-tunnel }

Input mode

```
(config-if)
```

Parameters

{access | trunk | protocol-vlan | mac-vlan | dot1q-tunnel}

Sets Layer 2 interface attributes.

access

Sets the applicable interface to access mode. When non-VLAN tunneling is used, untagged frames are sent or received in access mode. When VLAN tunneling is used, frames are sent or received in an access VLAN irrespective of whether the frames have a VLAN tag. Ports in access mode can be used only in a single VLAN.

trunk

Sets an interface to trunking mode. In trunking mode, untagged frames and tagged frames are sent and received.

protocol-vlan

Sets an interface to protocol VLAN mode. In protocol VLAN mode, untagged frames are sent and received. When a frame is received, the VLAN is determined by the protocol type of the frame. Tagged frames are discarded.

mac-vlan

Sets an interface to MAC VLAN mode. In MAC VLAN mode, untagged frames are sent and received. When a frame is received, the corresponding VLAN is determined from the source MAC address of the frame. Tagged frames are discarded.

dot1q-tunnel

Sets an interface to tunneling mode. In tunneling mode, frames are sent and received on an access VLAN irrespective of whether the frames have a VLAN tag.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   access, trunk, protocol-vlan, mac-vlan, or dot1q-tunnel

Default behavior

`access` (access mode) is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If an interface is set to trunking mode, set `allowed vlan` by using the `switchport trunk` command. If an interface is set to trunking mode and `allowed vlan` is not set, all frames on the applicable port are discarded.
2. If an interface is set to protocol VLAN mode, use the `switchport protocol` command to set a protocol VLAN. If protocol VLAN is not set, the applicable port operates as if it were in access mode.
3. If an interface is set to MAC VLAN mode, use the `switchport mac` command to set a MAC VLAN. If MAC VLAN is not set, the applicable port operates as if it were in access mode.
4. If an interface is set to tunneling mode, use the `switchport access` command to set an access VLAN. Ports in tunneling mode are not automatically added to the default VLAN. Even when the default VLAN is used as the access VLAN, use the `switchport access` command to explicitly enable the access VLAN. If access VLAN is not set, communication is not possible.

Related commands

None

switchport protocol

Sets protocol VLAN port information.

Syntax

To set information:

switchport protocol vlan <*vlan id list*>

switchport protocol native vlan <*vlan id*>

To change information:

switchport protocol {vlan <*vlan id list*> | vlan add <*vlan id list*> | vlan remove <*vlan id list*> | native vlan <*vlan id*>}

To delete information:

no switchport protocol vlan

no switchport protocol native vlan

Input mode

```
(config-if)
```

Parameters

vlan <*vlan id list*>

Sets the currently-valid protocol VLANs on the port. When this parameter is changed, the currently-valid protocol VLAN list replaces the specified list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

native vlan <*vlan id*>

Sets a VLAN that sends and receives frames of a protocol that does not match the configuration. Specifiable VLANs are port VLANs.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

vlan add <*vlan id list*>

Adds a currently-valid protocol VLAN on the port to the VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

vlan remove <*vlan id list*>

Removes a currently-valid protocol VLAN on the port from the VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

Default behavior

None. If a protocol VLAN port has been set by using the `switchport mode protocol` command, and this command is omitted, the default VLAN is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If no currently-valid protocol VLANs are set, the port operates as an access port.
2. If multiple protocol VLANs are set for a protocol VLAN port, be careful that you do not duplicate the protocols for the protocol VLAN.

Related commands

switchport mode

vlan protocol-based

vlan-protocol

switchport trunk

Sets trunk port information.

Syntax

To set information:

switchport trunk allowed vlan <*vlan id list*>

switchport trunk native vlan <*vlan id*>

To change information:

switchport trunk native vlan <*vlan id*>

switchport trunk allowed vlan {<*vlan id list*> | add <*vlan id list*> | remove <*vlan id list*>}

To delete information:

no switchport trunk allowed vlan

no switchport trunk native vlan

Input mode

`(config-if)`

Parameters

native vlan <*vlan id*>

Sets the native VLAN (VLAN that sends and receives untagged frames). Specifiable VLANs are port VLANs. If the native VLAN is not set explicitly, the default VLAN becomes the native VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

allowed vlan <*vlan id list*>

Sets the VLANs that use a trunk port for sending and receiving frames.

The frames of VLANs that have not been specified are discarded.

To send and receive untagged frames, you must specify the native VLAN. If you do not set the native VLAN to `allowed vlan`, untagged frames are discarded.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

add <*vlan id list*>

Adds a VLAN to the specified VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

remove <*vlan id list*>

Removes a VLAN from the specified VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

Default behavior

None. If trunking mode has been set by using the `switchport mode trunk` command and this command is omitted, communication is not possible.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

If an interface is set to trunking mode, you must set `allowed vlan`. If `allowed vlan` is not set, no frames will be sent from or received at the applicable interface.

Related commands

switchport mode

vlan

switchport vlan mapping

Sets tag translation information entries.

Syntax

To set or change information:

switchport vlan mapping <*vlan tag*> <*vlan id*>

To delete information:

no switchport vlan mapping <*vlan tag*> <*vlan id*>

Input mode

`(config-if)`

Parameters

<*vlan tag*>

Specifies the VLAN tag value used in a LAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4095

<*vlan id*>

Specifies the VLAN ID of a VLAN that handles frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

Tag translation is not performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To enable tag translation, you must specify `switchport vlan mapping enable`.
2. Tag translation is enabled only when the applicable port is in trunking mode.
3. Tag translation does not have an effect on the frames handled by the native VLAN, because frames which are sent or received by it have no VLAN tags. Do not specify the VLAN ID of the native VLAN for a VLAN tag or the VLAN ID. Alternatively, use the `vlan dot1q tag native` command to add VLAN tags to frames that are sent by the native VLAN and use them as the tagged frames.

Related commands

switchport mode trunk

switchport trunk

switchport vlan mapping enable

vlan dot1q tag native

switchport vlan mapping enable

Enables tag translation.

Syntax

To set information:

```
switchport vlan mapping enable
```

To delete information:

```
no switchport vlan mapping enable
```

Input mode

`(config-if)`

Parameters

None

Default behavior

Tag translation is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To enable tag translation, you must specify `switchport vlan mapping`.
2. Tag translation is enabled only when the applicable port is in trunking mode.
3. When tag translation is enabled for a port, do not set the TPID value to other than `0x8100`.

Related commands

switchport mode

switchport trunk

switchport vlan mapping

up-debounce

Sets the up-determination time for a VLAN interface after the VLAN interface goes down until another port in the VLAN comes up again as a port that can be used for communication.

Syntax

To set or change information:

up-debounce <*seconds*> [extend]

To delete information:

no up-debounce

Input mode

`(config-if) This can be set only for VLAN interfaces.`

Parameters

<*seconds*>

Sets the up-determination time (in seconds) for a VLAN interface when another port in the VLAN comes up as a port that can be used for communication.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3600

extend

Increases the chances for the VLAN debounce functionality to operate when the VLAN interface up and enables the functionality when the following occurs:

- When the Switch starts up
- When the `restart vlan` operation command is executed
- When the running configuration is changed by using the `copy` operation command
- When the VLAN status is changed from `disable` to `enable` by using the `state` command

1. Default value when this parameter is omitted:

   The chances for the VLAN debounce functionality to operate are not increased.

2. Range of values:

   None

Default behavior

If a port in the VLAN comes up, and becomes available to restore communication, the VLAN interface comes up immediately.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When systems are switched, if there is a port that can be used for communication, the VLAN interface comes up immediately regardless of whether `extend` is specified.
2. For a VLAN interface, if the setting value is changed during the up-determination time, the VLAN interface goes up after the changed setting value elapses since the time when the value was changed.
3. If the setting value is deleted during the up-determination time of a VLAN interface, the interface goes up when the value was deleted.

Related commands

None

vlan

Sets VLAN-related items.

Syntax

To set information:

vlan <*vlan id*>

vlan <*vlan id list*>

vlan <*vlan id*> protocol-based

vlan <*vlan id list*> protocol-based

vlan <*vlan id*> mac-based

vlan <*vlan id list*> mac-based

To delete information:

no vlan <*vlan id*>

no vlan <*vlan id list*>

Input mode

`(config)`

Parameters

<*vlan id*>

Specifies a VLAN ID. When this command is entered, the mode switches to `config-vlan` mode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*. Note, however, that the default VLAN (VLAN ID = 1) cannot be specified when information is deleted.

<*vlan id list*>

Specifies multiple VLAN IDs at one time. If you specify a VLAN ID for the first time, the applicable VLAN is newly created. When this command is entered, the mode switches to `config-vlan` mode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note, however, that the default VLAN (VLAN ID = 1) cannot be specified when information is deleted.

protocol-based

Specify this parameter for a protocol VLAN.

1. Default value when this parameter is omitted:

   The VLANs become port-based VLANs.

2. Note on using this parameter:

   - To specify protocol VLANs, you must specify `protocol-based`.

   - This parameter cannot be specified for any VLAN which has already been created as a port-based VLAN or a MAC VLAN.

   - This parameter and the VLAN tunneling functionality cannot be used at the same time.

mac-based

Specifies this parameter for MAC VLANs.

1. Default value when this parameter is omitted:

   The VLANs become port-based VLANs.

2. Note on using this parameter:

   - When specifying MAC VLANs, you must specify `mac-based`.

   - This parameter cannot be specified for any VLAN which has already been created as a port-based VLAN or a protocol-based VLAN

   - This parameter and the VLAN tunneling functionality cannot be used at the same time.

Default behavior

No VLANs are configured.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. There is always a default VLAN (VLAN ID = 1). The configuration items for the default VLAN are different from those of other normal VLANs.

2. If you specify a list by using <*vlan id list*>, you can configure multiple VLANs at the same time. Note, however, that if a list is specified (for multi-command mode) some commands cannot be used. For details, see the following table.

Table 15-1: Command availability in multi-command mode

#	Command	Available in multi-command mode
1	state {suspend | active}	Y
2	name	N
3	protocol	Y
4	mac-address	N
5	vlan-mac	Y

Legend Y: Can be used; N: Cannot be used

3. The default VLAN setting (`VLAN ID=1`) always exists in the configuration file and cannot be deleted. The initial state of the default VLAN is for all ports to be available as access ports.

4. The table below explains parameter items that can be set for the default VLAN, and behavior specific to the default VLAN.

   `vlan` command:

The following table applies to the `vlan` command.

Table 15-2: Handling default VLAN parameters

#	Parameter	Whether specifiable by the user	Behavior specific to the default VLAN
1	*<vlan id>*	F (fixed value)	Set when the Switch is started. Fixed at `1`. Cannot be changed or deleted.
2	*<vlan id list>*	N	--
3	protocol-based	N	Port VLAN
4	mac-based	N	Port VLAN

Legend F: Can be set as a fixed value; N: Cannot be set; --: Not applicable

`config-vlan` mode command:

The following table applies to the `config-vlan` mode command.

Table 15-3: Handling default VLAN parameters

#	Command	Parameter	Whether specifiable by the user	Behavior specific to the default VLAN
1	state {suspend | active}	--	Y	--
2	name	*<strings>*	Y	--
3	protocol	*<Protocol Name list>*	N	--
4	mac-address	*<MAC>*	N	--
5	vlan-mac	--	Y	--

Legend Y: Can be set; N: Cannot be set; --: Not applicable

5. When the `vlan` command is used to create a VLAN, information can be set for the VLAN interface by using the `interface vlan` command. For VLANs created by using the `vlan` command, use the `no interface vlan` command to delete information. For a VLAN created by using the `interface vlan` command, use the `no vlan` command to delete information.

Related commands

None

vlan-dot1q-ethertype

Sets the TPID for a VLAN tag.

Syntax

To set or change information:

vlan-dot1q-ethertype <*hex*>

To delete information:

no vlan-dot1q-ethertype

Input mode

`(config)`

Parameters

<*hex*>

Sets the TPID value of a VLAN tag which is assigned by a Switch. This command sets the default value of the entire Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Four-digit hexadecimal

Default behavior

`0x8100` is used as the TPID value. Note, however, that lines for which `switchport dot1q ethertype` is set, the setting value is used as the TPID value.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

vlan dot1q tag native

Adds a VLAN tag to frames that are sent in the native VLAN of a trunk port so that the frames can be treated as tagged frames.

Syntax

To set information:

vlan dot1q tag native

To delete information:

no vlan dot1q tag native

Input mode

`(config)`

Parameters

None

Default behavior

Frames that are sent in the native VLAN of a trunk port are sent as untagged frames without adding VLAN tags.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When `vlan dot1q tag native` is set, untagged frames are discarded by trunk ports.

Related commands

None

vlan-mac

Sets MAC addresses to be used for each VLAN. When L3 forwarding is performed, if you change the MAC used by a Switch on a per-VLAN basis, this makes operation easier when you connect to a Switch that does not perform MAC learning on a per-VLAN basis.

It is not necessary to set this command for VLANs which do not perform Layer 3 forwarding.

Syntax

To set information:

```
vlan-mac
```

To delete information:

```
no vlan-mac
```

Input mode

`(config-vlan)`

Parameters

None

Default behavior

Each switch uses one MAC address.

Impact on communication

Setting the `vlan-mac` command changes the MAC address reported by a Switch when the Switch performs Layer 3 forwarding (including both frames originated by and frames addressed to and forwarded by the Switch) from the MAC address of the Switch to an individual MAC address for each VLAN (deleting the command is the reverse of setting it). Because of this, if this command is set for an already-operating VLAN, MAC addresses learned, using the ARP protocol, by neighboring Layer 3 devices (routers, Layer 3 switches, or terminals) no longer match the MAC address reported for each VLAN of the Switch. As a result, communication might be disabled temporarily.

When the change is applied

If `vlan-mac-prefix` has been set, the change takes effect immediately after the setting value is changed. If `vlan-mac-prefix` has not been set, no change takes effect until `vlan-mac-prefix` is set.

Notes

None

Related commands

vlan-mac-prefix

vlan-mac-prefix

Sets an individual MAC address prefix for each VLAN.

Syntax

To set or change information:

vlan-mac-prefix <*mac*> <*mask*>

To delete information:

no vlan-mac-prefix

Input mode

`(config)`

Parameters

<*mac*> <*mask*>

Sets an individual MAC address to be used for each VLAN. Uses <*mac*> <*mask*> specified by using this command as the template, and automatically generates an MAC address for each VLAN by setting numbers corresponding to the VLAN in the lower order bits.

<*mac*>

Specifies the MAC address prefix.

<*mask*>

Specifies the mask for (pattern of high-order bits of) <*mac*> that are to be used unchanged.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   mask: Bit pattern with highest 8 to 34 bits turned `on`

3. Note on using this parameter:

   Multicast MAC addresses[#] cannot be set.

   #: An address in which the lowest bit of the first byte is 1.

Default behavior

The Switch MAC is used.

Impact on communication

If the `vlan-mac` command is set for a VLAN, when Layer 3 forwarding is performed by the VLAN (including both frames originated by, and frames addressed to and forwarded by, the Switch) the MAC address reported by the Switch for frames on that VLAN is changed. Because of this, the MAC addresses learned using ARP protocol by neighboring Layer 3 devices (routers, Layer 3 switches, or terminals) no longer match the MAC addresses reported for each VLAN of the Switch. As a result, communication might not be possible temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

vlan-mac

vlan-protocol

Sets the protocol name and protocol value for a protocol VLAN.

Syntax

To set or change information:

vlan-protocol <*protocol name*> [ethertype <*hex*>...] [llc <*hex*>...] [snap-ethertype <*hex*>...]

To delete information:

no vlan-protocol <*protocol name*>

Input mode

```
(config)
```

Parameters

<*protocol name*>

Sets the protocol name used for configuring the protocol VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   A string with 14 or fewer characters

ethertype <*hex*>

Specifies the EtherType value for an Ethernet V2-format frame.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Four-digit hexadecimal

3. Note on using this parameter:

   EtherType values which have already been set by users cannot be specified.

llc <*hex*>

Sets the LLC value (DSAP, SSAP) of an 802.3-format frame.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Four-digit hexadecimal

3. Note on using this parameter:

   LLC values which have already been set by users cannot be specified.

snap-ethertype <*hex*>

Specifies the EtherType value for an 802.3-format frame.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Four-digit hexadecimal

3. Note on using this parameter:

   EtherType values which have already been set by users cannot be specified.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed. Note, however, that for protocols that have not been specified by the `protocol` command for the protocol VLAN, the change is applied when the protocol name is specified by the `protocol` command.

Notes

None

Related commands

protocol

Chapter

16. Spanning Tree Protocol

instance
name
revision
spanning-tree bpdufilter
spanning-tree bpduguard
spanning-tree cost
spanning-tree disable
spanning-tree guard
spanning-tree link-type
spanning-tree loopguard default
spanning-tree mode
spanning-tree mst configuration
spanning-tree mst cost
spanning-tree mst forward-time
spanning-tree mst hello-time
spanning-tree mst max-age
spanning-tree mst max-hops
spanning-tree mst port-priority
spanning-tree mst root priority
spanning-tree mst transmission-limit
spanning-tree pathcost method
spanning-tree port-priority
spanning-tree portfast
spanning-tree portfast bpduguard default
spanning-tree portfast default
spanning-tree single
spanning-tree single cost
spanning-tree single forward-time
spanning-tree single hello-time
spanning-tree single max-age
spanning-tree single mode
spanning-tree single pathcost method
spanning-tree single port-priority
spanning-tree single priority
spanning-tree single transmission-limit
spanning-tree vlan
spanning-tree vlan cost
spanning-tree vlan forward-time
spanning-tree vlan hello-time
spanning-tree vlan max-age
spanning-tree vlan mode
spanning-tree vlan pathcost method
spanning-tree vlan port-priority
spanning-tree vlan priority
spanning-tree vlan transmission-limit

instance

Sets VLANs belonging to Multiple Spanning Tree MST instances.

Syntax

To set or change information:

instance <*mst instance id*> vlans <*vlan range*>

To delete information:

no instance <*mst instance id*>

Input mode

```
(config-mst)
```

Parameters

<*mst instance id*>

Sets an MST instance ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 4095

vlans <*vlan range*>

Sets VLANs belonging to MST instances. One VLAN ID can be set. You can use hyphens (`-`) or commas (`,`) to set multiple VLAN IDs at the same time.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4095

3. Note on using this parameter:

   - All VLANs that do not belong to other MST instances participate in MST instance ID0.

   - To configure the same MST region, the MST instance ID and the VLAN ID set by this parameter, as well as the values of the `name` parameter and the `revision` parameter, must match within the MST region.

Default behavior

All VLANs belong to MST instance ID0.

Impact on communication

When the `spanning-tree mode` command is used to set `mst`, communications are interrupted until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The `show` command does not display information about MST instance ID0.

2. When the Ring Protocol and Multiple Spanning Tree are used together, the VLAN IDs of VLANs specified by this command and the VLAN IDs specified by VLAN mapping for the Ring Protocol must match. Unmatched VLANs are put in the Blocking status.

Related commands

spanning-tree mst configuration

name

Sets a string to identify a Multiple Spanning Tree region.

Syntax

To set or change information:

name <*name*>

To delete information:

no name

Input mode

`(config-mst)`

Parameters

<*name*>

Sets the character string used to identify a region.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

3. Note on using this parameter:

   To configure the same MST region, the values for this parameter and the `revision` parameter, as well as those of the MST instance ID and the VLAN ID set by the `vlans` parameter, must match within the MST region.

Default behavior

`name` is set to `NULL`.

Impact on communication

When the `spanning-tree mode` command is used to set `mst`, communications are interrupted until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

spanning-tree mst configuration

revision

Sets revision numbers to identify Multiple Spanning Tree regions.

Syntax

To set or change information:

revision <*version*>

To delete information:

no revision

Input mode

```
(config-mst)
```

Parameters

<*version*>

Sets the revision number to identify a region.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

3. Note on using this parameter:

   To configure the same MST region, the values for this parameter and the `name` parameter, as well as those of the MST instance ID and the VLAN ID set by the `vlans` parameter, must match within the MST region.

Default behavior

`revision` is set to 0.

Impact on communication

When the `spanning-tree mode` command is used to set `mst`, communications are interrupted until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

spanning-tree mst configuration

spanning-tree bpdufilter

Sets the BPDU filter functionality for the applicable ports. This command is applied to the applicable ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set information:

```
spanning-tree bpdufilter enable
```

To delete information:

```
no spanning-tree bpdufilter
```

Input mode

```
(config-if)
```

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is set, the BPDU guard functionality is not valid.
2. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

None

spanning-tree bpduguard

Sets the BPDU guard functionality for the applicable ports. This command is applied to the applicable ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree), and operates on a port for which the PortFast functionality has been set.

Syntax

To set or change information:

spanning-tree bpduguard { enable | disable }

To delete information:

no spanning-tree bpduguard

Input mode

`(config-if)`

Parameters

{ enable | disable }

Setting `enable` causes the BPDU guard functionality to take effect. Setting `disable` stops operation of the BPDU guard functionality.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `enable` or `disable`

Default behavior

The setting of the `spanning-tree portfast bpduguard default` command is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree portfast default

spanning-tree portfast

spanning-tree portfast bpduguard default

spanning-tree cost

Sets the path cost of the applicable port. This command is applied to all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set or change information:

spanning-tree cost <*cost*>

To delete information:

no spanning-tree cost

Input mode

```
(config-if)
```

Parameters

<*cost*>

Specifies the path cost value. The lower the <*cost*> value, the higher the possibility that the port will be used for forwarding the applicable frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   When `short` is set by the `spanning-tree pathcost method` command:

   1 to 65535

   When `long` is set by the `spanning-tree pathcost method` command:

   1 to 200000000

3. Note on using this parameter:

   Changing the path cost value might change the topology.

Default behavior

The method of applying the path cost is set by the `spanning-tree pathcost method` command.

`1` is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the `spanning-tree vlan cost` command, the `spanning-tree single cost` command, or the `spanning-tree mst cost` command is set, the value of this command is not applied.
2. When the `spanning-tree vlan pathcost method` command or the `spanning-tree single pathcost method` command is set, the value of this command is not applied.
3. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree pathcost method

spanning-tree vlan pathcost method

spanning-tree vlan cost

spanning-tree single pathcost method

spanning-tree single cost

spanning-tree mst cost

spanning-tree disable

Stops operation of the Spanning Tree functionality for all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set information:

spanning-tree disable

To delete information:

no spanning-tree disable

Input mode

`(config)`

Parameters

None

Default behavior

The Spanning Tree Protocols are enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When a GSRP global configuration exists, the `no spanning-tree disable` command cannot be set.

Related commands

None

spanning-tree guard

Sets the guard functionality for the applicable ports. This command is applied to the applicable ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set or change information:

spanning-tree guard { loop | none | root }

To delete information:

no spanning-tree guard

Input mode

`(config-if)`

Parameters

{ loop | none | root }

If `loop` is set, the loop guard functionality is applied to the applicable ports. The loop guard functionality does not operate for Multiple Spanning Tree.

If `none` is set, the guard functionality of the applicable port is stopped.

If `root` is set, the root guard functionality is applied to the applicable ports.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `loop`, `none`, or `root`

Default behavior

The setting of the `spanning-tree loopguard default` command is used.

Impact on communication

When loop guard functionality is set for a port or channel group that does not receive BPDU, even after one such port comes up, communications of the port might remain disabled, or it might take time until communication is enabled.

When the change is applied

When settings for the `spanning-tree portfast default` command or the `spanning-tree portfast` command are deleted, if you change the configuration stored in memory without setting the `spanning-tree portfast default` command or the `spanning-tree portfast` command, the changes take effect immediately after the change.

Notes

1. If the `spanning-tree portfast default` command or the `spanning-tree portfast` command is set, the changes are not applied.
2. After the loop guard functionality is set, if a switch starts, systems are switched, a port (including a port in a channel group or NIF) comes up, a spanning tree program is restarted, or the spanning tree protocol type is changed, the loop guard functionality operates and the port is blocked. The loop guard functionality is not cleared until a BPDU is received.
3. If loop guard functionality is set while a port is on line, the functionality is not enabled. Loop guard functionality, set while a port is on line, is enabled when a BPDU reception timeout

occurs.

4. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree loopguard default

spanning-tree link-type

Sets the link type of the applicable port. This command is applied to the applicable ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree). If you want to change the high-speed topology when `rapid-pvst` or `mst` is set by the `spanning-tree mode` command, and `rapid-pvst` is set by the `spanning-tree vlan mode` command, the connection between bridges must be a point-to-point connection. If you want to change the high-speed topology when `rapid-stp` is set by the `spanning-tree single mode` command, the connection between bridges must be a point-to-point connection.

Syntax

To set or change information:

spanning-tree link-type { point-to-point | shared }

To delete information:

no spanning-tree link-type

Input mode

`(config-if)`

Parameters

{ point-to-point | shared }

If `point-to-point` is set, point-to-point connection is used for the link type. If `shared` is set, a shared connection is used for the link type.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `point-to-point` or `shared`

Default behavior

`point-to-point` is used for a full-duplex port and `shared` is used for a half-duplex port.

`point-to-point` is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The automatic restoration functionality is enabled if `point-to-point` is set in STP compatibility mode. The automatic restoration functionality does not operate if `shared` is set in STP compatibility mode.
2. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree mode

spanning-tree vlan mode

spanning-tree single mode

spanning-tree loopguard default

Sets the loop guard functionality that is used by default. This command is valid for ports of all Spanning Tree Protocols (PVST+ and Single Spanning Tree).

Syntax

To set information:

spanning-tree loopguard default

To delete information:

no spanning-tree loopguard default

Input mode

`(config)`

Parameters

None

Default behavior

If the `spanning-tree guard` command is set, that setting is used. If the `spanning-tree guard` command is not set, this command has no effect.

Impact on communication

When loop guard functionality is set for a port or channel group that does not receive BPDU, even after one such port comes up, communications of the port might remain disabled, or it might take time until communication is enabled.

When the change is applied

When settings for the `spanning-tree portfast default` command or the `spanning-tree portfast` command are deleted, if you change the configuration stored in memory without setting the `spanning-tree portfast default` command or the `spanning-tree portfast` command, the changes take effect immediately after the change.

Notes

1. If the `spanning-tree portfast default` command or the `spanning-tree portfast` command are set, the changes are not applied.
2. After the loop guard functionality is set, if a switch starts, systems are switched, a port (including a port in a channel group or NIF) comes up, a spanning tree program is restarted, or the spanning tree protocol type is changed, the loop guard functionality operates and the port is blocked. The loop guard functionality is not cleared until a BPDU is received.
3. If loop guard functionality is set while a port is on line, the functionality is not enabled. Loop guard functionality, set while a port is on line, is enabled when a BPDU reception timeout occurs.
4. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree guard

spanning-tree mode

The following explains settings for the Spanning Tree operating mode. This command applies to all Spanning Tree Protocols (PVST+ and Multiple Spanning Tree) other than Single Spanning Tree. If the `spanning-tree vlan mode` command is set in a PVST+ operating mode, the settings for that command are used.

Syntax

To set or change information:

spanning-tree mode { pvst | rapid-pvst | mst }

To delete information:

no spanning-tree mode

Input mode

`(config)`

Parameters

{ pvst | rapid-pvst | mst }

Sets the protocol to be used. If the protocol is changed during Spanning Tree operation, the Spanning Tree Protocol is re-initialized. If `pvst` is set, PVST+ is applied to all Spanning Tree Protocols. If `rapid-pvst` is set, rapid PVST+ is applied to all Spanning Tree Protocols. If `mst` is set, Multiple Spanning Tree is applied to all Spanning Tree Protocols. For Single Spanning Tree, `pvst` or `rapid-pvst` must be set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `pvst`, `rapid-pvst`, or `mst`

Default behavior

The configuration is explicitly set to `spanning-tree mode pvst`.

Impact on communication

Communication stops until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

spanning-tree link-type

spanning-tree mst configuration

Switches to `config-mst` mode in which you can set the information necessary for defining Multiple Spanning Tree regions. If this setting is deleted, all previously-set information for defining regions is deleted.

Syntax

To set information:

spanning-tree mst configuration

To delete information:

no spanning-tree mst configuration

Input mode

`(config)`

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

instance

name

revision

spanning-tree mst cost

Sets the path cost for the applicable Multiple Spanning Tree ports.

Syntax

To set or change information:

spanning-tree mst <*mst instance id list*> cost <*cost*>

To delete information:

no spanning-tree mst <*mst instance id list*> cost

Input mode

`(config-if)`

Parameters

<*mst instance id list*>

Sets an MST instance ID. One MST instance ID can be set. You can use hyphens (`-`) or commas (`,`) to set multiple MST instance IDs at one time.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 4095

<*cost*>

Specifies the path cost value. The lower the <*cost*> value, the higher the possibility that the port will be used for forwarding the applicable frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 200000000

3. Note on using this parameter:

   Changing the path cost value might change the topology.

Default behavior

The setting of the `spanning-tree cost` command is used.

`1` is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When setting information by using the `interface range` command, you cannot set multiple MST instance IDs at one time. Set one MST instance ID.

2. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree cost

spanning-tree mst forward-time

Sets the time required for a Multiple Spanning Tree state transitions.

Syntax

To set or change information:

spanning-tree mst forward-time <*seconds*>

To delete information:

no spanning-tree mst forward-time

Input mode

```
(config)
```

Parameters

<*seconds*>

Specifies the time in seconds required for the state of a port to change.

For ports in stp-compatible mode, only listening and learning states can be maintained for the specified period of time. If a port is not in stp-compatible mode, only discarding and learning states are maintained for the specified period of time (note that this applies only when a timer causes a state transition).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   4 to 30

Default behavior

The time required for the state of a port to change is set to 15 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree mst hello-time

Sets the interval for sending BPDUs in Multiple Spanning Tree.

Syntax

To set or change information:

spanning-tree mst hello-time <*hello time*>

To delete information:

no spanning-tree mst hello-time

Input mode

```
(config)
```

Parameters

<*hello time*>

Specifies the interval in seconds for sending BPDUs that are sent regularly from the Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

3. Note on using this parameter:

   If you set 1 then this might result in a changeable topology.

Default behavior

The interval for sending BPDUs is set to 2.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree mst max-age

Sets the maximum valid time of BPDUs that are sent via Multiple Spanning Tree.

Syntax

To set or change information:

spanning-tree mst max-age <*seconds*>

To delete information:

no spanning-tree mst max-age

Input mode

```
(config)
```

Parameters

<*seconds*>

Sets the maximum valid time in seconds for BPDUs that are sent from the Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   6 to 40

3. Note on using this parameter:

   If you set a value less than 20, then this might result in a changeable topology.

Default behavior

The maximum valid time of BPDUs that can be sent from a Switch is set to 20 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree mst max-hops

Sets the maximum-number-of-hops count for BPDUs in Multiple Spanning Tree.

Syntax

To set or change information:

spanning-tree mst max-hops <*hop number*>

spanning-tree mst <*mst instance id list*> max-hops <*hop number*>

To delete information:

no spanning-tree mst max-hops

no spanning-tree mst <*mst instance id list*> max-hops

Input mode

`(config)`

Parameters

<*mst instance id list*>

Sets an MST instance ID. One MST instance ID can be set. You can use hyphens (-) or commas (,) to set multiple MST instance IDs at one time.

1. Default value when this parameter is omitted:

   All MST instances are selected.

2. Range of values:

   0 to 4095

<*hop number*>

Specifies the maximum-number-of-hops count for BPDUs forwarded by the Switch.

1. Default value when this parameter is omitted:

   20

2. Range of values:

   2 to 40

Default behavior

The maximum-number-of-hops count for BPDUs is set to 20.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree mst port-priority

Sets the priority of the applicable Multiple Spanning Tree ports for each MST instance.

Syntax

To set or change information:

spanning-tree mst <*mst instance id list*> port-priority <*priority*>

To delete information:

no spanning-tree mst <*mst instance id list*> port-priority

Input mode

`(config-if)`

Parameters

<*mst instance id list*>

Sets an MST instance ID. One MST instance ID can be set. You can use hyphens (`-`) or commas (`,`) to set multiple MST instance IDs at one time.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 4095

<*priority*>

Sets the port priority. Use a multiple of 16 as the port priority. The lower the value, the higher the priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 240

3. Note on using this parameter:

   Changing the port priority might change the topology.

Default behavior

The setting of the `spanning-tree port-priority` command is used. If the `spanning-tree port-priority` command has not been set, the port priority is set to 128.

`0` is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When setting information by using the `interface range` command, you cannot set multiple MST instance IDs at one time. Set one MST instance ID.

2. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree port-priority

spanning-tree mst root priority

Sets the bridge priority for each MST instance in Multiple Spanning Tree.

Syntax

To set or change information:

spanning-tree mst <*mst instance id list*> root priority <*priority*>

To delete information:

no spanning-tree mst <*mst instance id list*> root priority

Input mode

```
(config)
```

Parameters

<*mst instance id list*>

Sets an MST instance ID. One MST instance ID can be set. You can use hyphens (-) or commas (,) to set multiple MST instance IDs at one time.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 4095

<*priority*>

Sets the bridge priority. The lower the value, the higher the priority. Use a multiple of 4096 as the bridge priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 61440

3. Note on using this parameter:

   Changing the bridge priority might change the topology.

Default behavior

The bridge priority is set to 32768.

When both Spanning Tree Protocols and the Ring Protocol are used together, 0 is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree mst transmission-limit

Sets the maximum number of BPDUs that can be sent during each hello-time interval for Multiple Spanning Tree.

Syntax

To set or change information:

spanning-tree mst transmission-limit <*count*>

To delete information:

no spanning-tree mst transmission-limit

Input mode

`(config)`

Parameters

<*count*>

Sets the maximum number of BPDUs that can be sent per hello-time interval.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The maximum number of BPDUs that can be sent is set to 3.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree pathcost method

Sets whether to use 16-bit values or 32-bit values as the path cost of ports. This command applies to all Spanning Tree Protocols (PVST+ and Single Spanning Tree) other than Multiple Spanning Tree.

When the `spanning-tree vlan pathcost method` command or the `spanning-tree single pathcost method` command is set, the value of this command is not applied.

If setting of the `spanning-tree cost`, `spanning-tree vlan cost`, or `spanning-tree single cost` command is omitted, the following value is applied to the path cost according to the interface speed and the `spanning-tree pathcost method` command settings:

- When `short` is set by the `spanning-tree pathcost method` command:

  10 Mbit/s: 100

  100 Mbit/s: 19

  1 Gbit/s: 4

  10 Gbit/s: 2

- When `long` is set by the `spanning-tree pathcost method` command:

  10 Mbit/s: 2000000

  100 Mbit/s: 200000

  1 Gbit/s: 20000

  10 Gbit/s: 2000

Syntax

To set or change information:

spanning-tree pathcost method { long | short }

To delete information:

no spanning-tree pathcost method

Input mode

`(config)`

Parameters

{ long | short }

If `long` is set, a 32-bit value is used. If `short` is set, a 16-bit value is used.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `long` or `short`

3. Note on using this parameter:

   - The default value of the path cost changes.

   - Changing the path cost value might change the topology.

   - If the path cost value is set to 65536 or larger, you cannot change the parameter to `short`.

Default behavior

`short` is set by path cost mode.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When `mst` is set by the `spanning-tree mode` command, the Multiple Spanning Tree operates using a 32-bit value. To set a value of 65536 or larger for the path cost using the `spanning-tree cost` command, you must set `long` for this command.

   You do not need to set this command before setting a path cost value using the `spanning-tree mst cost` command.

Related commands

spanning-tree cost

spanning-tree vlan pathcost method

spanning-tree vlan cost

spanning-tree single pathcost method

spanning-tree single cost

spanning-tree port-priority

Sets the port priority of the applicable ports. This command is applied to all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set or change information:

spanning-tree port-priority <*priority*>

To delete information:

no spanning-tree port-priority

Input mode

```
(config-if)
```

Parameters

<*priority*>

Sets the port priority. Use a multiple of 16 as the port priority. The lower the value, the higher the priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 240

3. Note on using this parameter:

   Changing the port priority might change the topology.

Default behavior

The settings of the `spanning-tree vlan port-priority`, `spanning-tree single port-priority`, or `spanning-tree mst port-priority` command are used. If the command described here has not been set, the port priority is set to 128.

`0` is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree vlan port-priority

spanning-tree single port-priority

spanning-tree mst port-priority

spanning-tree portfast

Sets the PortFast functionality for the applicable ports. This command is applied to the applicable ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set or change information:

spanning-tree portfast [{ trunk | disable }]

To delete information:

no spanning-tree portfast

Input mode

`(config-if)`

Parameters

{ trunk | disable }

If `trunk` is set, the PortFast functionality is applied to access, trunk, protocol, and MAC ports.

If `disable` is set, the PortFast functionality stops.

1. Default value when this parameter is omitted:

   The PortFast functionality, which is enabled on access, protocol, and MAC ports, is applied.

2. Range of values:

   `trunk` or `disable`

Default behavior

The setting of the `spanning-tree portfast default` command is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree portfast default

spanning-tree portfast bpduguard default

Sets the BPDU guard functionality to be used by default. This command is valid for all ports (PVST+, Single Spanning Tree, and Multiple Spanning Tree) on which the PortFast functionality is set.

Syntax

To set information:

spanning-tree portfast bpduguard default

To delete information:

no spanning-tree portfast bpduguard default

Input mode

`(config)`

Parameters

None

Default behavior

If the `spanning-tree bpduguard` command is set, that setting is used. If the `spanning-tree bpduguard` command is not set, this command does not operate.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree portfast default

spanning-tree portfast

spanning-tree bpduguard

spanning-tree portfast default

Sets the PortFast functionality to be used by default. This command is valid on the access, protocol, and MAC ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set information:

spanning-tree portfast default

To delete information:

no spanning-tree portfast default

Input mode

`(config)`

Parameters

None

Default behavior

If the `spanning-tree portfast` command has been set, that setting is used. If the `spanning-tree portfast` command has not been set, this command does not operate.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree portfast

spanning-tree loopguard default

spanning-tree guard

spanning-tree single

Starts calculation of the topology for Single Spanning Tree. If the Spanning Tree operating mode is PVST+, VLAN 1 is treated as Single Spanning Tree after this command is executed.

Syntax

To set information:

spanning-tree single

To delete information:

no spanning-tree single

Input mode

```
(config)
```

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If VLAN 1 was subject to PVST+ before this command was executed, executing this command stops PVST+ for VLAN 1. Removing Single Spanning Tree causes PVST+ to be applied to VLAN 1. If the operating mode is Multiple Spanning Tree, Single Spanning Tree does not operate.

Related commands

spanning-tree mode

spanning-tree single cost

Sets the path cost for the applicable Single Spanning Tree ports.

Syntax

To set or change information:

spanning-tree single cost <*cost*>

To delete information:

no spanning-tree single cost

Input mode

`(config-if)`

Parameters

<*cost*>

Specifies the path cost value. The lower the <*cost*> value, the higher the possibility that the port will be used for forwarding the applicable frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   When `short` is set by the `spanning-tree pathcost method` or the `spanning-tree single pathcost method` command:

   1 to 65535

   When `long` is set by the `spanning-tree pathcost method` or the `spanning-tree single pathcost method` command:

   1 to 200000000

3. Note on using this parameter:

   Changing the path cost value might change the topology.

Default behavior

The path cost is applied according to the setting of the `spanning-tree single pathcost method` command.

`1` is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree cost

spanning-tree pathcost method

spanning-tree single pathcost method

spanning-tree single forward-time

Sets the time required for the state of Single Spanning Tree to change.

Syntax

To set or change information:

spanning-tree single forward-time <*seconds*>

To delete information:

no spanning-tree single forward-time

Input mode

`(config)`

Parameters

<*seconds*>

Specifies the time in seconds required for the state of a port to change.

If `stp` (802.1D) is set by the `spanning-tree single mode` command, the listening state and the learning state are maintained for the specified period of time. If `rapid-stp` (802.1w) is set by the `spanning-tree single mode` command, the discarding state and the learning state are maintained for the set period of time (note that this applies only when a timer causes the transition).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   4 to 30

Default behavior

The time required for the state of a port to change is set to 15 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

spanning-tree single mode

spanning-tree single hello-time

Sets the interval for sending Single Spanning Tree BPDUs.

Syntax

To set or change information:

spanning-tree single hello-time <*hello time*>

To delete information:

no spanning-tree single hello-time

Input mode

`(config)`

Parameters

<*hello time*>

Specifies the interval in seconds for sending BPDUs that are sent regularly from the Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

3. Note on using this parameter:

   If you set 1 then this might result in a changeable topology.

Default behavior

The interval for sending BPDUs is set to 2.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree single max-age

Sets the maximum valid time of BPDUs that are sent via Single Spanning Tree.

Syntax

To set or change information:

spanning-tree single max-age <*seconds*>

To delete information:

no spanning-tree single max-age

Input mode

```
(config)
```

Parameters

<*seconds*>

Sets the maximum valid time in seconds for BPDUs that are sent from the Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   6 to 40

3. Note on using this parameter:

   If you set a value less than 20, then this might result in a changeable topology.

Default behavior

The maximum valid time of BPDUs that can be sent from a Switch is set to 20 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree single mode

Sets the operating mode of Single Spanning Tree.

Syntax

To set or change information:

spanning-tree single mode { stp | rapid-stp }

To delete information:

no spanning-tree single mode

Input mode

`(config)`

Parameters

{ stp | rapid-stp }

Sets the protocol to be used. If the protocol is changed during Spanning Tree operation, the Spanning Tree Protocol is re-initialized. If `stp` is set, Spanning Tree mode is used. If `rapid-stp` is set, rapid Spanning Tree mode is used.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `stp` or `rapid-stp`

Default behavior

`stp` is set for the Single Spanning Tree operating mode.

Impact on communication

If the `spanning-tree single` command is set, communications are interrupted until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree single pathcost method

Sets whether to use a 16-bit value or a 32-bit value as the path cost for Single Spanning Tree ports.

If the `spanning-tree single cost` command setting is omitted, the following values are applied to the path cost according to the interface speed and the setting of the `spanning-tree single pathcost method` command.

- If `short` is set by the `spanning-tree single pathcost method` command:

  10 Mbit/s: 100

  100 Mbit/s: 19

  1 Gbit/s: 4

  10 Gbit/s: 2

- If `long` is set by the `spanning-tree single pathcost method` command:

  10 Mbit/s: 2000000

  100 Mbit/s: 200000

  1 Gbit/s: 20000

  10 Gbit/s: 2000

Syntax

To set or change information:

spanning-tree single pathcost method { long | short }

To delete information:

no spanning-tree single pathcost method

Input mode

`(config)`

Parameters

{ long | short }

If `long` is set, a 32-bit value is used. If `short` is set, a 16-bit value is used.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `long` or `short`

3. Note on using this parameter:

   - The default value of the path cost changes.

   - Changing the path cost value might change the topology.

   - When 65536 or a larger value is set for the path cost, you cannot change the parameter to `short`.

Default behavior

The setting of the `spanning-tree pathcost method` command is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree single port-priority

Sets the priority for applicable Single Spanning Tree ports.

Syntax

To set or change information:

spanning-tree single port-priority <*priority*>

To delete information:

no spanning-tree single port-priority

Input mode

`(config-if)`

Parameters

<*priority*>

Sets the port priority. Use a multiple of 16 as the port priority. The lower the value, the higher the priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 240

3. Note on using this parameter:

   Changing the port priority might change the topology.

Default behavior

The setting of the `spanning-tree port-priority` command is used. If the `spanning-tree port-priority` command has not been set, the port priority is set to 128.

`0` is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

None

spanning-tree single priority

Sets the bridge priority for Single Spanning Tree.

Syntax

To set or change information:

spanning-tree single priority <*priority*>

To delete information:

no spanning-tree single priority

Input mode

```
(config)
```

Parameters

<*priority*>

Sets the bridge priority. The lower the value, the higher the priority. Use a multiple of 4096 as the bridge priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 61440

3. Note on using this parameter:

   Changing the bridge priority might change the topology.

Default behavior

The bridge priority is set to 32768.

When both Spanning Tree Protocols and the Ring Protocol are used together, 0 is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree single transmission-limit

Sets the maximum number of BPDUs that can be sent during the hello-time interval for Single Spanning Tree.

Syntax

To set or change information:

spanning-tree single transmission-limit <*count*>

To delete information:

no spanning-tree single transmission-limit

Input mode

`(config)`

Parameters

<*count*>

Sets the maximum number of BPDUs that can be sent per hello-time interval.

This parameter is valid only when `rapid-stp` (802.1w) is set by the `spanning-tree single mode` command. If `stp` (802.1D) is set by the `spanning-tree single mode` command, the maximum number of BPDUs that can be sent per second is 3 (fixed) and the setting value of this command is ignored.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The maximum number of BPDUs that can be sent is set to 3.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

spanning-tree single mode

spanning-tree single hello-time

spanning-tree vlan

Configures PVST+. If the `no spanning-tree vlan` command is set after the `spanning-tree single` command has been set, the applicable VLAN operates with Single Spanning Tree.

Syntax

To set information:

no spanning-tree vlan <*vlan id list*>

To delete information:

spanning-tree vlan <*vlan id list*>

Input mode

`(config)`

Parameters

<*vlan id list*>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

3. Note on using this command:

   If the `spanning-tree single` command has been set, VLAN1 does not operate in PVST+ mode.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

vlan

spanning-tree vlan cost

Sets the path cost for the applicable PVST+ ports.

Syntax

To set or change information:

spanning-tree vlan <*vlan id list*> cost <*cost*>

To delete information:

no spanning-tree vlan <*vlan id list*> cost

Input mode

`(config-if)`

Parameters

<*vlan id list*>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

<*cost*>

Specifies the path cost value. The lower the <*cost*> value, the higher the possibility that the port will be used for forwarding the applicable frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   When `short` is set by the `spanning-tree pathcost method` or the `spanning-tree vlan pathcost method` command:

   1 to 65535

   When `long` is set by the `spanning-tree pathcost method` or the `spanning-tree vlan pathcost method` command:

   1 to 200000000

3. Note on using this parameter:

   Changing the port priority might change the topology.

Default behavior

The method of applying the path cost is determined by the setting of the `spanning-tree vlan pathcost method` command.

`1` is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. <*vlan id list*> cannot be specified if the `interface range` command is used to set information.
2. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree cost

spanning-tree pathcost method

spanning-tree vlan pathcost method

spanning-tree vlan forward-time

Sets the time required for PVST+ state transition.

Syntax

To set or change information:

spanning-tree vlan <*vlan id list*> forward-time <*seconds*>

To delete information:

no spanning-tree vlan <*vlan id list*> forward-time

Input mode

`(config)`

Parameters

<*vlan id list*>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

<*seconds*>

Specifies the time in seconds required for the state of a port to change.

If `pvst` (802.1D) is set by the `spanning-tree mode` command or the `spanning-tree vlan mode` command, the listening state and the learning state are maintained for the set period of time.

If `rapid-pvst` (802.1w) is set by the `spanning-tree mode` command or the `spanning-tree vlan mode` command, the discarding state and the learning state are maintained for the set period of time (note that this applies only when the timer causes the transition).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   4 to 30

Default behavior

The time required for the state of a port to change is set to 15 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree vlan hello-time

Sets the interval for sending PVST+ BPDUs.

Syntax

To set or change information:

spanning-tree vlan <*vlan id list*> hello-time <*hello time*>

To delete information:

no spanning-tree vlan <*vlan id list*> hello-time

Input mode

`(config)`

Parameters

<*vlan id list*>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

<*hello time*>

Specifies the interval in seconds for sending BPDUs that are sent regularly from the Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

3. Note on using this parameter:

   If you set 1 then this might result in a changeable topology.

Default behavior

The interval for sending BPDUs is set to 2.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree vlan max-age

Sets the maximum valid time of BPDUs that are sent via PVST+.

Syntax

To set or change information:

spanning-tree vlan <*vlan id list*> max-age <*seconds*>

To delete information:

no spanning-tree vlan <*vlan id list*> max-age

Input mode

```
(config)
```

Parameters

<*vlan id list*>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

<*seconds*>

Sets the maximum valid time in seconds for BPDUs that are sent from the Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   6 to 40

3. Note on using this parameter:

   If you set a value less than 20, then this might result in a changeable topology.

Default behavior

The maximum valid time of BPDUs that can be sent from a Switch is set to 20 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree vlan mode

Sets the PVST+ operating mode.

Syntax

To set or change information:

spanning-tree vlan <*vlan id list*> mode { pvst | rapid-pvst }

To delete information:

no spanning-tree vlan <*vlan id list*> mode

Input mode

`(config)`

Parameters

<*vlan id list*>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

{ pvst | rapid-pvst }

Sets the protocol to be used. If the protocol is changed during Spanning Tree operation, the Spanning Tree Protocol is re-initialized. If `pvst` is set, PVST+ mode is used. If `rapid-pvst` is set, rapid PVST+ mode is used.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `pvst` or `rapid-pvst`

Default behavior

The PVST+ operating mode is set by the `spanning-tree mode` command.

Impact on communication

If `pvst` or `rapid-pvst` has been specified by the `spanning-tree mode` command, communications are interrupted until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

spanning-tree mode

spanning-tree vlan pathcost method

Sets whether to use a 16-bit value or a 32-bit value as the path cost for a PVST+ port.

If the `spanning-tree vlan cost` command setting is omitted, the following values are applied to the path cost according to the interface speed and the `spanning-tree vlan pathcost method` command settings:

- When `short` is set by the `spanning-tree vlan pathcost method` command:

  10 Mbit/s: 100

  100 Mbit/s: 19

  1 Gbit/s: 4

  10 Gbit/s: 2

- When `long` is set by the `spanning-tree vlan pathcost method` command:

  10 Mbit/s: 2000000

  100 Mbit/s: 200000

  1 Gbit/s: 20000

  10 Gbit/s: 2000

Syntax

To set or change information:

spanning-tree vlan <*vlan id list*> pathcost method { long | short }

To delete information:

no spanning-tree vlan <*vlan id list*> pathcost method

Input mode

`(config)`

Parameters

<*vlan id list*>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

{ long | short }

If `long` is set, a 32-bit value is used. If `short` is set, a 16-bit value is used.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `long` or `short`

3. Note on using this parameter:

- The default value of the path cost changes.

- Changing the path cost value might change the topology.

- When 65536 or a larger value is set for the path cost, you cannot change the parameter to `short`.

Default behavior

The setting of the `spanning-tree pathcost method` command is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

spanning-tree pathcost method

spanning-tree cost

spanning-tree vlan cost

spanning-tree vlan port-priority

Sets the priority for the applicable PVST+ ports.

Syntax

To set or change information:

spanning-tree vlan <*vlan id list*> port-priority <*priority*>

To delete information:

no spanning-tree vlan <*vlan id list*> port-priority

Input mode

`(config-if)`

Parameters

<*vlan id list*>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

<*priority*>

Sets the port priority. Use a multiple of 16 as the port priority. The lower the value, the higher the priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 240

3. Note on using this parameter:

   Changing the port priority might change the topology.

Default behavior

The setting of the `spanning-tree port-priority` command is used. If the `spanning-tree port-priority` command has not been set, the port priority is set to 128.

`0` is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. <*vlan id list*> cannot be specified if the `interface range` command is used to set information.

2. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree port-priority

spanning-tree vlan priority

Sets the PVST+ bridge priority.

Syntax

To set or change information:

spanning-tree vlan <*vlan id list*> priority <*priority*>

To delete information:

no spanning-tree vlan <*vlan id list*> priority

Input mode

```
(config)
```

Parameters

<*vlan id list*>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

<*priority*>

Sets the bridge priority. The lower the value, the higher the priority.

Use a multiple of 4096 as the bridge priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 61440

3. Note on using this parameter:

   Changing the bridge priority might change the topology.

Default behavior

The bridge priority is set to 32768.

When both Spanning Tree Protocols and the Ring Protocol are used together, 0 is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree vlan transmission-limit

Sets the maximum number of BPDUs that can be sent within the PVST+ hello-time interval.

Syntax

To set or change information:

spanning-tree vlan <*vlan id list*> transmission-limit <*count*>

To delete information:

no spanning-tree vlan <*vlan id list*> transmission-limit

Input mode

`(config)`

Parameters

<*vlan id list*>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

<*count*>

Sets the maximum number of BPDUs that can be sent per hello-time interval.

This parameter is effective only when `rapid-pvst` (802.1w) is set by the `spanning-tree mode` command or the `spanning-tree vlan mode` command. When `pvst` (802.1D) is set by the `spanning-tree mode` command or the `spanning-tree vlan mode` command, the maximum number of BPDUs that can be sent per second is 3 (fixed) and the value set by this command is ignored.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The maximum number of BPDUs that can be sent is set to 3.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

spanning-tree mode

spanning-tree vlan mode

Chapter

17. Ring Protocol

axrp

Sets the ring ID. In addition, to collect information necessary for the Ring Protocol functionality, switches to `config-axrp` mode. A maximum of 16 ring IDs can be set for a Switch.

If this setting is removed, the ring information that is already set for ring IDs is deleted.

Syntax

To set information:

axrp <*ring id*>

To delete information:

no axrp <*ring id*>

Input mode

`(config)`

Parameters

<*ring id*>

Sets the ring ID.

The same ring ID must be specified for all switches belonging to the same ring. Specify a unique ring ID for each different ring in a network.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When changing the ring configuration by setting or deleting this command, if the number of entries in the MAC address table reaches the maximum and all necessary entries cannot be registered, the Ring Protocol functionality cannot operate properly. For the capacity limit of the MAC address table, see the description of the applicable MAC address table in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the configuration entries of the functionalities that use the MAC address table.

Related commands

None

axrp virtual-link

Sets a virtual link ID used to identify the root bridge shared by a Spanning Tree Protocol and GSRP. Only one virtual link ID can be set for a Switch.

Syntax

To set or change information:

axrp virtual-link <*link id*> vlan <*vlan id*>

To delete information:

no axrp virtual-link <*link id*>

Input mode

`(config)`

Parameters

<*link id*>

Sets a virtual link ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 250

<*vlan id*>

Specifies a VLAN to be used for a virtual link.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. VLANs that are used as control VLANs cannot be specified.
2. A node in a Spanning Tree Protocol can consist of a maximum of two switches (including this Switch) that belong to the same Spanning Tree topology. Specify the same virtual link IDs for the two switches.
3. When the Ring Protocol is used with GSRP, set the same virtual link ID for the Switch that is used for GSRP.

Related commands

vlan

axrp vlan-mapping

Sets the VLAN mapping to be applied to a VLAN group and also the VLANs that participate in VLAN mapping.

Syntax

To set or change information:

axrp vlan-mapping <*mapping id*> vlan <*vlan id list*>

To change information:

axrp vlan-mapping <*mapping id*> {vlan <*vlan id list*> | vlan add <*vlan id list*> | vlan remove <*vlan id list*>}

To delete information:

no axrp vlan-mapping <*mapping id*>

Input mode

`(config)`

Parameters

<*mapping id*>

Specifies the VLAN mapping ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 128

vlan <*vlan id list*>

Sets the VLANs that participate in VLAN mapping. When specifying multiple VLANs, you can specify a range.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

vlan add <*vlan id list*>

Specifies the VLANs to be added to the VLAN list you have configured.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

vlan remove <*vlan id list*>

Specifies the VLANs to be removed from the VLAN list you have configured.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You cannot specify multiple VLAN mappings for one VLAN.
2. You cannot specify a VLAN mapping for a VLAN that is used as the control VLAN.
3. When the Ring Protocol is used with PVST+, only one VLAN ID can be specified for a VLAN mapping. If you want to control multiple VLANs by using the Ring Protocol, set the remaining VLAN IDs for other VLAN mapping IDs, and then assign them to a VLAN group of the applicable ring.
4. When the Ring Protocol is used with GSRP, within the following range of IDs you cannot use the same ID value concurrently as both a VLAN mapping ID and a VLAN group ID for GSRP:

   Range of IDs that cannot be used concurrently: 108 to 128
5. When the Ring Protocol is used with Multiple Spanning Tree, the VLAN IDs specified by this command and the VLANs that belong to the MST instance must match. Unmatched VLANs are put in the Blocking status.
6. When the Ring Protocol is used with the VRF functionality (when the `axrp-enable` or `axrp-enable-ipv4-ipv6` parameter of the `vrf mode` command is set), the range of VLAN mapping IDs for which VLANs can be set is from 1 to 64.

   Set VLAN mapping ID 1 for the VLAN used as the IP interface of the global network.

   In addition, use VLAN mapping IDs from 2 to 64 for the VLANs used as the IP interface to VRF so that the VRF ID coincides with the VLAN mapping ID. Communication will not be possible in any VLAN that does not satisfy these conditions. [OP-NPAR]
7. When changing the ring configuration by setting or deleting this command, if the number of entries in the MAC address table reaches the maximum and all necessary entries cannot be registered, the Ring Protocol functionality cannot operate properly. For the capacity limit of the MAC address table, see the description of the applicable MAC address table in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the configuration entries of the functionalities that use the MAC address table.

Related commands

vlan

axrp-primary-port

Sets the primary port on the master node.

If this command is set, the primary port is not assigned automatically on the master node, and the interface set by using this command operates as the primary port. The interfaces that can be specified are Ethernet interfaces and port channel interfaces.

Syntax

To set information:

axrp-primary-port <*ring id*> vlan-group <*group id*>

To delete information:

no axrp-primary-port <*ring id*> vlan-group <*group id*>

Input mode

```
(config-if)
```

Parameters

<*ring id*>

Sets the ring ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

vlan-group <*group id*>

Specifies a VLAN group ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 2

Default behavior

The primary port is assigned automatically.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For an interface for which no ring port is set, if you enter this command, no operation is performed.
2. While the Ring Protocol is operating, if you change or delete the primary port, this functionality is temporarily disabled. As a result, a loop might occur depending on the network configuration (ring configuration) to which the functionality is applied. To avoid a loop, before entering this command, place the interface that is the ring port in the shutdown

state.

3. When a Switch is on the following nodes, entering this command has no effect:
    - Transit node
    - Master node, which is a edge node for a shared link non-monitoring ring
4. You cannot specify an Ethernet interface that is part of a channel group as the primary port. Conversely, an Ethernet interface that is set as the primary port cannot be assigned to a channel group. Set the primary port to the port channel interface to which the applicable Ethernet interface belongs.
5. The ring ID must be associated with the same VLAN group as the primary port.
6. When changing the ring configuration by setting or deleting this command, if the number of entries in the MAC address table reaches the maximum and all necessary entries cannot be registered, the Ring Protocol functionality cannot operate properly. For the capacity limit of the MAC address table, see the description of the applicable MAC address table in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the configuration entries of the functionalities that use the MAC address table.

Related commands

mode

axrp-ring-port

axrp-ring-port

Sets an interface that operates as the ring port for the Ring Protocol. The interfaces that can be set are Ethernet interfaces and port channel interfaces.

Syntax

To set or change information:

axrp-ring-port <*ring id*> [{shared-edge | shared}]

To delete information:

no axrp-ring-port <*ring id*>

Input mode

`(config-if)`

Parameters

<*ring id*>

Sets the ring ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

{shared-edge | shared}

Specifies a ring port that configures a shared link.

shared-edge

When a Switch operates as the edge node in a shared-link non-monitoring ring, this parameter sets the ring port that will be a shared link.

Only one port can be specified for the ring ID.

shared

When a Switch operates as a transit node on a shared link, this parameter specifies the ring port that will be the shared link.

Two ports must be specified to correspond with the ring ID.

1. Default value when this parameter is omitted:

   The interface operates as a standard ring port.

2. Range of values:

   `shared-edge` or `shared`

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Two ring ports can be specified as corresponding to one ring ID.
2. In a multi-ring configuration with shared links, when a Switch is already operating as a master node in the neighboring ring, if a ring port with a shared-edge specified is set or deleted on a port which is used as the primary port, this functionality is disabled temporarily. As a result, a loop might occur depending on the network configuration (ring configuration) to which the functionality is applied. To avoid a loop, before entering this command, place the interface that is the ring port in the shutdown state.
3. An Ethernet interface that is part of a channel group cannot be specified as a ring port. Conversely, an Ethernet interface that is specified as a ring port cannot be part of a channel group. Set the ring port as the port channel interface to which the applicable Ethernet interface belongs.
4. If a Switch is specified as a master node, a primary port is assigned automatically to each VLAN group of registered ring ports. Note, however, that the interface specified by using the `axrp-primary-port` command takes precedence and operates as the primary port.
5. If a shared port is not specified as a shared node, the Ring Protocol functionality will not operate properly.
6. When the ring configuration is changed by setting, changing, or deleting this command, if the number of entries in the MAC address table reaches the maximum and all necessary entries cannot be registered, the Ring Protocol functionality will not operate properly. For the capacity limit of the MAC address table, see the description of the applicable MAC address table in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the configuration entries of the functionalities that use the MAC address table.

Related commands

mode

axrp-primary-port

control-vlan

Sets the VLAN to be used as a control VLAN. You can use the VLAN specified by using this command to send and receive control frames that monitor the ring status.

Setting the `forwarding-delay-time` parameter for a transit node allows you to set the time required to transfer the status of the control VLAN to `Forwarding` during initial operation. You can therefore adjust the time required before starting to monitor the status of received flush control frames on the transit node, to ensure that flush control frames sent by the master node are received.

Syntax

To set or change information:

control-vlan <*vlan id*> [forwarding-delay-time <*seconds*>]

To delete information:

no control-vlan

Input mode

`(config-axrp)`

Parameters

<*vlan id*>

Specifies the VLAN to be used as the control VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

   Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

forwarding-delay-time <*seconds*>

Sets the time (in seconds) required before the status of the control VLAN changes to `Forwarding` when the transit node Switch is started or when the Ring Protocol program is restarted.

1. Default value when this parameter is omitted:

   The control VLAN transitions to `Forwarding` immediately after the ring port comes up.

2. Range of values:

   1 to 65535

3. Note on using this parameter:

   To delete only this parameter, set `control-vlan` again with this parameter omitted. This operation is used to delete parameters.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You cannot specify a VLAN that is used as a control VLAN by another ring ID.
2. You cannot specify a VLAN that is used in a VLAN group.
3. While the Ring Protocol is operating, if you change or delete the control VLAN, this functionality is temporarily disabled. As a result, a loop might occur depending on the network configuration (ring configuration) to which the functionality is applied. To avoid a loop, before entering this command, place the interface that is the ring port in the shutdown state.
4. The VLAN specified as a control VLAN cannot be used with Spanning Tree Protocols.
5. A VLAN used as a virtual link cannot be specified as a control VLAN.
6. `forwarding-delay-time` is enabled only when the operating mode is transit node.
7. `forwarding-delay-time` operates when the following occurs:
    - The Switch is started (includes execution of the `reload` or `ppupdate` operation command).
    - A configuration file is copied to the running configuration (by executing the `copy` operation command)
    - A Ring Protocol program is restarted (including execution of the `restart axrp` operation command).
    - A VLAN program is restarted (including execution of the `restart vlan` operation command).
    - The switch is recovered from all BSU failures.
    - The system for BCU, CSU, or MSU is switched.
8. When the ring configuration is changed by setting, changing, or deleting this command, if the number of entries in the MAC address table reaches the maximum and all necessary entries cannot be registered, the Ring Protocol functionality will not operate properly. For the capacity limit of the MAC address table, see the description of the applicable MAC address table in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the configuration entries of the functionalities that use the MAC address table.

Related commands

vlan

disable

Disables the Ring Protocol functionality.

Syntax

To set information:

disable

To delete information:

no disable

Input mode

```
(config-axrp)
```

Parameters

None

Default behavior

The Ring Protocol functionality is enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If this command is entered while the Ring Protocol is operating, the Ring Protocol functionality is disabled. In this case, a loop might occur depending on a network configuration (ring configuration) to which the Ring Protocol functionality is applied. To avoid a loop, before entering this command, place the interface that is the ring port in the shutdown state.
2. When changing the ring configuration by setting or deleting this command, if the number of entries in the MAC address table reaches the maximum and all necessary entries cannot be registered, the Ring Protocol functionality cannot operate properly. For the capacity limit of the MAC address table, see the description of the applicable MAC address table in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the configuration entries of the functionalities that use the MAC address table.

Related commands

None

flush-request-count

Specifies the number of times the master node sends flush control frames, which clear the MAC address table, to the transit node in the ring if a ring failure occurs or when recovering from a failure.

Syntax

To set or change information:

flush-request-count <*count*>

To delete information:

no flush-request-count

Input mode

```
(config-axrp)
```

Parameters

<*count*>

Specifies the number of times that flush control frames are sent.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The number of times that flush control frames are sent is 3.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The first-received flush control frame causes entries in the MAC address table on the transit node to be cleared. If a flush control frame is received while MAC address table entries are being cleared, the clearing of entries is aborted.

Related commands

None

flush-request-transmit vlan

Sets sending of neighboring-ring flush control frames to the devices in the neighboring ring configuration to clear the MAC address table when a ring failure occurs or the failure is corrected.

For details about how to specify these settings, see *23.1.10 Configuring flush control frames for neighboring rings* in the manual *Configuration Guide Vol. 1 For Version 11.7*.

Syntax

To set or change information:

flush-request-transmit vlan <*vlan id*>

To delete information:

no flush-request-transmit vlan

Input mode

```
(config-axrp)
```

Parameters

<*vlan id*>

Specify the ID of the VLAN to which neighboring-ring flush control frames are to be sent.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

If this command is not specified, neighboring-ring flush control frames are not sent to the devices in the neighboring ring configuration.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Set this command on the master node. The command's functionality is not enabled when the command is set on a transit node.
2. Make sure that the VLAN ID you specify is a VLAN ID specified in VLAN mapping.

   Also, make sure this VLAN ID is used for only sending neighboring-ring flush control frames and is not used for forwarding data.

Related commands

vlan

forwarding-shift-time

For a transit node, sets the reception hold time for flush control frames. If no flush control frames are received within the reception hold time, the status of the ring port shifts from `Blocking` to `Forwarding`.

For a master node, sets the hold time until the status shifts to `Forwarding` if port up is detected on the secondary port.

Syntax

To set or change information:

forwarding-shift-time {<*seconds*> | infinity}

To delete information:

no forwarding-shift-time

Input mode

`(config-axrp)`

Parameters

{<*seconds*> | infinity}

For a transit node, specifies the reception hold time for flush control frames in seconds. If you specify `infinity`, there is no limit on the hold time, and the status of the ring port on the transit node does not switch to `Forwarding` until a flush control frame is received.

For a master node, specifies the hold time in seconds until the status of the secondary port changes to `Forwarding`. If you specify `infinity`, there is no limit to the hold time, and the status does not switch to `Forwarding` even if port up is detected on the secondary port.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535, or `infinity`

Default behavior

For a transit node, 10 seconds is used as the reception hold time for flush control frames.

For a master node, the hold time for the secondary port is `infinity`.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the sending interval for health check frames on the master node is longer than the reception hold time for flush control frames on the transit node, the status of the ring port on the transit node switches to `Forwarding` before the master node detects normal status. This could produce a temporary loop.

   Set the hold time value based on the interval at which health check frames are sent from the master node.

2. If the sending interval for health check frames on the master node is longer than the hold time

until the status shifts to `Forwarding` on the master node, the status of the secondary port switches to `Forwarding` before the master node detects normal status. This could produce a temporary loop.

Set the hold time value based on the interval at which health check frames are sent from the master node.

Related commands

None

health-check holdtime

If the master node does not receive a periodic health-check frame sent by the master node itself or by link non-monitoring ring shared edge nodes, this specifies how long to wait before determining that a failure has occurred.

Syntax

To set or change information:

health-check holdtime <*milli seconds*>

To delete information:

no health-check holdtime

Input mode

```
(config-axrp)
```

Parameters

<*milli seconds*>

Specifies the hold time in milliseconds until a health-check frame is received.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   32 to 12288

   Note, however, that values entered for the above command are aggregated to a value determined according to the following table when the value is actually applied.

Table 17-1: List of hold time setting values

#	Hold time entered by a command	Actual hold time
1	32	32
2	33 to 48	48
3	49 to 64	64
4	65 to 96	96
5	97 to 128	128
6	129 to 192	192
7	193 to 256	256
8	257 to 384	384
9	385 to 512	512
10	513 to 768	768
11	769 to 1024	1024
12	1025 to 1536	1536
13	1537 to 2048	2048
14	2049 to 3072	3072

#	Hold time entered by a command	Actual hold time
15	3073 to 4096	4096
16	4097 to 6144	6144
17	6145 to 8192	8192
18	8193 to 12288	12288

Default behavior

The reception hold time for health check frames is set to 256 milliseconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For this command, set a value greater than the setting value of the `health-check interval` command. If you use this command to set a value equal to or smaller than the setting value of `health-check interval` command, a health-check timeout is detected.
2. When the hold time elapses, the master node determines that a failure has occurred, performs error processing, and then switches to monitoring for recovery status.

Related commands

None

health-check interval

Sets the interval for sending health-check frames from a master node or from shared edge nodes in a shared link non-monitoring ring.

Syntax

To set or change information:

health-check interval <*milli seconds*>

To delete information:

no health-check interval

Input mode

`(config-axrp)`

Parameters

<*milli seconds*>

Specifies the interval for sending health-check frames in milliseconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   10 to 10000

Default behavior

The interval for sending health-check frames is 100 milliseconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Set a value greater than the setting value of this command for the `health-check holdtime` command. If you set a value equal to or smaller than the setting value of this command for the `health-check holdtime` command, a health-check timeout is detected.
2. Set the same interval for sending health-check frames for the master nodes in the same ring and for the shared edge nodes in a shared link non-monitoring ring. If these values are different, fault detection will not work properly.

Related commands

None

mode

Sets the operating mode of the Switch used for the ring.

In addition, if the ring configuration is a multi-ring configuration with shared links, sets the attributes of a ring configured by Switches, and the positioning of the Switches in the ring.

Syntax

To set or change information:

mode {master | transit} [ring-attribute {rift-ring | rift-ring-edge <*edge node id*>}]

To delete information:

no mode

Input mode

`(config-axrp)`

Parameters

{master | transit}

Specifies the operating mode.

master

Operates as a master node.

transit

Operates as a transit node.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `master` or `transit`

ring-attribute {rift-ring | rift-ring-edge <*edge node id*>}

Specifies a shared-link non-monitoring ring (a ring that does not monitor shared links) as the attributes of the ring in a multi-ring configuration with shared links, and specifies the positioning of a Switch in the ring.

If you specify `rift-ring-edge`, you must specify the `shared-edge` parameter for the `axrp-ring-port` command.

rift-ring

Operates as a node that is part of a shared link non-monitoring ring (but not an edge nodes). This parameter can be specified for the master node only.

rift-ring-edge <*edge node id*>

Operates as a node (shared node) which is the edge node in a shared link non-monitoring ring. To differentiate between two edge nodes, specify an edge node ID (1 or 2) for each Switch.

1. Default value when this parameter is omitted:

   For master nodes, the Switch operates as the master node for a shared link monitoring ring (ring that monitors shared links).

   For transit nodes, the Switch operates as a shared link monitoring ring or a transit node of a shared link non-monitoring ring.

2. Range of values:

   `rift-ring`, `rift-ring-edge1`, or `rift-ring-edge 2`

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Set only one master node Switch in a ring. If you specify multiple master node Switches, the Ring Protocol functionality will not operate properly.
2. If you change or delete the mode while Ring Protocol is operating, the functionality is temporarily disabled. As a result, a loop might occur depending on the network configuration (ring configuration) to which the functionality is applied. To avoid a loop, before entering this command, place the interface that is the ring port in the shutdown state.
3. If you set a master node (`master rift-ring`) of a shared link non-monitoring ring in a Switch, the maximum number (16) of ring IDs might not be set. For details, see *22.5.4(2) Maximum number of multi-rings* in the manual *Configuration Guide Vol. 1 For Version 11.7*.
4. If you specify `rift-ring-edge` for the `ring-attribute` parameter, you must specify the `shared-edge` parameter for the `axrp-ring-port` command.
5. Specify different edge node IDs for each edge node in shared link non-monitoring rings within the same ring. If the setting is not correct, the ring functionality will not operate properly.
6. When the ring configuration is changed by setting, changing, or deleting this command, if the number of entries in the MAC address table reaches the maximum and all necessary entries cannot be registered, the Ring Protocol functionality will not operate properly. For the capacity limit of the MAC address table, see the description of the applicable MAC address table in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the configuration entries of the functionalities that use the MAC address table.

Related commands

None

name

Sets the name for identifying a ring.

Syntax

To set or change information:

name <*name*>

To delete information:

no name

Input mode

```
(config-axrp)
```

Parameters

<*name*>

Sets the name for identifying a ring.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

`NULL` is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

preempt-delay

Sets the delay time between detection of fault recovery by the master node and path switchback operation.

When this command is set, if the master node detects fault recovery, recovery operations are not performed until the path switchback suppression time elapses.

Syntax

To set or change information:

preempt-delay { <*seconds*> | infinity }

To delete information:

no preempt-delay

Input mode

`(config-axrp)`

Parameters

{ <*seconds*> | infinity }

<*seconds*>

Specifies the path switchback suppression time in seconds.

infinity

The suppression time becomes unlimited and the master node does not start restoration operations until the `clear axrp preempt-delay` command is executed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3600, or `infinity`

Default behavior

The path switchback operation is not suppressed.

Impact on communication

None

When the change is applied

If the ring status is normal, the value is applied to operation immediately after this command is set or changed. If an error occurs in a ring, the value is applied to operation from the next time.

If this command is deleted, the value is applied to operation immediately.

Notes

1. To set this functionality, set `infinity` for `forwarding-shift-time` of all transit nodes that configure a ring, or set a value greater than the suppression time for path switchback operation. If you specify a value smaller than the suppression time for path switchback operation, a loop might occur.

Related commands

None

vlan-group

Sets the VLAN group that will be used for the Ring Protocol and the mapping IDs of the VLANs participating in the VLAN groups.

A maximum of two VLAN groups can be set for a ring. In addition, by creating two VLAN groups, loads can be balanced (shared) between the two VLANs.

Syntax

To set or change information:

vlan-group <*group id*> vlan-mapping <*mapping id list*>

To delete information:

no vlan-group <*group id*>

Input mode

```
(config-axrp)
```

Parameters

<*group id*>

Specifies the VLAN group ID that will be used for the Ring Protocol.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 2

vlan-mapping <*mapping id list*>

Specifies the mapping IDs of the VLANs participating in a VLAN group. One VLAN mapping ID can be set. Use hyphens (`-`) or commas (`,`) to specify multiple VLAN mapping IDs at the same time.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 128

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the same VLAN mapping is assigned to VLAN groups in different rings, these rings cannot share the same port as a ring port. Note, however, that it is possible to share the same ring port if it is a shared link ring port (a ring port for which `shared` or `shared-edge` is specified).
2. If a Switch is specified as a master node, a primary port is assigned automatically to each

VLAN group of registered ring ports. If the `axrp-primary-port` command is already entered, the specified interface has precedence and set as the primary port.

3. When the ring configuration is changed by setting, changing, or deleting this command, if the number of entries in the MAC address table reaches the maximum and all necessary entries cannot be registered, the Ring Protocol functionality will not operate properly. For the capacity limit of the MAC address table, see the description of the applicable MAC address table in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the configuration entries of the functionalities that use the MAC address table.

Related commands

axrp vlan-mapping

Chapter

18. Policy-based Switching

default (policy-switch-list)

Specifies the default policy-based switching behavior. The default behavior here refers to how policy-based switching treats packets if all routes are unable to forward them.

You can specify only one default behavior setting per policy-based switching list information item.

Syntax

To set or change information:

default {permit | deny}

To delete information:

no default

Input mode

`(config-pol-sw)`

Parameters

{permit | deny}

Sets the default policy-based switching behavior.

permit

Packets are forwarded by the normal destination interface.

deny

The command discards packets.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify `permit` or `deny`.

Default behavior

The command discards packets.

Impact on communication

If you change the settings of the default policy-based switching behavior for policy-based switching list information that has already been set as an access list, the affected packets might temporarily be discarded.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

policy-switch-list

policy-channel-group

Sets the channel group number of the destination interface information for policy-based switching.

The destination interface information items are selected in ascending order of the application sequence values set in the policy-based switching list information.

A maximum of eight destination interface information items, which include the channel group number and NIF number/port number, can be set for each policy-based switching list information item.

Syntax

To set or change information:

[<*sequence*>] policy-channel-group <*channel group number*>

To delete information:

no <*sequence*>

Input mode

```
(config-pol-sw)
```

Parameters

<*sequence*>

Specifies the sequence in which the destination interface information for policy-based switching is applied.

1. Default value when this parameter is omitted:

   If no destination interface information is set for policy-based switching, the initial value is ten.

   If the destination interface information has been set, the initial value is the maximum value for the application sequence that has been set plus ten.

   Note, however, that if the maximum value for the application sequence is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<*channel group number*>

Specifies the channel group number for link aggregation of the destination interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about the channel group number, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

If you change the destination interface information for policy-based switching list information that has already been set as an access list, the affected packets might temporarily be discarded.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For the channel group number parameter, specify the channel group number that belongs to the VLAN ID set by using the `policy-vlan` command.
2. Before specifying the channel group number parameter, set link aggregation.
3. When changing the applicable channel group number, delete the channel group number parameter setting for this command first

Related commands

interface vlan

channel-group mode

permit(advance access-list)

permit (mac access-list extended)

permit (ip access-list extended)

permit (ipv6 access-list)

policy-switch-list

policy-vlan

policy-interface (policy-switch-list)

policy-switch-list resequence

policy-interface (policy-switch-list)

Sets the NIF number/port number of the destination interface information for policy-based switching.

The destination interface information items are selected in ascending order of the application sequence values set in the policy-based switching list information.

A maximum of eight destination interface information items, which include the NIF number/port number and channel group number, can be set for each policy-based switching list information item.

Syntax

To set or change information:

[<*sequence*>] policy-interface {gigabitethernet | tengigabitethernet} <*nif no.*>/<*port no.*>

To delete information:

no <*sequence*>

Input mode

```
(config-pol-sw)
```

Parameters

<*sequence*>

Specifies the sequence in which the destination interface information for policy-based switching is applied.

1. Default value when this parameter is omitted:

   If no destination interface information is set for policy-based switching, the initial value is ten.

   If the destination interface information has been set, the initial value is the maximum value for the application sequence that has been set plus ten.

   Note, however, that if the maximum value for the application sequence is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

{gigabitethernet | tengigabitethernet} <*nif no.*>/<*port no.*>

Specifies the NIF number and port number of the destination interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about NIF number and port number, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

If you change the destination interface information for policy-based switching list information that has already been set as an access list, the affected packets might temporarily be discarded.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Specify a NIF number and port number that belong to the VLAN ID set by using the `policy-vlan` command for the NIF number/port number of the destination interface.

Related commands

interface vlan

permit(advance access-list)

permit (mac access-list extended)

permit (ip access-list extended)

permit (ipv6 access-list)

policy-switch-list

policy-vlan

policy-channel-group

policy-switch-list resequence

policy-switch-list

Specifies settings related to policy-based switching.

Entering this command switches to `config-pol-sw` mode, in which the policy-based switching list information for the list number can be set.

A maximum of 1000 policy-based switching list information items can be set per switch.

Syntax

To set or change information:

policy-switch-list <*policy switch list no.*>

To delete information:

no policy-switch-list <*policy switch list no.*>

Input mode

`(config)`

Parameters

<*policy switch list no.*>

Specifies the list number for the policy-based switching list information.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 1 to 1000 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The policy-based switching list information that is used as an access list cannot be deleted.
2. Before specifying this command, set the route allocation pattern to `extended`.

Related commands

permit(advance access-list)

permit (mac access-list extended)

permit (ip access-list extended)

permit (ipv6 access-list)

policy-interface (policy-switch-list)

default (policy-switch-list)

recover (policy-switch-list)

policy-switch-list resequence

policy-switch-list default-aging-interval

Sets the interval over which the monitoring of the forward ability of policy-based switching is temporarily stopped during a system switchover in the BCU, CSU, or MSU. During this interval, the status before a system switchover is applied to the output destination route of policy-based switching.

Syntax

To set or change information:

policy-switch-list default-aging-interval <*seconds*>

To delete information:

no policy-switch-list default-aging-interval

Input mode

```
(config)
```

Parameters

<*seconds*>

Specifies, in seconds, the interval over which the monitoring of the forward ability is stopped.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3600

Default behavior

The interval over which the monitoring of the forward ability is stopped is 200 seconds.

Impact on communication

None

When the change is applied

The change is applied when the command is set.

Notes

1. While the monitoring of the forward ability is stopped, if you use this command to change the interval, monitoring restarts when the new period minus the elapsed time has passed.

Related commands

policy-switch-list

policy-switch-list default-init-interval

Sets the interval over which the monitoring of the forward ability of policy-based switching is temporarily stopped while, for example, the switch is starting. During this interval, frames that are subject to policy-based switching are discarded.

Syntax

To set or change information:

policy-switch-list default-init-interval <*seconds*>

To delete information:

no policy-switch-list default-init-interval

Input mode

`(config)`

Parameters

<*seconds*>

Specifies, in seconds, the interval over which the monitoring of the forward ability is stopped.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3600

Default behavior

The interval over which the monitoring of the forward ability is stopped is 200 seconds.

Impact on communication

None

When the change is applied

The change is applied when the command is set.

Notes

1. While the monitoring of whether data is being transferred is stopped, if you use this command to change the interval, monitoring restarts when the new period minus the elapsed time has passed.

Related commands

policy-swich-list

policy-switch-list resequence

Resets the sequence in which destination interfaces for policy-based switching are applied.

Syntax

To set or change information:

policy-switch-list resequence <*policy switch list no.*> [<*starting sequence*> [<*increment sequence*>]]

Input mode

`(config)`

Parameters

<*policy switch list no.*>

Specifies the list number for the policy-based switching list information.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 1 to 1000 in decimal.

<*starting sequence*>

Specifies the starting number of the sequence value.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294966494 in decimal.

<*increment sequence*>

Specifies the sequence-value increment.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   1 to 100 in decimal

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

policy-switch-list

policy-interface (policy-switch-list)

policy-channel-group

policy-vlan

Sets the VLAN ID of the destination interface for policy-based switching.

You can specify only one VLAN ID for the destination interface per policy-based switching list information item.

Syntax

To set or change information:

policy-vlan <*vlan id*>

To delete information:

no policy-vlan

Input mode

```
(config-pol-sw)
```

Parameters

<*vlan id*>

Specifies the VLAN ID of the destination interface for a packet.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specifies the VLAN ID of the destination interface.

   For details about the VLAN ID, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Before using this command, set a VLAN interface.
2. Before you change or delete this command, delete both the `policy-interface` (`policy-switch-list`) and `policy-channel-group` command.
3. When specifying the default VLAN (VLAN ID = 1) for the VLAN ID of the destination interface, explicitly set `vlan 1` for the VLAN interface.

Related commands

interface vlan

permit (advance access-list)

permit (mac access-list extended)

permit (ip access-list extended)

permit (ipv6 access-list)

policy-switch-list
policy-interface (policy-switch-list)
policy-channel-group

recover (policy-switch-list)

Specifies the switchback behavior of policy-based switching destination interfaces.

You can specify only one switchback behavior setting per policy-based switching list information item.

Syntax

To set or change information:

recover {on | off}

To delete information:

no recover

Input mode

`(config-pol-sw)`

Parameters

{on | off}

Specifies the switchback behavior of policy-based switching destination interfaces.

on

Executes switchbacks.

off

Does not execute switchbacks.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Either `on` or `off` can be specified.

Default behavior

Executes switchbacks.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you change the routes in policy-based switching list information after setting the `off` parameter for the list, you need to confirm that the parameter has already been applied to the list before changing the routes. You can confirm this by using the `show cache policy-switch` operation command.

Related commands

policy-switch-list

Chapter

19. IGMP Snooping

ip igmp snooping (global)

Suppresses the IGMP snooping functionality on a Switch.

Syntax

To set information:

```
no ip igmp snooping
```

To delete information:

```
ip igmp snooping
```

Input mode

`(config)`

Parameters

None

Default behavior

The IGMP snooping functionality is enabled on a Switch.

Impact on communication

The IGMP snooping functionality stops.

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. When this command is used to enable the IGMP snooping functionality, if the number of entries in the MAC address table reaches the maximum and all necessary entries cannot be registered, the IGMP snooping functionality cannot operate properly. For the capacity limit of the MAC address table, see the description of the applicable MAC address table in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the configuration entries of the functionalities that use the MAC address table.

Related commands

None

ip igmp snooping (interface)

Enables the IGMP snooping functionality on a VLAN interface.

Syntax

To set information:

ip igmp snooping

To delete information:

no ip igmp snooping

Input mode

```
(config-if)
```

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. When this command is used to enable the IGMP snooping functionality on a VLAN interface, if the number of entries in the MAC address table reaches the maximum and all necessary entries cannot be registered, the IGMP snooping functionality cannot operate properly. For the capacity limit of the MAC address table, see the description of the applicable MAC address table in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the configuration entries of the functionalities that use the MAC address table.

Related commands

None

ip igmp snooping fast-leave

Immediately stops multicast communication to the applicable port if IGMP Leave and IGMPv3 Report (detachment request) messages are received on a VLAN interface.

Syntax

To set information:

ip igmp snooping fast-leave

To delete information:

no ip igmp snooping fast-leave

Input mode

`(config-if)`

Parameters

None

Default behavior

If IGMP Leave and IGMPv3 Report (detachment request) messages are received, make sure there are no members from the same multicast group on the applicable port, and then stop multicast communication. Multicast communication will continue (for a default value of 3 seconds) for the check process after IGMP Leave and IGMPv3 Report (detachment request) messages are received.

Impact on communication

None

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. Immediately stops multicast communication to the applicable port if you set this command and receive IGMP Leave and IGMPv3 Report (detachment request) messages. For this reason, if there are members from the same multicast group on the applicable port, multicast communication to the applicable members stops temporarily. In this case, multicast communication is restarted when an IGMP Report (membership request) message is received again from the applicable member.

Related commands

None

ip igmp snooping mrouter

Specifies a multicast router port on a VLAN interface.

Syntax

To set information:

ip igmp snooping mrouter interface <*interface type*> <*interface number*>

To delete information:

no ip igmp snooping mrouter interface <*interface type*> <*interface number*>

Input mode

`(config-if)`

Parameters

<*interface type*> <*interface number*>

Specifies an interface for which a multicast router port is set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*interface type*> <*interface number*>, the following values can be specified:

   - gigabitethernet <*nif no.*>/<*port no.*>

   - tengigabitethernet <*nif no.*>/<*port no.*>

   For <*nif no.*>/<*port no.*>, specify a NIF number or a port number. The specifiable ranges for <*nif no.*> and <*port no.*> is the numbers of the NIF and the port that belong to the VLAN.

   - port-channel <*channel group number*>

   The channel group number that can be specified for <*channel group number*> is the number of the channel group that contains the VLAN. For details about the setting range of the channel group number, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. If `ip igmp snooping` is not specified for the applicable interface, this functionality does not operate.
2. A maximum of eight multicast router ports can be set for each VLAN.
3. Some port-channel ports cannot be specified as multicast router ports. If you do so, the applicable port becomes invalid.

Related commands

ip igmp snooping

ip igmp snooping querier

Enables the IGMP querier functionality on a VLAN interface.

Syntax

To set information:

```
ip igmp snooping querier
```

To delete information:

```
no ip igmp snooping querier
```

Input mode

`(config-if)`

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. If `ip igmp snooping` is not specified for the applicable interface or the IP address is not set, the querier functionality does not operate.

Related commands

ip igmp snooping

ip address

Chapter

20. MLD Snooping

ipv6 mld snooping (global)

Suppresses the MLD snooping functionality on a Switch.

Syntax

To set information:

```
no ipv6 mld snooping
```

To delete information:

```
ipv6 mld snooping
```

Input mode

```
(config)
```

Parameters

None

Default behavior

Enables the MLD snooping functionality on a Switch.

Impact on communication

The MLD snooping functionality stops.

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. When this command is used to enable the MLD snooping functionality, if the number of entries in the MAC address table reaches the maximum and all necessary entries cannot be registered, the MLD snooping functionality cannot operate properly. For the capacity limit of the MAC address table, see the description of the applicable MAC address table in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the configuration entries of the functionalities that use the MAC address table.

Related commands

None

ipv6 mld snooping (interface)

Enables the MLD snooping functionality on a VLAN interface.

Syntax

To set information:

```
ipv6 mld snooping
```

To delete information:

```
no ipv6 mld snooping
```

Input mode

`(config-if)`

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. When this command is used to enable the MLD snooping functionality on a VLAN interface, if the number of entries in the MAC address table reaches the maximum and all necessary entries cannot be registered, the MLD snooping functionality cannot operate properly. For the capacity limit of the MAC address table, see the description of the applicable MAC address table in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the configuration entries of the functionalities that use the MAC address table.

Related commands

None

ipv6 mld snooping mrouter

Specifies a multicast router port on a VLAN interface.

Syntax

To set information:

ipv6 mld snooping mrouter interface <*interface type*> <*interface number*>

To delete information:

no ipv6 mld snooping mrouter interface <*interface type*> <*interface number*>

Input mode

`(config-if)`

Parameters

<*interface type*> <*interface number*>

Specifies an interface for which a multicast router port is set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*interface type*> <*interface number*>, the following values can be specified:

   - gigabitethernet <*nif no.*>/<*port no.*>

   - tengigabitethernet <*nif no.*>/<*port no.*>

   For <*nif no.*>/<*port no.*>, specify a NIF number or a port number. The specifiable range for <*nif no.*> and <*port no.*> is the numbers of the NIF and the port that belong to the VLAN.

   - port-channel <*channel group number*>

   The channel group number that can be specified for <*channel group number*> is the number of the channel group that contains the VLAN. For details about the setting range of the channel group number, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. If `ipv6 mld snooping` is not specified for the applicable interface, this functionality does not operate.
2. A maximum of eight multicast router ports can be set for each VLAN.
3. Some port-channel ports cannot be specified as multicast router ports. If you do so, the applicable port becomes invalid.

Related commands

ipv6 mld snooping

ipv6 mld snooping querier

Enables the MLD querier functionality on a VLAN interface.

Syntax

To set information:

ipv6 mld snooping querier

To delete information:

no ipv6 mld snooping querier

Input mode

```
(config-if)
```

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. If `ipv6 mld snooping` is not specified for the applicable interface or the IP address is not set, the querier functionality does not operate.

Related commands

ipv6 mld snooping

ipv6 address

Chapter

21. Error Messages Displayed When Editing the Configuration

21.1 Error messages displayed when editing the configuration

21.1.1 Common

Table 21-1: Common error messages

Message	Description
<value1> has already been set -- *<value2>*.	*<value1>* information has already been set. *<value2>* could not be set. Delete *<value1>* information or check if information you expected is set.
<value1> has already been set.	*<value1>* information has already been set. Delete *<value1>* information or check if information you expected is set.
<value1> is not in range from *<value2>* to *<value3>*.	The value of the *<value1>* parameter is outside the valid range. Set a value within the range.
	<value1>: Parameter name *<value2>*: Minimum value *<value3>*: Maximum value
Can not change it because data is not corresponding.	Cannot be changed because there is no matching data. Check if information to be changed exists.
Can not change mode from *<value1>* to *<value2>*.	Changing *<value1>* to *<value2>* is not allowed. Delete *<value1>*, and then add *<value2>*.
Can not delete it because data is not corresponding.	Data cannot be deleted because there is no matching data or duplicated data is specified. Check if there is data to be deleted or duplicated data is specified.
Can't delete this configuration referred by other configuration.	This configuration cannot be changed because it is specified by another configuration. Delete the configuration that refers to this configuration, and then retry the deletion.
Essential parameter *<value1>* has no value.	Because the *<value1>* information is a prerequisite condition for a setting that does not exist, the setting cannot be specified. Set the *<value1>* information.
Interface not found.	The specified interface cannot be found. Check the interface setting.
Invalid DUID. -- *<value1>*	*<value1>* is outside the valid DUID range. Set a value within the range.
	<value1>: Invalid value
Invalid IPv4 address. -- *<value1>*	*<value1>* is outside the valid IPv4 address range. Set a value within the range.
	<value1>: Invalid value
Invalid IPv6 address. -- *<value1>*	*<value1>* is outside the valid IPv6 address range. Set a value within the range.
	<value1>: Invalid value
Invalid line type.	The line type is invalid. Different line types are set within the same NIF.
Invalid MAC address. -- *<value1>*	*<value1>* is outside the valid MAC address range. Set a value within the range.
	<value1>: Invalid value

Message	Description
Invalid nif number. -- <*value1*>	<*value1*> is outside the valid NIF number range. Set a value within the range.
	<*value1*>: Invalid value
Invalid port number. -- <*value1*>	<*value1*> is outside the valid port number range. Set a value within the range.
	<*value1*>: Invalid value
Invalid Mask. -- <*value1*>	<*value1*> is outside the valid subnet mask range. Set a value within the range.
	<*value1*>: Invalid value
Maximum number of entries are already defined (config memory shortage). <*value1*>	Shared memory for the configuration is full. Delete entries that are no longer needed, execute the `save` command, and then add an entry.
	<*value1*>: Entry name
Maximum number of entries are already defined. <*value1*>	An attempt is being made to set a configuration that is larger than the capacity limit or to change a configuration in an environment already at the maximum capacity limit. Delete configurations that are no longer used, and then set the configuration again.
	<*value1*>: Entry name for the maximum capacity limit
Not found <*value1*>.	The specified <*value1*> information could not be found. Check if the <*vlaue1*> information has been set.
Port is not mounted -- <*value1*>.	The number of the port which is not mounted is specified. Set the number of the port which is mounted or check the status of the applicable NIF and port in the Switch.
	<*value1*>: NIF number/port number
Syntax error -- <*value1*>.	The configuration syntax or the value is invalid. Set the configuration again with the correct syntax or value.
	<*value1*>: Invalid value
The different name is already defined.	A different name is already set.
The number in which list specification is possible is <*value1*>.	The maximum number of specifiable elements is <*value1*>. Check if the number does not exceed the capacity limit.
	<*value1*>: Maximum number of elements that can be specified for a list
The sequence number exceeded the maximum value. Try "resequence" Command.	The sequence number exceeds the maximum value. To specify an entry, execute the `resequence` command, and then specify this entry again.
This configuration has already been set.	This configuration has already been set.
Too long value or illegal format (max <*value1*> characters).	The number of characters exceeds the maximum value (<*value1*>), or an invalid character exists. Use the determined format.
	<*value1*>: Number of characters that can be entered
Too long value or illegal format (max <*value1*> digit number).	The number of characters you entered exceeds the maximum number of digits (<*value1*>), or an invalid character exists. Use the determined format.

Message	Description
	<value1>: Number of digits that can be entered

21.1.2 Editing configurations and operation information

Table 21-2: Error messages displayed when editing the configuration

Message	Description
<process> is starting. Please try again.	A program is being started. Wait a while, and then re-execute the command.
	<process>: Program name
A specified number of interfaces exceeds the limitation.	The interface cannot be set because the number of interfaces exceeds the maximum value.
Cannot change standby configuration, because it is mismatch between active and standby system.	The configuration of the standby system cannot be changed because the type of boards installed on the active system and the type of boards installed on the standby system are different.
Cannot change standby configuration, because standby config memory shortage.*<reason>*	The configuration of the standby system cannot be changed because the standby system does not have enough shared memory. Use the `save` command or the `synchronize` command to match the configurations of both the active system and the standby system.
	<reason>: Additional information
Can't execute config command, please try again.	A communication error occurred between processes. Wait a while, and then re-execute the command.
Configuration command syntax error.line *<line number>* : "*<error syntax>*"	A configuration command of the source file has a syntax error.
	<line number>: Number of lines in a copy file *<error syntax>*: Error syntax
Configuration data cannot temporarily delete. Please try again.	Deletion is not permitted temporarily because the configuration you entered is not completed. Wait a while, and then re-execute the command.
Configuration file is empty.	There are no contents in the configuration.
Connection failed between active and standby system.	Communication between the active system and the standby system failed. The configuration might not be applied to the standby system. Use the `synchronize diff` command to check the synchronization status of the configuration. If the synchronization status between both systems is not good, execute the `save` or `synchronize` command to match the configurations of both systems.
Data transfer failed. (*<reason>*)	Transferring the configuration file to the remote server failed. Re-execute the command with the `debug` parameter specified for checking.
	<reason>: Additional information
File format error.	The file format is invalid. Make sure the name of the specified file is correct.
File name is a directory.	Directories cannot be specified. Specify a file name.
File name too long.	The specified file name is too long. Shorten the file name.
Filename or directory path is too long.	The path to the target is too long. Shorten the path length.

Message	Description
Logical inconsistency occurred.	A conflict occurred in the configuration. If you are editing data in a level-2 or level-3 configuration command mode, use the `show running-config` operation command to check whether the command that switched to the target command mode was deleted. If you interrupted the `end` or `quit` (`exit`) command by pressing **Ctrl** + **C**, and then executed the configuration command, use the `end` command to exit the configuration command mode. If the above cases do not apply, wait a while, and then re-execute the command.
No enough parameters.	No parameters are specified. Specify the necessary parameters.
No such file or directory.	The specified file or directory is not found. Specify the correct file name or directory name.
Not enough memory, configuration file is too big.	There is not enough memory to save the configuration because it is too large.
Not enough space on device.	Capacity at the write destination is insufficient. Delete files that are no longer needed.
Now configuration data is changing. Please try again.	The configuration you entered cannot be edited because it is not completed. Wait a while, and then re-execute the command.
Permission denied.	You do not have write permission for the target.
Resource temporarily unavailable.	Resource is temporarily insufficient. Wait a while, and then re-execute the command.
The command execution failed, because another command executing.	The command cannot be executed because it conflicts with a command which is being executed.
The command execution failed, because configuration file is editing.	This command cannot be executed because another user is editing the configuration.
The command execution failed, because configuration file is saving.	No edit command can be executed while saving the configuration.
The command execution failed, because mismatch found between active and standby configuration.	The configuration for the active system and the standby system are not the same. Use the `save` command or the `synchronize` command to match the configurations of both the active system and the standby system.
The command execution failed, because multiple commands can not execute simultaneously.	Multiple commands cannot be executed concurrently.
The command execution failed, because NIF board setting.	The command cannot be executed because the NIF board is being replaced.
The command execution failed, because software version mismatched.	The command cannot be executed because the software versions of the active system and the standby system are different.
The command execution failed, because switchover executing.	The command cannot be executed because the system is being switched.
The command execution failed, because system synchronizing active and standby configuration.	The command cannot be executed because the configuration of the standby system is synchronized with the configuration of the active system.

Message	Description
The configuration file on the active system was successfully changed, but the configuration file on the standby system was not changed because it failed in the copy of the configuration file.	Saving the configuration to the active system is successful, but the applying the configuration to the standby system failed.
The configuration on the active system was successfully changed, but the configuration on the standby system was not changed.<*reason*>	The configuration of the standby system cannot be changed because a problem occurred in an internal program. Use the `save` command or the `synchronize` command to match the configurations of both the active system and the standby system.
	<*reason*>: Additional information
The saving command is being executed, please try again.	The operation is not permitted because the `save` command is being executed. Wait a while, and then re-execute the command.
This configuration is active.	The configuration cannot be changed because it matches the installation.

21.1.3 Login security and RADIUS or TACACS+ information

Table 21-3: Error messages related to login security and RADIUS or TACACS+

Message	Description
Maximum number of entries are already defined. <*value1*>	You are trying to add more than the allowable maximum number of entries. Delete entries that are no longer needed, and then add the entries.
	<*value1*>: Entry name
Port Number is duplicate between auth port and acct port.	The port numbers for `auth-port` and `acct-port` are the same.

21.1.4 Host names and DNS information

Table 21-4: Error messages related to host names and DNS

Message	Description
Same name <*value*> has already been set.	The same name (<*value*>) has already been set.

21.1.5 Switch management information

Table 21-5: Error messages related to switch management

Message	Description
Cannot change the configuration because there is an inconsistency between fldm and ip dhcp snooping.	The configuration cannot be changed because there is a conflict between the DHCP snooping setting and the flow distribution pattern setting. If you set the flow distribution pattern as shown below, delete the DHCP snooping setting: • fldm prefer default standard • fldm prefer {default | filter-only | qos-only | filter | qos} extended • fldm prefer qos-only extended-advance
Cannot change the configuration because there is an inconsistency between fwdm and policy based routing.	The configuration cannot be changed because there is an inconsistency between the allocation pattern settings for routing table entries and the policy-based routing settings. Review the configuration.

Message	Description
Cannot change the fldm, because the maximum number of entries are exceeded.	The capacity limit after the flow distribution pattern is changed will be exceeded. Before changing the flow distribution pattern, set the number of entries so that it can be fewer than the capacity limit of the flow distribution pattern after the change.
Cannot change the hardware mode for access list logging, because access list logging is set.	`access-log` for `system hardware-mode` cannot be deleted because access list logging is set. To delete `access-log` for `system hardware-mode`, delete the access list logging setting first. Applicable commands are as follows: • access-log enable • access-log interval • access-log rate-limit • access-log threshold
Cannot change the hardware mode for access list logging, because access-list is set.	`access-log` for `system hardware-mode` cannot be deleted because the access list for which `log` is specified is set. To delete `access-log` for `system hardware-mode`, delete the access list for which `log` is specified.
Cannot set the fldm, because of advance access-list or advance qos-flow-list.	The current flow distribution pattern cannot be set because a list that cannot be specified is applied. If you specify `standard` or `extended` as the flow distribution pattern, delete `advance access-list` and `advance qos-flow-list` first.
Cannot set the fldm, because of flow mac mode.	The current flow distribution pattern cannot be set because MAC mode is set. If you specify `standard-advance` or `extended-advance` as the flow distribution pattern, delete the MAC mode setting first.

21.1.6 Power saving functionality information [AX6700S] [AX6600S]

Table 21-6: Error messages related to the power saving functionality

Message	Description
Cannot change <*value1*> configuration while "adaptive-power-control enable" exist.	`adaptive-power-control enable` has already been set. <*value1*> could not be set. Delete `adaptive-power-control enable` or check if information you expected is set.
	<*value1*>: Indicates a command name.
Cannot change <*value1*> configuration while "power-control mode1" exist.	`power-control mode1` has already been set. <*value1*> could not be set. Delete `power-control mode1` or check if information you expected is set.
	<*value1*>: Indicates a command name.
Cannot change <*value1*> configuration while "redundancy bsu-load-balancing smac" or "redundancy bsu-mode fixed" exist.	The `redundancy bsu-load-balancing smac` command or the `redundancy bsu-mode fixed` command has already been set. <*value1*> could not be changed. Delete the `redundancy bsu-load-balancing smac` command or the `redundancy bsu-mode fixed` command. Alternatively, check whether the expected entry has already been set.
	<*value1*>: Indicates a command name.
Cannot change <*value1*> configuration while "redundancy standby-bsu cold" exist.	`redundancy standby-bsu cold` has already been set. <*value1*> could not be set. Delete `redundancy standby-bsu cold` or check whether information you expected is set.
	<*value1*>: Indicates a command name.

Message	Description
Cannot change <*value1*> configuration while "schedule-power-control time-range" exist.	`schedule-power-control time-range` has already been set. <*value1*> could not be set. Delete `schedule-power-control time-range` or check whether information you expected is set.
	<*value1*>: Indicates a command name.
Cannot set <*value1*> configuration while changing power control mode.	<*value1*> could not be set because the power control mode is being changed. Check if the power control of the `show system` command does not show `changing`.
	<*value1*>: Indicates a command name.
Cannot set the schedule, because there is no interval of 30 minutes or more between the "start-time" and the "end-time".	The schedule cannot be set because a difference between the start time and the end time is less than 30 minutes. Check the start date and time and the end date and time for `schedule-power-control time-range`.
Relations between "end-time" and "start-time" are inconsistent.	The schedule cannot be set because a date and time earlier than the start date and time is specified for the end date and time. Check the start date and time and the end date and time for `schedule-power-control time-range`.
Relations between "schedule-power-control time-range" and other "schedule-power-control time-range" are inconsistent.	The schedule cannot be set because `schedule-power-control time-range` overlaps with another time set for `schedule-power-control time-range`. Check `schedule-power-control time-range` you set or `schedule-power-control time-range` to be set.
Relations between adaptive-power-control max-psp and UPC entry are inconsistent.	The configuration cannot be changed because there is a conflict between the number of PSPs to be used while traffic-based power saving functionality is enabled and QoS flow list settings with bandwidth monitoring. To change the number of PSPs to be used while traffic-based power saving functionality is enabled, delete the QoS flow list of which bandwidth monitoring is specified for the VLAN interface on the receiving side.
Relations between adaptive-power-control max-psp and upc-storm-control mode are inconsistent.	The configuration cannot be changed because there is a conflict between the number of PSPs to be used while traffic-based power saving functionality is enabled and bandwidth monitoring storm control mode settings. To change the number of PSPs to be used while traffic-based power saving functionality is enabled, specify `upc-in-in` or `upc-in-and-storm-control` for bandwidth monitoring storm control mode.
Relations between schedule-power-control max-psp and UPC entry are inconsistent.	The configuration cannot be changed because there is a conflict between the number of PSPs to be used while scheduled power saving functionality is enabled and QoS flow list settings with bandwidth monitoring. To change the number of PSPs to be used while scheduled power saving functionality is enabled, delete the QoS flow list of which bandwidth monitoring is specified for the VLAN interface on the receiving side.
Relations between schedule-power-control max-psp and upc-storm-control mode are inconsistent.	The configuration cannot be changed because there is a conflict between the number of PSPs to be used while scheduled power saving functionality is enabled and bandwidth monitoring storm control mode settings. To change the number of PSPs to be used while scheduled power saving functionality is enabled, specify `upc-in-in` or `upc-in-and-storm-control` for bandwidth monitoring storm control mode.

21.1.7 Ethernet information

Table 21-7: Ethernet error messages

Message	Description
Can not change media-type.	The applicable port cannot be changed from 10BASE-T, 100BASE-TX, or 1000BASE-T to 1000BASE-X, and vice versa.
Cannot attach the interface specified as a ring-port to the channel-group.	The interface set as a ring port cannot participate in the port channel. To allow the specified interface to participate in the port channel, first delete the ring-related configuration.
Cannot attach the interface that specified cfm enable to the channel-group.	The interface port of which CFM is set to `enable` cannot participate in the port channel. To allow the specified interface to participate in the port channel, first delete `enable` for CFM.
Cannot attach the interface that specified mep to the channel-group.	The interface for which MEP is set cannot participate in the port channel. To allow the specified interface to participate in the port channel, first delete MEP.
Cannot attach the interface that specified mip to the channel-group.	The interface for which MIP is set cannot participate in the port channel. To allow the specified interface to participate in the port channel, first delete MIP.
The command execution failed, because NIF <*value1*> is not mounted.	The command cannot be executed because the specified NIF is not installed.
	<*value1*>: NIF number
this command is different from this one in channel-group port.	The configured command and the port channel configuration do not match. Match the configuration of the port channel to the configuration of the command.

21.1.8 Link aggregation information

Table 21-8: Link aggregation error messages

Message	Description
Can not change channel-group mode.	The channel group mode cannot be changed. To change it, you must specify multiple ports to delete channel group mode, and then set it again
Can not delete interface of channel-group because specified port status is up.	The port cannot be deleted because `shutdown` is not set on some ports. Use the configuration to shut down the applicable ports.
Channel-group <*value1*> has already been set -- <*value2*> cannot be set.	The same mode cannot be set under the same interface.
	<*value1*>: Channel group you have set <*value2*>: Channel group you attempted to set
Maximum number of channel-group port are already defined.	No more ports can be set. Review the number of ports for each channel group.
Relations between interface of channel-group and tpid and jumbo_frame in port configuration are inconsistent.	Information about the interface for which `channel-group` is set and the interface for which `tpid` and `jumbo_frame` are set is inconsistent.
The different kind of channel-group mode has already been set -- <*mode*> cannot be set.	The mode of the channel group which is currently set cannot be changed.
	<*mode*>: Mode you attempted to set

Message	Description
this command is different from this one in channel-group port.	Different settings were found on ports specified for the same channel group. The configuration of the ports specified for the same channel group must either match or be deleted.

21.1.9 MAC address table information

Table 21-9: MAC address table error messages

Message	Description
Invalid MAC address. -- <*value1*>	The specified MAC address cannot be set because it is used by the Ring Protocol. Specify a MAC address other than `0012.E2E0.0F00` to `0012.E2E0.0F0F`.
	<*value1*>: Specified MAC address
Relations between vlan in mac-address-table static configuration and switchport configuration are inconsistent.	The `mac-address-table static` VLAN specification and the `switchport` configuration do not match. A VLAN set by using `mac-address-table static` must be specified for `switchport access` or `switchport trunk allowed vlan` of the interface that has been set.

21.1.10 VLAN information

Table 21-10: VLAN error messages

Message	Description
Cannot change vlan configuration referred by flow configuration.	The specified vlan configuration cannot be changed because it is specified by a filter or the QoS configuration. To change the specified vlan configuration, delete the filter or the QoS configuration set for the specified vlan configuration first.
Cannot change vlan configuration, because the target port has a qos-flow-list with user id parameters.	The settings for the VLAN cannot be changed because the QoS flow list that contains user ID specification (<*user id*>, `llrlq1`, or `llrlq2`) is applied to the Outbound QoS flow list. If a QoS flow list entry for which user ID is specified is applied, set the same shaper settings (shaper mode or the number of shaper queues) in the NIF to which the interfaces contained in the VLAN belong.
Cannot change vlan configuration, because the vlan has a qos-flow-list with user id parameter.	The settings for the VLAN cannot be changed because the QoS flow list that contains user ID specification (<*user id*>, `llrlq1`, or `llrlq2`) is applied to the Outbound QoS flow list. Delete the QoS flow list that contains user ID specification first.
Cannot delete protocol referred by VLAN configuration.	You are trying to specify a protocol name to be deleted by using the `protocol` command of the VLAN. Delete the `protocol` command specification, and then delete the protocol name.
Can't delete vlan <*vlan id*> configuration referred by <*value1*> configuration.	The specified VLAN cannot be deleted because it is used by another configuration.
	<*vlan id*>: Indicates the VLAN ID. <*value1*>: Configuration for which VLAN is set
Can't set <*value1*> which is not configured to use vlan <*vlan id*>.	The specified VLAN ID has not been set.
	<*value1*>: Configuration for which VLAN ID is set <*vlan id*>: Indicates the VLAN ID.

Message	Description
Duplicate translated-tag.	The specified translated ID is being used by another VLAN. Check the following: • The same translated ID is not used by another VLAN. • The VLAN ID for which `allowed-vlan` is specified, but `translated-tag` is not specified is not specified.
Maximum number which can be used is exceeded.	A maximum of 16 protocol values (`ethertype` value, `llc` value, and `snap-ethertype` value) are used in the entire Switch. No more than 16 VLANs can be set.
Not found VLAN-ID <*vlan id*>.	The specified VLAN ID is not set.
	<*vlan id*>: Indicates the VLAN ID.
Relations between flow mac mode and access-list are inconsistent.	MAC mode is specified for the specified VLAN and an access list is set for the specified Ethernet interface. Because of this, the specified VLAN ID cannot be set for the Ethernet interface.
Relations between flow mac mode and qos-flow-list are inconsistent.	MAC mode is specified for the specified VLAN and the QoS flow list is set for the specified Ethernet interface. Because of this, the specified VLAN ID cannot be set for the Ethernet interface.
Relations between igmp snooping and l2-isolation are inconsistent.	The IGMP snooping functionality and the Layer 2 relay blocking functionality cannot be set concurrently.
Relations between mac-based and vlan-tunneling-enable are inconsistent.	MAC VLANs and VLAN tunneling cannot be set concurrently.
Relations between mld snooping and l2-isolation are inconsistent.	The MLD snooping functionality and the Layer 2 relay blocking functionality cannot be set concurrently.
Relations between protocol-based and vlan-tunneling-enable are inconsistent.	A protocol VLAN and VLAN tunneling cannot be set concurrently.
Relations between vlan in mac-address-table static configuration and switchport configuration are inconsistent.	The `mac-address-table static` VLAN specification and the `switchport` configuration do not match. A VLAN set by using `mac-address-table static` must be specified for `switchport access` or `switchport trunk allowed vlan` of the interface that has been set.
Relations between vlan-tunneling and IP configuration are inconsistent.	VLAN tunneling information and IP information are inconsistent. When VLAN tunneling is set, IP information cannot be set.
VLAN is not MAC VLAN.	A VLAN specified by `switchport mac vlan` is not a MAC VLAN. Specify a MAC VLAN.
VLAN is not Port VLAN.	The specified VLAN is not a port VLAN. Specify a port VLAN.
VLAN is not Protocol VLAN.	A VLAN specified by `switchport protocol vlan` is not a protocol VLAN. Specify a protocol VLAN.

21.1.11 Spanning Tree information

Table 21-11: Spanning Tree error messages

Message	Description
Can not configure spanning-tree when gsrp is configured.	The Spanning Tree Protocol cannot be set because GSRP is set.
Cost is over 65535, please set up in 1 to 65535 or set pathcost method to long.	The value for `cost` is equal to or greater than 65535. Set the `cost` value from 1 to 65535 or set `long` for `pathcost method`.

Message	Description
Inconsistency is found between the vrf mode and the spanning-tree configuration.	The spanning tree cannot be set because VRF is set.
Maximum number of MST instance are already defined.	The number of MST instances has already reached the maximum number. The maximum number of MST instances that can be set is 16.
Pathcost method is short, please set up in 1 to 65535 or set pathcost method to long.	`short` is set for `pathcost method`. Set the `cost` value from 1 to 65535 or set `long` for `pathcost method`.
Relations between PVST+ and l2protocol-tunnel stp configuration are inconsistent.	PVST+ and BPDU forwarding cannot be set concurrently.
Relations between PVST+ and the protocol-vlan or mac-vlan configuration are inconsistent.	PVST+ and a protocol VLAN or a MAC VLAN cannot be set concurrently.
spanning-tree: maximum number of MST instance are already defined.	The number of MST instances has already reached the maximum number. The maximum number of MST instances that can be set is 16.

21.1.12 Ring Protocol information

Table 21-12: Ring Protocol error messages

Message	Description
axrp-<*ring id*>-<*group id*>: vlan-mapping <*mapping id*> is already configured in another vlan-group.	The specified VLAN mapping has already been set for a VLAN group in the same ring. Either delete the VLAN mapping from another VLAN group or use another VLAN mapping.
	<*ring id*>: Ring ID <*group id*>: VLAN group ID <*mapping id*>: VLAN mapping ID
axrp-<*ring id*>: cannot configure this command to channel-group port.	A ring port cannot be set for an interface that is participating in a port channel.
	<*ring id*>: Ring ID
axrp-<*ring id*>: maximum number of ring-id are already defined.	The maximum number of ring IDs that can be used in a Switch is 16. No more than 16 VLANs can be set. To add a ring ID, you must first delete a registered ring ID.
	<*ring id*>: Ring ID
axrp-<*ring id*>: maximum number of ring-port are already defined.	Set two ring ports for each ring ID. To set another port as a ring port, first delete a ring port that has already been set.
	<*ring id*>: Ring ID
axrp-<*ring id*>: shared-edge port is already defined in another ring-port.	As for shared ports, `shared-edge` is already set for another ring port. To set another port as a `shared-edge` shared port, first delete a shared port that has already been set.
	<*ring id*>: Ring ID
axrp-<*ring id*>: The maximum number of entries are exceeded.	The number of entries exceeded the capacity limit. Delete the ring that has already been set, and then add it.
	<*ring id*>: Ring ID

Message	Description
axrp-<*ring id*>: this interface is already defined as a ring port of other ring configured the same vlan-mapping.	The specified interface has already been set as a ring port of another ring to which the same VLAN mapping as the ring set by using this command is applied. Set the applicable interface as a shared link or specify another interface.
	<*ring id*>: Ring ID
axrp-<*ring id*>: vlan <*vlan id*> is already configured in control-vlan of other ring.	The specified VLAN has already been set in the control VLAN of another ring. Either delete the applicable VLAN from the other ring's control VLAN or use another VLAN.
	<*ring id*>: Ring ID <*vlan id*>: Indicates the VLAN ID.
axrp-<*ring id*>: vlan <*vlan id*> is already configured in virtual-link.	The specified VLAN has already been set for a virtual link. Either delete the applicable VLAN from the virtual link or use another VLAN.
	<*ring id*>: Ring ID <*vlan id*>: Indicates the VLAN ID.
axrp-<*ring id*>: vlan <*vlan id*> is already configured in vlan-mapping.	The specified VLAN has already been set for VLAN mapping. Either delete the applicable VLAN from the VLAN mapping or use another VLAN.
	<*ring id*>: Ring ID <*vlan id*>: Indicates the VLAN ID.
axrp-<*ring id*>: vlan-mapping <*mapping id*> is already configured in vlan-group of other ring.	The specified VLAN mapping has already been set for a VLAN group in another ring. Either delete the VLAN mapping from the other VLAN group or use other VLAN groups.
	<*ring id*>: Ring ID <*mapping id*>: VLAN mapping ID
axrp-virtual-link-<*link id*>: vlan <*vlan id*> is already configured in control-vlan.	The specified VLAN has already set in the control VLAN. Either delete the applicable VLAN from the control VLAN or use another VLAN.
	<*link id*>: Virtual link ID <*vlan id*>: Indicates the VLAN ID.
axrp-vlan-mapping-<*mapping id*>: vlan <*vlan id*> is already configured in control-vlan.	The specified VLAN has already been set in the control VLAN. Either delete the applicable VLAN from the control VLAN or use another VLAN.
	<*mapping id*>: VLAN mapping ID <*vlan id*>: Indicates the VLAN ID.
axrp-vlan-mapping-<*mapping id*>: vlan <*vlan id*> is already configured in other vlan-mapping.	The specified VLAN has already been set for another mapping. Either delete the applicable VLAN from the other VLAN mapping or use another VLAN.
	<*mapping id*>: VLAN mapping ID <*vlan id*>: Indicates the VLAN ID.

Message	Description
Inconsistency is found between the vrf mode and the axrp configuration.	After the VRF functionality is applied, commands cannot be set because any of the following reasons: • The Ring Protocol cannot be set if `l2protocol-disable`, `l2protocol-disable-ipv4-ipv6`, or `gsrp-enable-ipv4-ipv6` is set for the `vrf mode` command. • When the configuration of the Ring Protocol is set, `l2protocol-disable`, `l2protocol-disable-ipv4-ipv6`, and `gsrp-enable-ipv4-ipv6` cannot be set for the `vrf mode` command. • A value equal to or greater than 65 cannot be set as a VLAN mapping ID if `axrp-enable` or `axrp-enable-ipv4-ipv6` is set for the `vrf mode` command. Specify a value equal to or less than 64 as a VLAN mapping ID. • If a value equal to or greater than 65 is set as a VLAN mapping ID, you cannot set `axrp-enable` and `axrp-enable-ipv4-ipv6` for the `vrf mode` command. Specify a value equal to or less than 64 as a VLAN mapping ID.
vlan-mapping-id <*vlan mapping id*> is already configured in vlan-group-id.	The specified VLAN mapping ID has already been set as a VLAN group ID. Either delete the applicable VLAN group ID from GSRP or use another VLAN mapping ID.
	<*vlan mapping id*>: VLAN mapping ID

21.1.13 Policy-based switching information

Table 21-13: Policy-based switching error messages

Message	Description
Because VLAN ID is used by Policy base switching not revocable.	The VLAN ID of the destination interface cannot be changed because it is being used by policy-based switching. Delete all the routing information for policy-based switching, and then try again.
Cannot change and delete vlan because interface appointed uses by policy based switching.	The VLAN ID set for the interface cannot be changed or deleted, because the specified interface is being used in policy-based switching. When changing or deleting the VLAN ID set for the specified interface, first delete the routes that are used in policy-based switching.
Cannot change and delete vlan because port-channel appointed uses by policy based switching.	The VLAN ID set for a channel group cannot be changed or deleted, because the specified channel group is being used in policy-based switching. When changing or deleting the VLAN ID set for the specified channel group, first delete the routes that are used in policy-based switching.
Cannot change the configuration because there is an inconsistency between fldm and policy based switching.	The configuration cannot be changed because there is an inconsistency between the allocation pattern settings for flow table entries and the policy-based switching settings. Review the configuration.
Cannot change the configuration because there is an inconsistency between fwdm and policy based switching.	The configuration cannot be changed because there is an inconsistency between the allocation pattern settings for routing table entries and the policy-based switching settings. Review the configuration.
Cannot set policy based switching entry because specified interface is invalid.	Policy-based switching cannot be set for the following reasons: • The specified destination interface does not exist. • The specified destination channel group does not exist. • The VLAN ID of the specified destination interface or destination channel group and the VLAN ID set by using the `policy-vlan` command do not match. Check for the above problems, fix the problems, and then set policy-based switching.

Message	Description
Cannot set the configuration because there is an inconsistency between vlan and policy based switching.	The VLAN ID of the destination interface cannot be edited because there is an inconsistency between the VLAN ID of the destination interface for policy-based switching and the filter condition settings. When editing the VLAN ID of the destination interface for policy-based switching, delete the filter detection conditions first. You cannot specify, for filter detection conditions, a VLAN ID other than the VLAN ID of the destination interface specified in the policy-based switching list information.
Can't execute command it because data is not corresponding.	The list number specified by the `policy-switch-list resequence` command does not exist.
The list number specified by resequence of policy base switching does not have the target route.	There is no target route in the list number specified by the `policy-switch-list resequence`.
The maximum number of entries are exceeded.	The number of routes in the policy-based switching group exceeds the capacity limit of the Switch.

21.1.14 IGMP snooping information

Table 21-14: IGMP snooping error messages

Message	Description
Maximum number of mrouter are already defined.	The number of mrouters that can be specified for each VLAN by using the IGMP snooping functionality is 8. No more than 8 mrouters can be set.
Maximum number of VLAN are already defined.	The number of VLANs that can be specified by using the IGMP snooping functionality is 256. No more than 256 VLANs can be set.
Relations between igmp snooping and vlan mapping are inconsistent.	VLAN mapping cannot be specified for a trunk port in a VLAN for which the IGMP snooping functionality is set.
Relations between igmp snooping and vlan-tunneling are inconsistent.	The IGMP snooping functionality and VLAN tunneling cannot be specified concurrently.
Relations between mrouter in igmp snooping configuration and channel-group configuration are inconsistent.	To specify an mrouter by using a channel group number, specify a channel group number that has already been set.
Relations between mrouter in igmp snooping configuration and switchport configuration are inconsistent.	The port or the channel group specified by an mrouter does not belong to the applicable VLAN. Specify the port or the channel group that belongs to the VLAN.

21.1.15 MLD snooping information

Table 21-15: MLD snooping error messages

Message	Description
Maximum number of mrouter are already defined.	The number of mrouters that can be specified for each VLAN by using the MLD snooping functionality is 8. No more than 8 mrouters can be set.
Maximum number of VLAN are already defined.	The number of VLANs that can be specified by using the MLD snooping functionality is 256. No more than 256 VLANs can be set.
Relations between mld snooping and vlan mapping are inconsistent.	VLAN mapping cannot be specified for a trunk port in a VLAN for which the MLD snooping functionality is set.
Relations between mld snooping and vlan-tunneling are inconsistent.	The MLD snooping functionality and VLAN tunneling cannot be specified concurrently.

Message	Description
Relations between mrouter in mld snooping configuration and channel-group configuration are inconsistent.	To specify an mrouter by using a channel group number, specify a channel group number that has already been set.
Relations between mrouter in mld snooping configuration and switchport configuration are inconsistent.	The port or the channel group specified by an mrouter does not belong to the applicable VLAN. Specify the port or the channel group that belongs to the VLAN.

Index