AX3800S/AX3650S Software Manual

Configuration Guide Vol. 1

For Version 11.10

AX38S-S001X-40

AlaxalA

■ Relevant products

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

■ Export restrictions

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

■ Trademarks

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

Ethernet is a registered trademark of Xerox Corporation.

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

IPX is a trademark of Novell, Inc.

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

Octpower is a registered trademark of NEC Corporation.

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

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

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

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

VLANaccessClient is a trademark of NEC Soft, Ltd.

VLANaccessController and VLANaccessAgent are trademarks of NEC Corporation.

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

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

■ Reading and storing this manual

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

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

■ Notes

Information in this document is subject to change without notice.

■ Editions history

December 2012 (Edition 5) AX38S-S001X-40

■ Copyright

History of Amendments

[For version 11.10]

Summary of amendments

Location and title	Changes
3.1.1 Maximum number of lines	• Descriptions were changed because AX3800S series switches now support stack ports.
3.2 Capacity limit	• Notes were added to *(1) Number of table entries for AX3830S series switches* and *(2) Number of table entries for AX3650S series switches* of 3.2.1 *Number of table entries*. • A note was added to *(1) MAC address table* of 3.2.3 *Layer 2 switching*. • *(2) VLAN* of 3.2.3 *Layer 2 switching* was changed because AX3800S series switches now support stack ports. • 3.2.4 *Filters and QoS* was changed because AX3800S series switches now support stack ports.
7 Description of Stack Functionality	• AX3800S series switches now support stack ports.
7.3.2 Stack port and stack link	• Descriptions were changed because AX3800S series switches now support stack ports.
7.7.2 Notes on stacks	• *(9) Using the master selection priority 1* was added.
8 Settings and Operation for Stack Functionality	• AX3800S series switches now support stack ports.
8.1.8 Adding a stack link	• This subsection was added.
8.1.9 Deleting a stack link	• This subsection was added.
8.2.3 Displaying the switch state and the switch number on the front panel	• This subsection was added.

In addition to the above change, minor editorial corrections have been made.

[For version 11.9]

Summary of amendments

Item	Changes
Range of Switch models	• A description for AX3830S-44X4QW was added.
Line and module capacities	• A description for AX3830S-44X4QW was added.
Capacity limit	• A description for AX3830S-44X4QW was added to *(2) VLAN* in *Layer 2 switching.* • A description of the layer3-6 flow detection mode for the receiving side was added to *Filters and QoS.* • *(5) Policy-based routing (IPv4)* in *Forwarding IPv4 and IPv6 packets* was changed because AX3800S series switches now support IPv4 policy-based routing. • The number of PIM-SM or PIM-SSM multicast interfaces and the number of multicast neighboring routers were changed in *(1) IPv4 multicasting* and *(2) IPv6 multicasting in IPv4 and IPv6 multicast routing protocols*.
Switch states	• *(2) Change process after a switch state transition* was added.
Operation management of stack	• A description was added to *(2) Execution of operation commands*. • *(6) Software management* was changed.
Notes on stacks	• *(8) Switching over the master switch* was added.
Deleting a member switch (backup switch)	• A workflow for deleting a member switch (master switch) was changed.

Item	Changes
Description of the 40GBASE-R interface	• This section was added.
Configuration of the 40GBASE-R interface	• This section was added.
Description of the QSFP+ port	• This section was added.

[For version 11.8]

Summary of amendments

Item	Changes
Line and module capacities	• A description of stack ports was added to *Maximum number of lines*.
Capacity limit	• The number of VLANs and the number of VLAN tunnels in the stack configuration were added to *Layer 2 switching*. • The maximum number of filter entries in the stack configuration was added to *Filters and QoS*.
Operation terminals	• A description of a serial connection with a member switch in the stack configuration was added.
Description of Stack	• This chapter was added.
Settings and Operation for Stack	• This chapter was added.

[For version 11.7]

Summary of amendments

Item	Changes
Hardware for AX3830S series switches	• PS-A03R, PS-D03, and PS-D03R were added to the description of the power supply units. • FAN-04R was added to the description of the fan units.
Hardware for AX3650S series switches	• PS-D03 was added to the description of the power supply units.
Software	• Descriptions were changed because AX3650S series switches now support OS-L3SL-A/OS-L3SL. • A description of policy-based routing was added.
Capacity limit	• The number of static entries was changed in *(1) MAC address table* in *Layer 2 switching*. • A description of the layer3-6 flow detection mode for the receiving side was added to *Filters and QoS*. • *(5) Policy-based routing (IPv4)* was added to *Forwarding IPv4 and IPv6 packets*.

[For version 11.6]

This manual contains descriptions of the AX3650S that were in the manual *AX3600S Software Manual For Version 11.5*.

Summary of amendments

Item	Changes
Features of the Switch	• Descriptions for AX3800S series switches were added.
Range of Switch models	• Descriptions for AX3800S series switches were added.
External view	• Descriptions for AX3800S series switches were added.
Hardware for AX3830S series switches	• This subsection was added.

Item	Changes
Software	- Descriptions for AX3800S series switches were added.
Line and module capacities	- Descriptions for AX3800S series switches were added to *Maximum number of lines*. - Descriptions for AX3800S series switches were added to *Mounted power supply unit*.
Capacity limit	- Descriptions for AX3800S series switches were added to *Number of table entries*. - *Filters and QoS* was added. - Descriptions for AX3800S series switches were added to *DHCP snooping*. - The range of IP addresses that are excluded from assignment was added to *(7) DHCP server* in *Forwarding IPv4 and IPv6 packets*. - Descriptions for AX3800S series switches were added to *IPv4 and IPv6 routing protocols*.
Permitting login from VRF by using Telnet protocol	- *(2) To permit login via Telnet from a specific VRF* was added.
Permitting login from VRF by using FTP	- *(2) To permit login via FTP from a specific VRF* was added.
Functionality	- Connection specifications of AX3800S series switches were added to *(b) 10BASE-T, 100BASE-TX, and 1000BASE-T connection specifications*.

Preface

Applicable products and software versions

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

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

Unless otherwise noted, this manual describes the functions applicable to both the AX3800S and AX3650S series of switches, and functionalities common to each software package. For functionalities that are not common to both AX3800S and AX3650S series switches, and functionalities not common to OS-L3SA-A/OS-L3SA and OS-L3SL-A/OS-L3SL are indicated as follows:

[AX3800S]:

The description applies to AX3800S switches.

[AX3650S]:

The description applies to AX3650S switches.

[OS-L3SA]:

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

The functions supported by optional licenses are indicated as follows:

[OP-DH6R]:

The description applies to the OP-DH6R optional license.

[OP-OTP]:

The description applies to the OP-OTP optional license.

[OP-VAA]:

The description applies to the OP-VAA optional license.

Corrections to the manual

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

Intended readers

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

Readers must have an understanding of the following:

- The basics of network system management

Manual URL

You can view this manual on our website at:

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

Reading sequence of the manuals

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

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

Quick Start Guide
(AX36S-Q001X)

● **Determining the hardware facility conditions and how to handle the hardware**

Hardware Instruction Manual
(AX36S-H001X)

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

Configuration Guide Vol.1
(AX38S-S001X)

Vol.2
(AX38S-S002X)

Vol.3
(AX38S-S003X)

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

Configuration Command Reference Vol. 1
(AX38S-S004X)

Vol.2
(AX38S-S005X)

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

Operation Command Reference Vol. 1
(AX38S-S006X)

Vol.2
(AX38S-S007X)

● **Understanding messages and logs**

Message and Log Reference
(AX38S-S008X)

● **Understanding the MIB**

MIB Reference
(AX38S-S009X)

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

Troubleshooting Guide
(AX36S-T001X)

Conventions: The terms "Switch" and "switch"

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

AX3800S series switch

AX3650S series switch

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

Abbreviations used in the manual

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

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

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

Conventions: KB, MB, GB, and TB

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

Contents

Preface i

PART 1: Overview and Capacity Limits of the Switch

PART 2: Operation Management

5. Command Operations 83

6. Configuration 93

7. Description of Stack Functionality 111

PART 4: Layer 2 Switching

Chapter

1. Overview of the Switch

This chapter describes the features of the Switch.

1.1 Overview of the Switch

In today's businesses, PCs are provided to every worker and corporate networks are used for many purposes such as IP telephony, Internet access, and core business activities. As a result, businesses are faced with ever-growing communication traffic.

Networks carry mission-critical data that influences corporate profits. Formerly, the mission-critical market was focused on Internet service providers (ISPs) and network providers. In the future, however, this market will increasingly expand into corporate and public local area networks.

Through their applicability to mission-critical fields, the Switch provides flexible options for building a highly reliable, available, and scalable information network infrastructure.

Product concept

The Switch is a compact box-type multilayer switch that achieves a balance between switching capacity, cost, and the functionality required by corporate networks while also incorporating the carrier-grade switch technology developed by ALAXALA Networks Corporation to realize its guaranteed network concept.

The Switch delivers the following functionality:

- Provide cutting-edge IPv6 and multicast capabilities, plus routing protocols such as OSPF and BGP4 used by large-scale networks, for configuring a wide variety of flexible networks.
- Support various types of network redundancy for highly reliable and highly available networking.
- The stack functionality connects multiple switches to make them operate as one logical switch, providing centralized management, redundancy, and scalability.
- Feature link aggregation and 10 Gbit/s and 40 Gbit/s ports which provide sufficient network capacity to meet increased traffic demands.
- Provide a guaranteed network to protect the entire range of traffic handled within a company (such as core work data, VoIP telephony data, teleconferencing, video streaming, and CAD data) using QoS technology and other functions.
- Safeguard networks by security functionality such as high-performance filtering and user authentication.
- Enable full-wire-rate packet forwarding.
- Support Open Autonomic Networking (OAN) to reduce the total cost of designing, configuring, and operating a network.
- Network partitioning that reduces the costs required to configure and operate a network by virtually handling and integrating multiple service networks in a physical network.

1.2 Features of the Switch

(1) Support for a variety of high-speed VLAN functionality

- Layer 2 VLAN functionality
    - Equipped with port VLAN, protocol VLAN, and MAC VLAN functionality
    - Enables purpose-built VLANs
- Spanning Tree Protocols
    - Supports the Spanning Tree Protocol (IEEE 802.1D), the Rapid Spanning Tree Protocol (IEEE 802.1w), PVST+, and Multiple Spanning Tree (IEEE 802.1s)
- Layer 2 - Virtual Private Network (L2-VPN) using VLAN tunneling

(2) Robust security

- Authentication and quarantine solutions
    - Layer 2 authentication functionality (IEEE 802.1X, Web authentication, MAC-based authentication, authentication VLAN) enables individual PCs to be authenticated and placed into a VLAN, while maintaining the freedom of the physical configuration at the network edges.
    - By combining a quarantine server and authentication server, a quarantine solution can be implemented whereby a PC is automatically connected to an enterprise VLAN only if it has passed a quarantine check.
- Advanced and fine-grained packet filtering
    - Hardware-based high-performance filtering processes
    - Partial specification of L2, L3, or L4 headers
- Support for user login and password authentication via RADIUS or TACACS+ and for setting restrictions on which commands a user can execute
- Ability to block unauthorized DHCP servers and terminals with fixed IP addresses
    - Unauthorized DHCP servers and terminals with fixed IP addresses can be blocked using DHCP snooping.

(3) Guaranteed communication quality by using powerful hardware-based QoS functionality

- High-performance hardware-based QoS processing
- Precise QoS control by specification of detailed parameters (L2, L3, and L4 headers)
- Wide range of QoS control functionality

  L2-QoS (including IEEE 802.1p, bandwidth controls, priority controls, and drop controls) and IP-QoS (including Diff-Serv, bandwidth controls, priority controls, and drop controls)
- Wealth of the hierarchical shaper functionality for an integrated voice and data network

  Clear audio in which VoIP packets are preferentially transmitted.

(4) Support for 10G and 40G Ethernet

- Support for 10G and 40G Ethernet
    - The Switch can be connected to AX7800S, AX6700S, AX6600S, or AX6300S series switches to create a high-performance 10G local area network.
    - An SFP+ transceiver can be used as a 10G Ethernet transceiver, which is compatible with

both 1G and 10G Ethernet ports.

- QSFP+ is used as a transceiver for 40G Ethernet (AX3830S-44X4QW).
- Connection solutions are available at a low cost by using a directly attached cable.

(5) Stack functionality to achieve fault-tolerant switches

- ■ Highly scalable, fault-tolerant switches
  - A configuration that uses multiple switches allows uninterrupted communications even if a failure occurs in some of the switches.
  - The number of available ports can be increased by adding a switch.
- ■ Traffic relay independent of the bandwidth of a stack port
  - If a destination is a link aggregation where ports are handled by multiple member switches, data can be transferred from the link aggregation port of the member switch handling the line that has received data.
- ■ Non-stop software updates
  - Software can be updated by switching between the master switch and the backup switch, without interrupting network communication.
- ■ Cost reduction through centralized management
  - Centralized management can be achieved by operating multiple switches as one switch.

(6) Proven routing functions

- ■ Sophisticated and stable routing
  - Each model provides a site-to-site connection based on wide-area Ethernet and IP-VPN services with reliable routing based on OSPF and BGP functionality and load distribution based on multipaths.
  - Proven routing software on a par with ALAXALA's high-end models
- ■ IPv6 multicast support
  - The same peak performance for both IPv4 and IPv6
  - IPv6 routing at full-wire speed over 10G Ethernet
  - Wealth of IPv6 routing protocols (static, RIPng, OSPFv3, BGP4+, PIM-SM, PM-SSM, and MLD) for building flexible IPv6 networks of every description
  - Rich functionality including IPv4/IPv6 Dual Stack and network management for IPv6-only environments (SNMP over IPv6)
- ■ Excellent support for IPv4 routing protocols
  - Supports a wealth of proven IPv4 routing protocols

    (static, RIP, OSPF, BGP4, PIM-SM and PIM-SSM, IGMP)
- ■ Policy-based routing
  - Supports policy-based routing in which optimal routes are selected according to the status of a forwarding destination.

(7) Network partitioning support

- ■ Reduction in costs through horizontal and vertical integration of networks
  - The VRF functionality virtually handles logically divided multiple switches in one switch, thus integrating multiple networks that are normally physically divided into a single physical network.

- Implemented networks can be easily configured, operated, and managed by aggregating Layer 3 devices at a data center and locating Layer 2 devices in offices and branches.

(8) High reliability for configuring mission-critical networks

- ■ High product quality
  - High reliability assured through exacting component selection and strict design and testing standards
  - Stable routing processing based on software used successfully by carriers and ISPs
- ■ Redundant power design for high reliability as a stand-alone device
- ■ Variety of redundant network configurations
  - High-speed path switching

    Rapid Spanning Tree Protocol (IEEE 802.1w and IEEE 802.1s), GSRP#1, Autonomous Extensible Ring Protocol#2 (abbreviated hereafter to Ring Protocol), link aggregation (IEEE 802.3ad), hot standby (VRRP), static/VRRP polling#3, and other functionality
  - Load balancing

    Equal traffic balancing at the IP level based on OSPF equal-cost multipath routing

#1

Gigabit Switch Redundancy protocol. For details, see *14. Description of GSRP* in the manual *Configuration Guide Vol. 2 For Version 11.10.*

#2

For details about the Ring Protocol, see *23. Description of the Ring Protocol* in this manual.

#3

A monitoring functionality that polls a node on a specified path to check its reachability, and dynamically selects a new route in conjunction with the Virtual Router Redundancy protocol (VRRP) or static routing.

(9) High port density and compact size

- Compact 1U chassis
- Maximum of 44 10GBASE-R (SFP+) or 1000BASE-X (SFP) ports and 4 40GBASE-R (QSFP+) ports (AX3830S-44X4QW)
- Maximum of 26 1000BASE-X (SFP) ports (AX3650S-20S6XW)
- Maximum of 48 10BASE-T, 100BASE-TX, and 1000BASE-T ports (AX3650S-48T4XW)

(10) Top-class network management, maintenance, and operation

- Offers IPv4/v6 Dual Stack and full network management functionality for IPv6 environments, including SNMP over IPv6.
- In addition to the basic MIB-II, supports a wide range of MIBs including IPv6 MIB and RMON.
- Supports port mirroring to monitor and analyze traffic (through both receiving and sending ports).
- Capable of analyzing traffic characteristics using sFlow and the sFlow-MIB.
- Online maintenance

  Partial reboot when the configuration is changed ensures continuous communication.

- Support for SD memory cards
    - Users can easily back up the configuration and save error information.
    - Maintenance tasks are simplified.
- The Ethernet ports, console port, and the memory card slot are all on the front panel.
- Supports the Ethernet Connectivity Fault Management (CFM) functionality for network maintenance and management.

(11) Support for Open Autonomic Networking (OAN)#

- ■ More efficient operation and lower total cost of ownership (TCO) through IT system linkage and automated network operation and management
    - AX-Config-Master

      Automatic configuration that eliminates any need for devices to be configured individually

      Configuration consistency check over the entire network

      Security assurance when collecting or distributing device configuration information
    - AX-ON-API

      A new device control method, used instead of CLI or SNMP

      Standard IT systems technology, such as Extensible Markup Language (XML), the Simple Object Access protocol (SOAP), and Netconf, implemented in network devices for the enterprise

      Users can set the parameters for VLANs, interfaces, and link aggregation.

#

For details, see *AX-Config-Master part* in the *OAN User's Guide*.

(12) Low power consumption

- ■ Architecture design and parts selection were performed with lower power consumption in mind. This helps to reduce the total cost of ownership (TCO) after implementation.
- ■ Power saving
    - Provides power saving functionality that limits power supplied to ports, LEDs, and the Switch itself. Functionality can be selected according to the operational status of the user.
- ■ Low power consumption through scheduling
    - In accordance with scheduling settings (for example, Sundays, Saturdays, long weekends, national holidays, or nighttime), the Switch automatically limits the power supplied to ports, and the Switch itself automatically wakes up from power saving mode.
- ■ Visualization of power consumption information
    - Consumed power and total consumption can be displayed with operation commands and MIBs.

Chapter

2. Switch Configuration

This chapter describes all the Switch models, including their configurations and appearance.

2.1 Range of Switch models

This Switch is a 1U size box-type Ethernet switch. AX3830S series switches are equipped with a maximum of 44 10GBASE-R ports and a maximum of 4 40GBASE-R ports, and AX3650S series switches are equipped with a maximum of 48 10/100/1000BASE-T ports and a maximum of 6 10GBASE-R ports.

AX3800S and AX3650S series switches come with functionality such as link aggregation, VLANs, Spanning Tree Protocols, GSRP, IGMP and MLD snooping, and Layer 2 authentication. The switches support IPv4/IPv6 unicast and multicast hardware routing; routing protocols such as RIP, OSPF, and BGP4; and network partitioning. They provide advanced filters and QoS (receiving side and sending side), and support wire-rate and non-blocking switching.

The following table describes models by the maximum number of ports each provides.

Table 2-1: Switch models by maximum number of ports

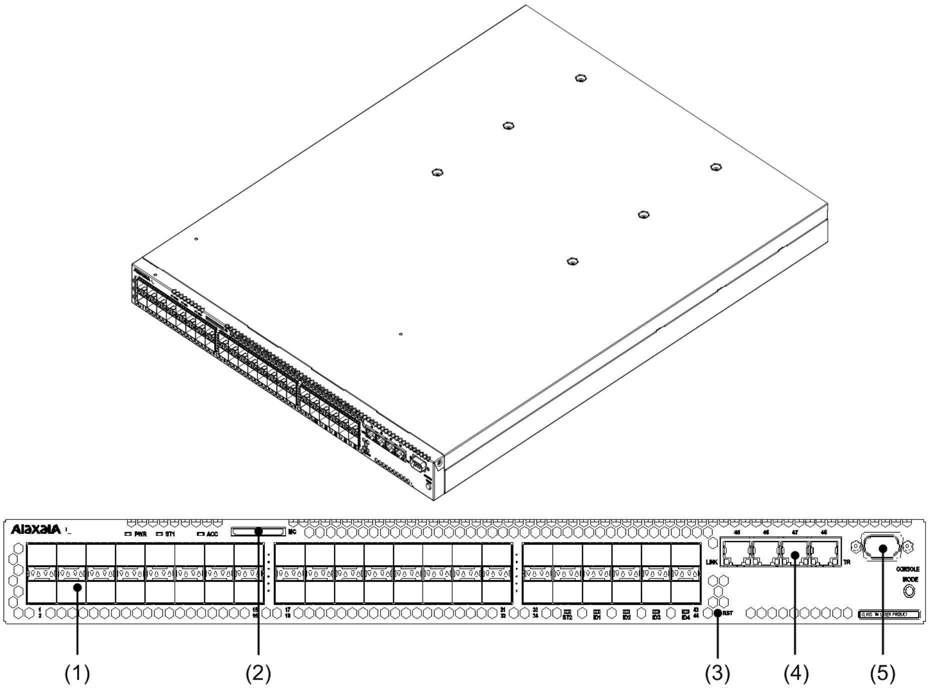
Categorized by maximum number of ports#	**Model**	**Model**
48 ports (10/100/1000BASE-T) 44 ports (1000BASE-X) 44 ports (10GBASE-R)	AX3830S	• AX3830S-44XW (redundant power model)
48 ports (10/100/1000BASE-T) 44 ports (1000BASE-X) 44 ports (10GBASE-R) 4 ports (40GBASE-R)	AX3830S	• AX3830S-44X4QW (redundant power model)
24 ports (10/100/1000BASE-T) 6 ports (1000BASE-X) 6 ports (10GBASE-R)	AX3650S	• AX3650S-24T6XW (redundant power model)
24 ports (10/100/1000BASE-T) 26 ports (1000BASE-X) 6 ports (10GBASE-R)	AX3650S	• AX3650S-20S6XW (redundant power model)
48 ports (10/100/1000BASE-T) 4 ports (1000BASE-X) 4 ports (10GBASE-R)	AX3650S	• AX3650S-48T4XW (redundant power model)

#: For details on the maximum number of ports that can be used concurrently, see *3.1 Line and module capacities*.

2.1.1 External view

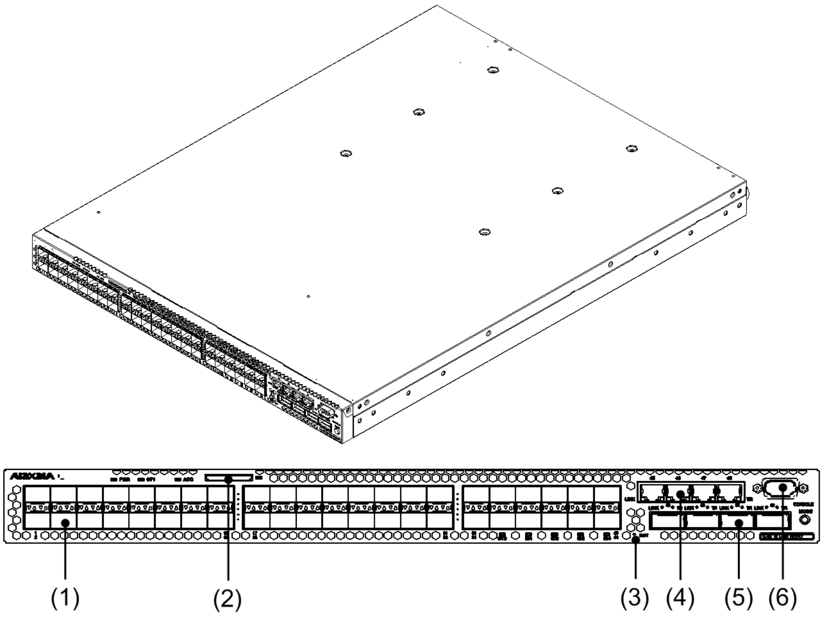
External views of the models are shown below.

Figure 2-1: AX3830S-44XW model



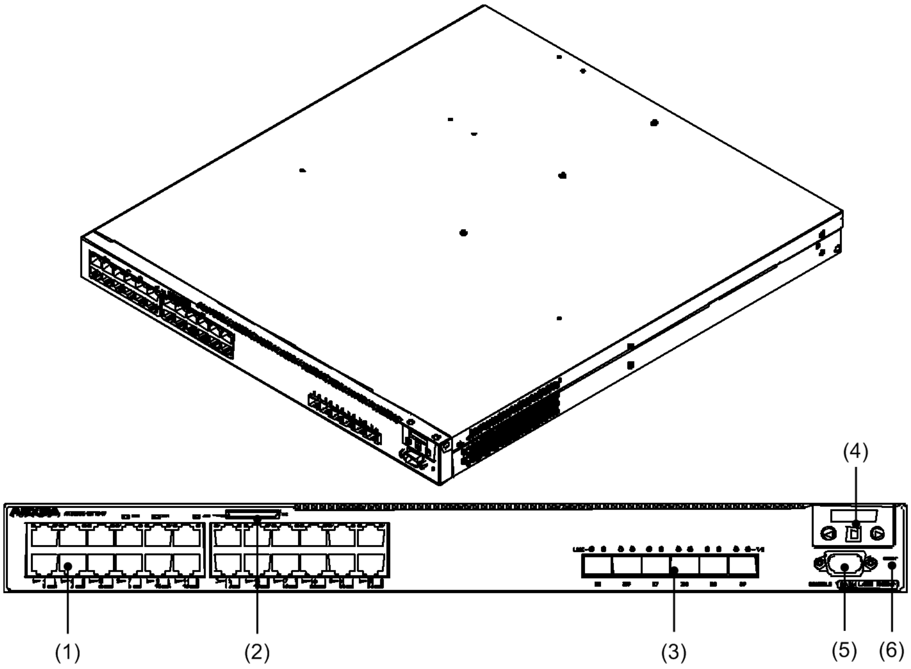
(1) SFP+ module slots
(2) Memory card slot
(3) RESET button
(4) 10/100/1000BASE-T Ethernet ports
(5) Console port

Figure 2-2: AX3830S-44X4QW model



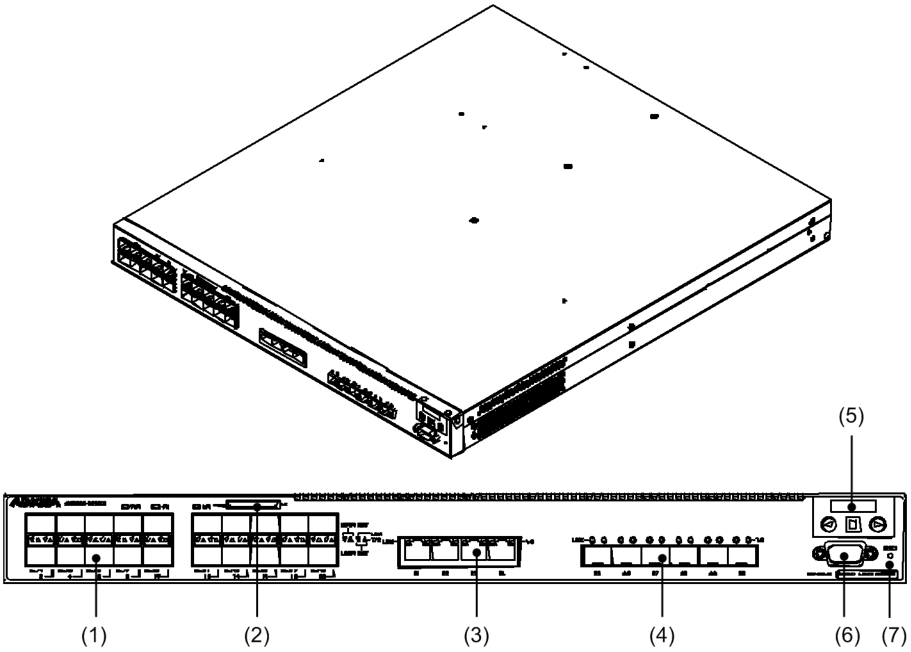
(1) SFP+ module slots
(2) Memory card slot
(3) RESET button
(4) 10/100/1000BASE-T Ethernet ports
(5) QSFP+ module slots
(6) CONSOLE port

Figure 2-3: AX3650S-24T6XW model



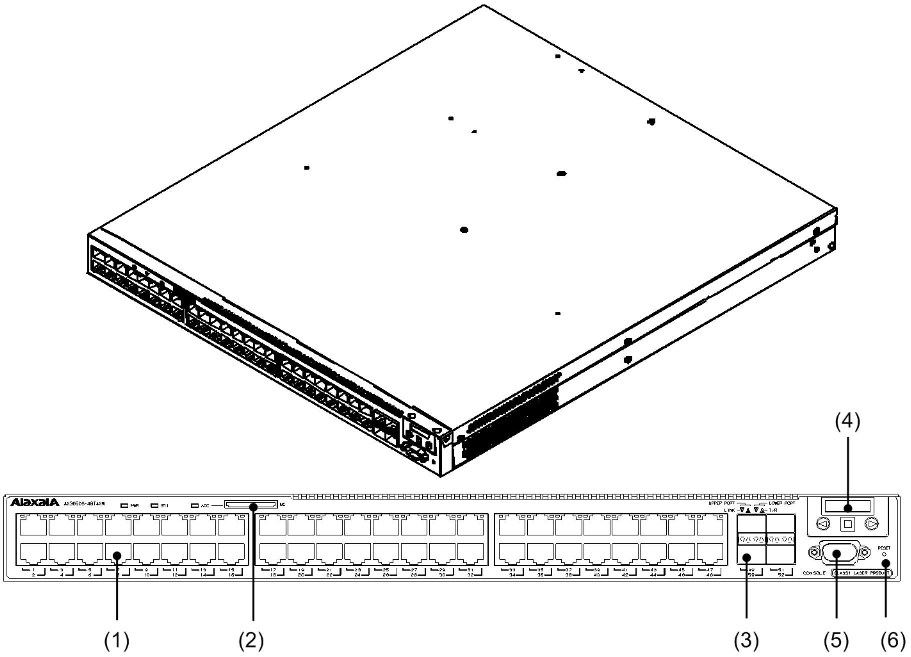
(1) 10/100/1000BASE-T Ethernet ports
(2) Memory card slot
(3) SFP+ module slots
(4) System operation panel
(5) Console port
(6) RESET button

Figure 2-4: AX3650S-20S6XW model



(1) SFP module slots
(2) Memory card slot
(3) 10/100/1000BASE-T Ethernet ports
(4) SFP+ module slots
(5) System operation panel
(6) Console port
(7) RESET button

Figure 2-5: AX3650S-48T4XW model



(1) 10/100/1000BASE-T Ethernet ports
(2) Memory card slot
(3) SFP+ module slots
(4) System operation panel
(5) Console port
(6) RESET button

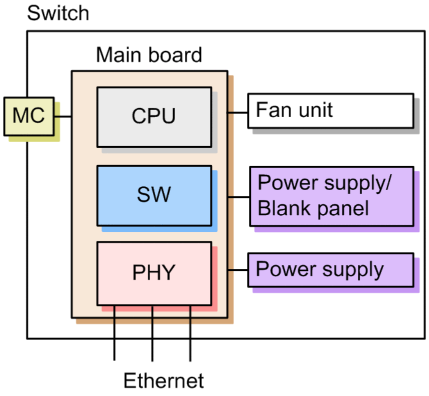
2.2 Switch components

2.2.1 Hardware for AX3830S [AX3800S]

The Switch is a redundant power model. You can configure a redundant power system by installing two PS-A03, PS-A03R, PS-D03, or PS-D03R units. In addition, either front-inlet, back-outlet or back-inlet, front-outlet air flow is possible depending on the choice of power supply unit and fan unit. For details, see the *Hardware Instruction Manual*.

The following figures show the hardware configuration.

Figure 2-6: Hardware configuration



Legend: MC: Memory Card
SW: Switch processor
PHY: Physical Interface

(1) Device chassis

The main board, power supply unit, and fan are enclosed within the device chassis. Both the power supply unit and fan unit contained within this Switch are removable.

(2) Main board

The main board consists of CPU, SW, and PHY subunits.

- CPU (central processing unit)

  Manages all the hardware, controls the SW and PHY subunits, and performs protocol processing via software.

  The software is stored in the CPU subunit's internal memory.

- MC (memory card)

  MC slot. By inserting a memory card, you can take a backup of the configuration or collect dump information.

- SW (switch processor)

  Handles L2 frame switching and L3 (IPv4 or IPv6) packet switching. The SW subunit performs hardware-based processing including MAC address learning and aging, link aggregation, routing table lookups, filter or QoS table lookups, and DMA transfers of packets addressed to the device and packets originated by the device. These functions together enable IP forwarding.

- PHY (physical Interface)

  An interface subunit supporting various kinds of media.

(3) PS-A03, PS-A03R, PS-D03, and PS-D03R

PS-A03, PS-A03R, PS-D03, and PS-D03R are power supply units that generate DC power for use within the Switch from an external power supply. Up to two power supply units can be installed, and units can be replaced without powering off the Switch when using a redundant power supply unit. When using only one power supply unit, a blank panel (BPNL-01) is inserted into the empty slot.

The Switch is equipped with a fan to cool the Switch's internal components.

(4) FAN-04 and FAN-04R

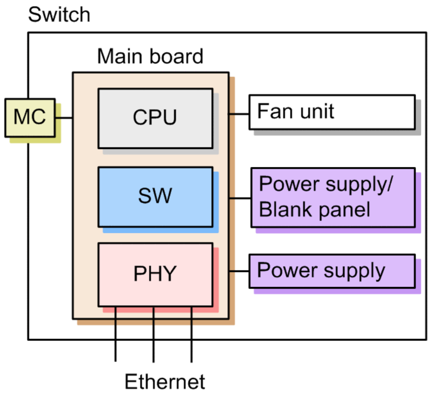
FAN-04 and FAN-04R are fan units that cool the inside of the Switch. One fan unit is inserted into the fan slot. Because a fan unit contains four fans, the Switch can be cooled normally even if one of the fans stops. The fan unit can also be replaced without powering off the Switch during operation.

2.2.2 Hardware for AX3650S [AX3650S]

The Switch is a redundant power model. You can configure a redundant power system by installing two PS-A03 or PS-D03 units. For details, see the *Hardware Instruction Manual*.

The following figures show the hardware configuration.

Figure 2-7: Hardware configuration



Legend: MC: Memory Card
SW: Switch processor
PHY: Physical Interface

(1) Device chassis

The main board, power supply unit, and fan are enclosed within the device chassis. Both the power supply unit and fan contained within this Switch are removable.

(2) Main board

The main board consists of CPU, SW, and PHY subunits.

- CPU (central processing unit)

  Manages all the hardware, controls the SW and PHY subunits, and performs protocol processing via software.

  The software is stored in the CPU subunit's internal memory.

- MC (memory card)

  MC slot. By inserting a memory card, you can take a backup of the configuration or collect dump information.

- SW (switch processor)

Handles L2 frame switching and L3 (IPv4 or IPv6) packet switching. The SW subunit performs hardware-based processing including MAC address learning and aging, link aggregation, routing table lookups, filter or QoS table lookups, and DMA transfers of packets addressed to the device and packets originated by the device. These functions together enable IP forwarding.

- PHY (Physical Interface)

  An interface subunit supporting various kinds of media. Several models are available depending on the line type and the number of ports.

(3) PS-A03/PS-D03

The PS-A03 and PS-D03 are power supply units that generate DC power for use within the Switch from an external power supply. Up to two power supply units can be installed, and units can be replaced without powering off the Switch when using a redundant power supply unit. When using only one power supply unit, a blank panel (BPNL-01) is inserted into the empty slot.

The Switch is equipped with a fan to cool the Switch's internal components.

(4) FAN-03

FAN-03 is a fan unit that cools the inside of the Switch. One fan unit is inserted into the fan slot. Because a fan unit contains four fans, the Switch can be cooled normally even if one of the fans stops. The fan unit can also be replaced without powering off the Switch during operation.

2.2.3 Software

The following table describes which model of the Switch supports which software.

Table 2-2: Which model of the Switch supports which software

Software abbreviation	Description
OS-L3SA-A/OS-L3SA	L3S advanced software VLAN, Spanning Tree Protocols, RIP, OSPF, BGP, policy-based routing, multicast, VRF, SNMP, LLDP, etc.
OS-L3SL-A/OS-L3SL	L3 light software VLAN, Spanning Tree Protocols, RIP, multicast, SNMP, LLDP, etc. Note: No VRF, OSPF, BGP, and policy-based routing functionality

The following table describes the optional licenses of the Switch. Optional licenses are used in common by AX3800S and AX3650S series switches.

Table 2-3: Optional licenses used in the Switch

Optional license abbreviation	Description
OP-DH6R	IPv6 DHCP relay
OP-OTP	One-time password authentication
OP-VAA	Authentication VLAN

Chapter

3. Capacity Limit

This chapter describes the capacity limits for the Switch.

3.1 Line and module capacities

3.1.1 Number of lines

The following table describes the maximum number of lines that each model can handle.

Table 3-1: Maximum number of lines

Model	Ethernet					
	40GBASE-R (QSFP+)	10GBASE-R (SFP+)	1000BASE-X (SFP)	100BASE-FX (SFP)	10/100/1000 BASE-T	Stack port
AX3830S-44XW	--	44[#1]	44[#2]	--	48[#3]	2[#4]
AX3830S-44X4QW	4[#5]	44[#1]	44[#2]	--	48[#3]	2[#6]
AX3650S-24T6XW	--	6[#1]	6[#2]	--	24	2[#4]
AX3650S-20S6XW	--	6[#1]	20 + 6[#2]	20[#7]	24[#8]	2[#4]
AX3650S-48T4XW	--	4[#1]	4[#2]	--	48	2[#4]

Legend: --: Not applicable

#1

The maximum number of lines when 10GBASE-R is connected to an SFP+ slot. If using 1000BASE-X or the slot is used as stack port, subtract the number of SFP lines from this figure.

#2

The maximum number of lines when 1000BASE-X is connected to an SFP+ slot.

If using 10GBASE-R or the slot is used as stack port, subtract the number of SFP lines from this figure.

#3

The maximum number of lines when 10/100/1000BASE-T (SFP) is connected to the four UTP ports on the chassis and the SFP+ slots. If using 10GBASE-R or 1000BASE-X for an SFP+ slot, subtract the number of such lines from this figure.

The four UTP ports on the Switch support full-duplex communication only. If 10/100/1000BASE-T SFP is connected to the SFP+ slot, the port only supports 1000BASE-T.

#4

The maximum number of lines when an SFP slot is used as stack port.

#5

The maximum number of lines when 40GBASE-R is connected to a QSFP+ slot. If using as a stack port, subtract the number of SFP lines from this figure.

#6

The maximum number of lines when QSFP+ slot or SFP+ slot is used as a stack port.

#7

The maximum number of lines when 100BASE-FX is connected to an SFP slot. If using 1000BASE-X, subtract the number of SFP lines from this figure.

#8

The maximum number of lines when 10/100/1000BASE-T (SFP) is connected to the four UTP ports on the chassis and the SFP slots. If using 1000BASE-X or 100BASE-FX, subtract the number of such lines from this figure.

3.1.2 Mounted power supply unit

(1) Redundant power model

The redundant power model can handle two power supply units. If using only one power supply unit, make sure a blank panel is connected.

(a) AX3830S models

- AX3830S-44XW
- AX3830S-44X4QW

(b) AX3650S models

- AX3650S-24T6XW
- AX3650S-20S6XW
- AX3650S-48T4XW

3.1.3 Amount of installed memory

The table below describes the amount of installed memory and internal flash memory. The installed memory and internal flash memory cannot be expanded for the Switch.

Table 3-2: Amount of installed memory and internal flash memory

Item	All models
Installed memory	1024 MB
Internal flash memory capacity	512 MB

3.2 Capacity limit

3.2.1 Number of table entries

You can change the allocation pattern of table entries by selecting a mode, according to the Switch environment. The following three modes are available: IPv4 mode, IPv4/IPv6 mode, and IPv6 unicast priority mode. You can set which mode to use by executing the `swrt_table_resource` configuration command.

This subsection describes the number of table entries for each mode.

For the number of multipath route entries supported by each mode, see *Table 7-5 Multipath specifications* in the manual *Configuration Guide Vol. 3 For Version 11.10*.

(1) Number of table entries for AX3830S series switches

The following table describes the maximum number of table entries per switch in each mode.

Table 3-3: Maximum switch entries

Item		Maximum switch entries		
		IPv4 mode	**IPv4/IPv6 mode**	**IPv6 unicast priority mode**
IPv4	Unicast route	13312	8192	1024
	Multicast route	1024	256	16
	ARP#1	8190#2	5120	128
IPv6	Unicast route	--	2048	7560
	Multicast route	--	128	16
	NDP#1	--	1024	1024
L2	MAC address table	131072#3		

Legend: --: Not applicable

#1

When an extranet is used, if communication occurs on a directly connected route imported from another VRF, the ARP and NDP entries used for that communication will also be created in the VRF to which the route has been imported. As with normal ARP and NDP entries, the ARP and NDP entries created in the VRF where the route has been imported use resources equivalent to one entry. **[OS-L3SA]**

#2

When using IPv4 multicasting, the total number of ARP entries plus multicast routing entries must not exceed 8190.

#3

Registering the maximum capacity limit might not be possible due to hardware limitations.

The table below describes the maximum number of dynamic entries and the maximum number of static entries. Make sure that the total number of dynamic entries and static entries does not exceed the maximum entries supported by the Switches.

(a) IPv4 mode

The following table describes the maximum number of dynamic and static entries when using the

IPv4 mode.

Table 3-4: Maximum number of dynamic and static entries

Category	Item	Maximum switch entries	Maximum dynamic entries	Maximum static entries
IPv4	Unicast route entries	13312	13312	2048
	Multicast route entries	1024	1024	--
	ARP	8190	8190	4096

Legend: --: Not supported

(b) IPv4/IPv6 mode

The following table describes the maximum number of dynamic entries and the maximum number of static entries when using the IPv4/IPv6 mode.

Table 3-5: Maximum number of dynamic and static entries

Category	Item	Maximum switch entries	Maximum dynamic entries	Maximum static entries
IPv4	Unicast route entries	8192	8192	2048#
	Multicast route entries	256	256	--
	ARP	5120	5120	4096
IPv6	Unicast route entries	2048	2048	2048#
	Multicast route entries	128	128	--
	NDP	1024	1024	128

Legend: --: Not supported

#

Make sure that the total number of IPv4 and IPv6 entries does not exceed 2048.

(c) IPv6 unicast priority mode

The following table describes the maximum number of dynamic entries and the maximum number of static entries when using the IPv6 unicast priority mode.

Table 3-6: Maximum number of dynamic and static entries

Category	Item	Maximum switch entries	Maximum dynamic entries	Maximum static entries
IPv4	Unicast route entries	1024	1024	1024#
	Multicast route entries	16	16	--
	ARP	128	128	128
IPv6	Unicast route entries	7560	7560	2048#
	Multicast route entries	16	16	--
	NDP	1024	1024	128

Legend: --: Not supported

#

Make sure that the total number of IPv4 and IPv6 entries does not exceed 2048.

(2) Number of table entries for AX3650S series switches

The following table describes the maximum number of table entries per switch in each mode.

Table 3-7: Maximum switch entries

Item		Maximum switch entries		
		IPv4 mode	IPv4/IPv6 mode	IPv6 unicast priority mode
IPv4	Unicast route	16384	8192	1024
	Multicast route	1024	1024	16
	ARP#1	11264#2	2048	128
IPv6	Unicast route	--	4096	7680
	Multicast route	--	256	768
	NDP#1	--	2048	2048
L2	MAC address table	32768#3		

Legend: --: Not applicable

#1

When an extranet is used, if communication occurs on a directly connected route imported from another VRF, the ARP and NDP entries used for that communication will also be created in the VRF to which the route has been imported. As with ARP and NDP entries, the ARP and NDP entries created in the VRF where the route has been imported use resources equivalent to one entry. **[OS-L3SA]**

#2

When using IPv4 multicasting, the total number of ARP entries plus multicast routing entries must not exceed 11264.

#3

Registering the maximum capacity limit might not be possible due to hardware limitations.

The table below describes the maximum number of dynamic entries and the maximum number of static entries. Make sure that the total number of dynamic entries and static entries does not exceed the maximum switch entries.

(a) IPv4 mode

The following table describes the maximum number of dynamic and static entries when using the IPv4 mode.

Table 3-8: Maximum number of dynamic and static entries

Category	Item	Maximum switch entries	Maximum dynamic entries	Maximum static entries
IPv4	Unicast route entries	16384	16384	2048
	Multicast route entries	1024	1024	--

Category	Item	Maximum switch entries	Maximum dynamic entries	Maximum static entries
	ARP	11264	11264	4096

Legend: --: Not supported

(b) IPv4/IPv6 mode

The following table describes the maximum number of dynamic entries and the maximum number of static entries when using the IPv4/IPv6 mode.

Table 3-9: Maximum number of dynamic and static entries

Category	Item	Maximum switch entries	Maximum dynamic entries	Maximum static entries
IPv4	Unicast route entries	8192	8192	2048#
	Multicast route entries	1024	1024	--
	ARP	2048	2048	2048
IPv6	Unicast route entries	4096	4096	2048#
	Multicast route entries	256	256	--
	NDP	2048	2048	128

Legend: --: Not supported

#

Make sure that the total number of IPv4 and IPv6 entries does not exceed 2048.

(c) IPv6 unicast priority mode

The following table describes the maximum number of dynamic entries and the maximum number of static entries when using the IPv6 unicast priority mode.

Table 3-10: Maximum number of dynamic and static entries

Category	Item	Maximum switch entries	Maximum dynamic entries	Maximum static entries
IPv4	Unicast route entries	1024	1024	1024#
	Multicast route entries	16	16	--
	ARP	128	128	128
IPv6	Unicast route entries	7680	7680	2048#
	Multicast route entries	768	768	--
	NDP	2048	2048	128

Legend: --: Not supported

#

Make sure that the total number of IPv4 and IPv6 entries does not exceed 2048.

3.2.2 Link aggregation

The following table describes the capacity limits for link aggregation that can be configured.

Table 3-11: Capacity limits for link aggregation

Model	Maximum number of ports per channel group	Maximum number of channel groups per switch
All models	8	32 (in standalone mode)
		52 (in stack mode)

3.2.3 Layer 2 switching

(1) MAC address table

The Layer 2 switch functionality allows the MAC addresses of any connected hosts to be dynamically learned and entered in the MAC address table. This functionality also allows static MAC address entries to be entered in the MAC address table.

The following table describes the maximum number of MAC addresses that can be entered in the MAC address table.

Table 3-12: Maximum number of entries in the MAC address table

Model	Per switch	
	Maximum number of entries	Number of static entries
AX3800S models	131072#	2048
AX3650S models	32768#	

#

Registering the maximum capacity limit might not be possible due to hardware limitations.

When the number of MAC addresses exceeds the capacity limits, no new MAC addresses can be learned until previously learned entries are aged out. As a result, packets destined for unlearned MAC addresses will be flooded to all ports in that VLAN domain.

The maximum number of entries in the MAC address table cannot be changed by the configuration for the Switch.

(2) VLAN

The following table describes the number of VLANs that can be configured on a switch.

Table 3-13: Number of VLANs supported **[AX3800S]**

Model	VLANs per port	VLANs per switch	Total per-port VLANs per switch	
			In standalone mode	In stack mode
AX3830S-44XW	4094#	4094#	49152	10000
AX3830S-44X4QW			53248	10000

#: The number of VLANs that can be set is 4093 in a stack configuration.

Table 3-14: Number of VLANs supported **[AX3650S]**

Model	VLANs per port	VLANs per switch	Total per-port VLANs per switch	
			In standalone mode	In stack mode
AX3650S-24T6XW	4094#	4094#	30720	10000
AX3650S-20S6XW			30720	10000
AX3650S-48T4XW			53248	10000

#: The number of VLANs that can be set is 4093 in a stack configuration.

We recommend that you configure no more than 1024 VLANs. In a stack configuration, the recommended number of VLANs is no more than 1024 divided by the number of units that make up the stack (for a configuration of two units, the recommended number of VLANs is 512 or fewer).

The total number of VLANs across all ports on the switch is the number of VLANs configured on each port added together for all the ports on the switch. For example, in a 24-port switch, if 2000 VLANs are configured on ports 1 to 10, and one VLAN is configured on ports 11 to 24, the total per-port VLANs per switch will be 20014. If the total exceeds the capacity limit, CPU usage will increase, response to configuration commands and operation commands will be slower, and commands might fail to execute. Even in a stack configuration, the total number of VLANs per port in the switch is equal to the supported number for a single switch in the entire stack regardless of the number of units that make up the stack.

(a) Protocol VLAN

A protocol VLAN identifies protocols based on the values of the Ethernet-Type, LLC SAP, and SNAP type fields in an Ethernet frame. The following tables describe the capacity limits for configuring a protocol VLAN.

Table 3-15: Number of types of protocols for protocol VLANs

Model	Per port	Per switch
All models	16	16

Table 3-16: Number of protocol VLANs

Model	Per port	Per switch
All models	48#	48

#: The maximum protocol VLANs supported by a trunk port. A protocol port can support a maximum of 16 protocol VLANs.

(b) MAC VLAN

The following table describes the capacity limits for configuring MAC VLANs.

Table 3-17: Maximum number of MAC addresses registered in a MAC VLAN

Model	Maximum number of MAC addresses registered by the configuration	Maximum number of MAC addresses registered by Layer 2 authentication	Maximum number of MAC addresses that can be registered concurrently
AX3800S models	1024	1024	1024
AX3650S models	1024	1024	2048

When the `mac-based-vlan static-only` configuration command is set, the following capacity limits apply.

Table 3-18: Maximum number of registered MAC addresses when mac-based-vlan static-only is set

Model	Maximum number of MAC addresses registered by the configuration	Maximum number of MAC addresses registered by Layer 2 authentication
All models	1024	0

(c) VLAN tunneling

The following table describes the number of VLAN tunnels that can be configured.

Table 3-19: Maximum number of VLAN tunnels

Model	Per switch
All models	4094#

#: The number of VLANs that can be set is 4093 in a stack configuration.

(d) Tag translation

The following table describes the number of tag translation information entries that can be configured.

Table 3-20: Number of tag translation information entries

Model	Per switch
All models	768

(e) MAC addresses for each VLAN

The following table describes the total number of MAC addresses that can be configured for a VLAN interface (MAC addresses for a VLAN for Layer-3 communication) in a switch.

Table 3-21: Total number of MAC addresses set for a VLAN interface

Model	Per switch
AX3830S models	128
AX3650S models	1024

(3) Spanning Tree Protocols

The following table describes the capacity limits for each type of Spanning Tree Protocols.

The number of VLAN ports in a Spanning Tree Protocol is the total number of ports belonging to a VLAN for which the Spanning Tree Protocol is deployed. For channel groups, the number of physical ports per channel group is calculated. However, the following VLANs and ports are excluded from the number of VLAN ports.

- VLANs for which the `suspend` parameter is set by the `state` configuration command
- Ports for which VLAN tunneling is set
- Ports for which the BPDU filter functionality is not set when the BPDU guard functionality is used
- Access ports for which the PortFast functionality and BPDU filter functionality are set

Table 3-22: Capacity limits for PVST+

Model	**Compatible with Ring Protocol**	**Number of applicable VLANs**	**VLAN ports#1**
All models	No	250	256#2
	Yes	128	200#2

#1

This is the total number of ports configured in each VLAN incorporated in the Spanning Tree Protocol (the product of the VLAN count and port count).

For example, if 100 VLANs are defined and two lines participate in each VLAN, the total number of ports incorporated in the Spanning Tree Protocol will be 100 x 2 = 200.

When the Spanning Tree Protocol is used with VLAN tunneling, the access ports are not included in the number of ports.

#2

Excludes ports that have PortFast enabled.

Table 3-23: Capacity limits for Single Spanning Tree

Model	**Compatible with Ring Protocol**	**Number of applicable VLANs**	**Number of VLAN ports#1**	**VLAN ports#1 (when PVST+ is also used#2)**
All models	No	1024#3	5000	1000
	Yes	1024#3	4000	800

#1

This is the total number of ports configured in each VLAN incorporated in the Spanning Tree Protocol (the product of the VLAN count and port count).

For example, if 100 VLANs are defined and two lines participate in each VLAN, the total number of ports incorporated in the Spanning Tree Protocol will be 100 x 2 = 200.

When the Spanning Tree Protocol is used with VLAN tunneling, the access ports are not included in the number of ports.

#2

The total maximum value when PVST+ target ports are included is 1000.

#3

When used together with PVST+, the number of PVST+ target VLANs is subtracted from the value.

Table 3-24: Capacity limits for Multiple Spanning Tree

Model	Compatible with Ring Protocol	Number of applicable VLANs	Number of VLAN ports#1	Number of MST instances	Number of VLANs in each MST instance#2
All models	No	1024	5000	16	50
	Yes	1024	4000	16	50

#1

This is the total number of ports configured in each VLAN incorporated in the Spanning Tree Protocol (the product of the VLAN count and port count).

For example, if 100 VLANs are defined and two lines participate in each VLAN, the total number of ports incorporated in the Spanning Tree Protocol will be 100 x 2 = 200.

When the Spanning Tree Protocol is used with VLAN tunneling, the access ports are not included in the number of ports.

#2

Excludes MST instance 0. The number of target VLANs in MST instance 0 is 1024. You can check the numbers of target VLANs and VLAN ports by using the `show spanning-tree port-count` operation command during operation.

(4) Ring Protocol

(a) Ring Protocol

The following table describes the capacity limits for Ring Protocol.

Table 3-25: Capacity limits for Ring Protocol

Item	Per ring	Per switch
Number of rings	--	24#1
Number of VLAN mappings	--	128
Number of VLAN groups	2	48#2
Number of VLANs in a VLAN group	1023#3, #4	1023#3, #4
Number of ring ports#5	2	48#2

Legend: --: Not applicable

#1

If the Ring Protocol is used together with a Spanning Tree Protocol or with GSRP, or if the multi-fault monitoring functionality is used, the number will be 8.

#2

If the Ring Protocol is used together with a Spanning Tree Protocol or with GSRP, or if the multi-fault monitoring functionality is used, the number will be 16.

#3

The maximum recommended number of VLANs for a switch.

The control VLAN needed for each ring accounts for one VLAN, leaving a maximum of 1023 VLANS available for VLAN groups. As the number of rings increases, the number available for VLAN groups decreases.

#4

The multi-fault monitoring functionality accounts for one VLAN per ring, which reduces the maximum number of VLANs available for VLAN groups.

#5

Each channel group is counted as one port.

(b) Virtual links

The following table describes the capacity limits for virtual links.

Table 3-26: Capacity limits for virtual links

Item	Maximum number
Number of virtual link IDs per switch	1
Number of VLANs per virtual link	1
Number of ring nodes per base	2
Number of bases for virtual links in a network	250

(c) Multi-fault monitoring functionality

The following table describes the capacity limits for the multi-fault monitoring functionality.

Table 3-27: Capacity limits for the multi-fault monitoring functionality

Item	Maximum number
Number of multi-fault monitoring-enabled rings per switch	4
Multi-fault monitoring VLANs per ring	1
Number of multi-fault monitoring VLANs per switch	4

(5) IGMP snooping and MLD snooping

The following table describes the capacity limits for IGMP snooping.

Table 3-28: Capacity limits for IGMP snooping

Item	Maximum number
Number of configurable VLANs	32 **[AX3800S]** 64 **[AX3650S]**
Number of VLAN ports[#1]	512
Number of registered entries[#2, #3]	500

#1

The total number of ports in which IGMP snooping is active (sum of the ports within IGMP snooping-enabled VLANs). For example, if IGMP snooping is enabled in 16 VLANs, each of which has 10 ports, there will be 160 IGMP snooping-enabled ports.

#2

The maximum number of registered entries, including multicast addresses for control packets used by the routing protocols. Such entries are registered on receipt of a group participation request for a control packet. When a VLAN uses multiple routing protocols concurrently, the number of registered entries corresponds to the number of multicast addresses used by the control packet of the routing protocols concerned.

#3

When IGMP snooping is used with IPv4 or IPv6 multicast, this is the sum of multicast IP addresses learned by all VLANs. When IGMP snooping is not used with IPv4 or IPv6 multicast, this is the sum of the multicast MAC addresses learned by all VLANs.

The following table describes the capacity limits for MLD snooping.

Table 3-29: Capacity limits of MLD snooping

Item	Maximum number
Number of configurable VLANs	32
Number of VLAN ports#1	512
Number of registered entries#2, #3	500

#1

The total number of ports in which MLD snooping is active (sum of the ports within MLD snooping-enabled VLANs). For example, if MLD snooping is enabled in 16 VLANs, each of which has 10 ports, there will be 160 IGMP snooping-enabled ports.

#2

The maximum number of registered entries, including multicast addresses for control packets used by the routing protocols. Such entries are registered on receipt of a group participation request for a control packet. When a VLAN uses multiple routing protocols concurrently, the number of registered entries corresponds to the number of multicast addresses used by the control packet of the routing protocols concerned.

#3

When MLD snooping is not used with IPv6 multicast, this is the sum of the multicast MAC addresses learned by each VLAN. When MLD snooping is used with IPv6 multicast, this is the sum of the multicast IP addresses learned by each VLAN.

3.2.4 Filters and QoS [AX3800S]

The detection conditions for filters and QoS are set by configuration commands (`access-list` and `qos-flow-list`). The following describes filter and QoS capacity limits, given by the maximum number of entries set in an access or flow list that can be converted into the format used internally by a switch.

The Switches provide flow detection modes that are common to both filter and QoS control. Select a flow detection mode to determine resource allocation based on the filter and QoS detection conditions. Set the required mode on both the receiving and sending sides, using the appropriate configuration command below. The conditions for determining the maximum allowable flow entries differ according to the mode you select.

- Configuration command `flow detection mode`: Sets the receving-side flow detection mode.
- Configuration command `flow detection out mode`: Sets the sending-side flow detection mode.

The receiving side supports the filter and QoS functionality, and the sending side supports the filter functionality. For the number of filter entries on the receiving side, see *(1) Number of filter entries on the receiving side* or *(2) Number of QoS entries on the receiving side*, and for the number of filter entries on the sending side, see *(3) Number of filter entries on the sending side*.

(1) Number of filter entries on the receiving side

The following table describes the maximum number of filter entries on the receiving side that can be set for each switch for each receiving-side flow detection mode.

Table 3-30: Maximum number of filter entries on the receiving side

Receiving-side flow detection mode	Maximum number of filter entries on the receiving side[#1]		
	MAC conditions	IPv4 conditions	IPv6 conditions
layer3-1	512 x *n*[#2]	512 x *n*[#2]	--
layer3-2	--	1024 x *n*[#2]	--
layer3-5	--	256 x *n*[#2]	256 x *n*[#2]
layer3-6	--	256 x *n*[#2]	256 x *n*[#2]
layer3-dhcp-1	--	256	--

Legend: --: Not applicable, *n*: Number of member switches

#1

When a filter entry is added, a discard entry, which is enabled when flow is undetected, is automatically applied to the Ethernet interface or VLAN interface. This means that the full number of filter entries is not available. Count the number of available filter entries as follows:

Example 1:

Entry condition: 1 entry is set for Ethernet interface 1/0/1.

Number of entries: 2 entries (the entry to be set and the discard entry for Ethernet interface 1/0/1) are used.

Number of remaining entries: (*maximum-number-of-filter-entries-on-the-receiving-side*) - (*number-of-entries*)

Example 2:

Entry condition: 2 entries are assigned to Ethernet interface 1/0/1 and 3 entries are assigned to the VLAN10 interface.

Number of entries: 7 entries (5 entries to be set, the discard entry for Ethernet interface 1/0/1, and the discard entry for the VLAN10 interface) are used.

Number of remaining entries: (*maximum-number-of-filter-entries-on-the-receiving-side*) - (*number-of-entries*)

#2

In a stack configuration, the capacity limits increase according to the number of member switches. However, the capacity limits of the VLAN interface remain the same.

In standalone mode, *n* is 1.

(2) Number of QoS entries on the receiving side

The following table describes the maximum number of QoS entries on the receiving side that can be set for each switch in each receiving-side flow detection mode.

Table 3-31: Maximum number of QoS entries on the receiving side

Receiving-side flow detection mode	Maximum number of QoS entries on the receiving side		
	MAC conditions	IPv4 conditions	IPv6 conditions
layer3-1	128 x *n*#	128 x *n*#	--
layer3-2	--	256 x *n*#	--
layer3-5	--	128 x *n*#	128 x *n*#
layer3-6	--	128 x *n*#	128 x *n*#
layer3-dhcp-1	--	128	--

Legend: --: Not applicable, *n*: Number of member switches

#

In a stack configuration, the capacity limits increase according to the number of member switches. However, the capacity limits of the VLAN interface remain the same.

In standalone mode, *n* is 1.

(3) Number of filter entries on the sending side

The following table describes the maximum number of filter entries on the sending side that can be set for each switch in each sending-side flow detection mode.

Table 3-32: Maximum number of filter entries on the sending side

Sending-side flow detection mode	Maximum number of filter entries on the sending side#1		
	MAC conditions	IPv4 conditions	IPv6 conditions
layer3-1-out	--	1024 x *n*#2	--
layer3-2-out	256 x *n*#2	256 x *n*#2	256 x *n*#2

Legend: --: Not applicable, *n*: Number of member switches

#1

When a filter entry is added, a discard entry, which is enabled when flow is undetected, is automatically applied to the Ethernet interface or VLAN interface. This means that the full number of filter entries is not available. Count the number of available filter entries as follows:

Example 1:

Entry condition: 1 entry is set for Ethernet interface 1/0/1.

Number of entries: 2 entries (the entry to be set and the discard entry for Ethernet interface 1/0/1) are used.

Number of remaining entries: (*maximum-number-of-filter-entries-on-the-sending-side*) - (*number-of-entries*)

Example 2:

Entry condition: 2 entries are assigned to Ethernet interface 1/0/1 and 3 entries are assigned to the VLAN10 interface.

Number of entries: 7 entries (5 entries to be set, the discard entry for Ethernet interface 1/0/1, and the discard entry for the VLAN10 interface) are used.

Number of remaining entries: (*maximum-number-of-filter-entries-on-the-sending-side*) - (*number-of-entries*)

#2

In a stack configuration, the capacity limits increase according to the number of member switches. However, the capacity limits of the VLAN interface remains the same.

In standalone mode, *n* is 1.

(4) Number of TCP/UDP port number detection patterns

The table below describes the capacity limits for the TCP/UDP port number detection patterns used in filter or QoS flow detection conditions. These patterns refer to hardware resources that are used with the port settings in a flow detection condition.

Table 3-33: Capacity limits for the TCP/UDP port number detection patterns

Model	Maximum number per switch
AX3830S models	32 x *n*#

Legend: *n*: Number of member switches

#

In a stack configuration, the capacity limits increase according to the number of member switches.

The TCP/UDP port number detection patterns are used with the flow detection condition settings described in the table below. The patterns are not used only at creation of an access list (`access-list`) or QoS flow list (`qos-flow-list`). For the TCP/UDP port number detection patterns to be used, apply the created access list and QoS flow list to the interface by using the following configuration commands:

- ip access-group
- ipv6 traffic-filter
- ip qos-flow-group
- ipv6 qos-flow-group

Table 3-34: Flow detection condition parameters that use the TCP/UDP port number detection patterns

Flow detection condition parameter	Available specifications	Receiving-side flow detection mode	Sending-side flow detection mode
		All modes	All modes
Source port number	Single specification (`eq`)	--	--
	Range specification (`range`)	Y	Not applicable
Destination port number	Single specification (`eq`)	--	--
	Range specification (`range`)	Y	Not applicable

Legend:

Y: The TCP/UDP port number detection patterns are used.

--: The TCP/UDP port number detection patterns are not used.

The TCP/UDP port number detection patterns are shared in some cases for the Switch:

1. Filter entries and QoS entries are shared only if there are multiple filter or QoS entries.
2. Patterns are shared between TCP and UDP.
3. Patterns are not shared between source and destination port numbers.
4. Patterns are shared between IPv4- and IPv6-based flow detection conditions.

The following table describes some examples of using the TCP/UDP port number detection patterns.

Table 3-35: Usage examples of the TCP/UDP port number detection patterns

Pattern usage example#	Number of parameters	Display from the show system operation command (Value for Used of Resources (Used/Max))
Filter entry: • Source port range (10-30) Filter entry: • Source port range (10-40)	A different range of source port numbers is specified in the two entries. Therefore, the following two patterns are used: • Source port range (10-30) • Source port range (10-40)	2
Filter entry: • No source port number specified • Destination port range (10-20) Filter entry: • No source port number specified • Destination port range (10-20) QoS entry: • No source port number specified • Destination port range (10-20)	This is an example of the first type of shared pattern. All three entries share a pattern with the same destination port range (10-20). Therefore, the following one pattern is used: • Destination port range (10-20)	2
QoS entry: • TCP specified • Source port range (10-20) • No destination port number specified QoS entry: • UDP specified • Source port range (10-20) • No destination port number specified	This is an example of the second type of shared pattern. Both entries share a pattern with the same source port range (10-20). Therefore, the following one pattern is used: • Source port range (10-20)	1
QoS entry: • Source port range (10-20) • Destination port range (10-20)	This is an example of the third type of pattern, which is not shared. Although the same range is specified, a pattern is not shared between the source port range and the destination port range. Therefore, the following two patterns are used: • Source port range (10-20) • Destination port range (10-20)	2
QoS entry: • Source port range in an IPv4 condition (10-20) QoS entry: • Source port range in an IPv6 condition (10-20)	This is an example of the fourth type of shared pattern. Both entries share a pattern with the same source port range (10-20). Therefore, the following one pattern is used: • Source port range (10-20)	1

Note: The values in parentheses are the range of specifiable values when you specify the `eq` parameter or the `range` parameter.

3.2.5 Filters and QoS [AX3650S]

The detection conditions for filters and QoS are set by configuration commands (`access-list` and `qos-flow-list`). The following describes filter and QoS capacity limits, given by the maximum number of entries set in an access or flow list that can be converted into the format used internally by a switch.

The Switches provide flow detection modes that are common to both filter and QoS control. Select a flow detection mode to determine resource allocation based on the filter and QoS detection conditions. Use the appropriate configuration command shown below to set the required mode on both the receiving and sending sides. The conditions for determining the maximum allowable flow entries differ according to the mode you select. Set the flow entries within the range of per-interface entry limits for the particular interface and switch model you are using.

- Configuration command `flow detection mode`: Sets the receiving-side flow detection mode.
- Configuration command `flow detection out mode`: Sets the sending-side flow detection mode.

The receiving side supports the filter and QoS functionality, and the sending side supports the filter functionality. For the number of filter entries on the receiving side, see *(1) Number of filter entries on the receiving side* or *(2) Number of QoS entries on the receiving side*, and for the number of filter entries on the sending side, see *(3) Number of filter entries on the sending side*.

(1) Number of filter entries on the receiving side

(a) Mode layer3-1: Maximum number of filter entries

The following table describes the maximum number of filter entries that can be set when you select the layer3-1 flow detection mode for the receiving side.

Table 3-36: Mode layer3-1: Maximum number of filter entries

Model	**Interface type**	**Maximum number of filter entries on the receiving side#1**					
		Per interface		**Per switch**		**Per stack**	
		MAC conditions	**IPv4 conditions**	**MAC conditions**	**IPv4 conditions**	**MAC conditions**	**IPv4 conditions**
AX3650S-24T6XW AX3650S-20S6XW AX3650S-48T4XW	Ethernet	512	512	1536#2	1536#2	1536 x *n*#2, #3	1536 x *n*#2, #3
	VLAN	512	512	512	512	512	512

Legend: *n*: Number of member switches

#1

When a filter entry is added, a discard entry, which is enabled when flow is undetected, is automatically applied to the Ethernet interface or VLAN interface. This means that the full number of filter entries is not available. Count the number of available filter entries as follows:

Example 1:

Entry condition: 1 entry is set for Ethernet interface 1/0/1.

Number of entries: 2 entries (the entry to be set and the discard entry for Ethernet interface 1/0/1) are used.

Number of remaining entries: 510.

Example 2:

Entry condition: 2 entries are assigned to Ethernet interface 1/0/1 and 3 entries are assigned to Ethernet interface 1/0/2.

Number of entries: 7 entries (5 entries to be set, the discard entry for Ethernet interface 1/0/1, and the discard entry for Ethernet interface 1/0/2) are used.

Number of remaining entries: 505.

#2

Entry limits differ according to the port range. For details, see *Table 3-37: Mode layer3-1: Maximum number of filter entries (per port range)*.

#3

In a stack configuration, the capacity limits increase according to the number of member switches.

The table below describes the maximum number of filter entries that can be set per switch for each range of port numbers. When an Ethernet interface is used with the models in this table, the entry limits differ for each port range. Make sure that you set the number of entries within the given range.

Table 3-37: Mode layer3-1: Maximum number of filter entries (per port range)

Model	**Port range**	**Maximum number of filter entries on the receiving side#**	
		MAC conditions	**IPv4 conditions**
AX3650S-24T6XW	Ports 1-12	512	512
	Ports 13-24	512	512
	Ports 25-30	512	512
AX3650S-20S6XW	Ports 1-10	512	512
	Ports 11-20	512	512
	Ports 21-30	512	512
AX3650S-48T4XW	Ports 1-24	512	512
	Ports 25-48	512	512
	Ports 49-52	512	512

#

See #1 in *Table 3-36: Mode layer3-1: Maximum number of filter entries*.

(b) Mode layer3-2: Maximum number of filter entries

The following table describes the maximum number of filter entries that can be set when you select the layer3-2 flow detection mode for the receiving side.

Table 3-38: Mode layer3-2: Maximum number of filter entries

Model	Interface type	Maximum number of filter entries on the receiving side[#1]		
		Per interface	Per switch	Per stack
		IPv4 conditions	IPv4 conditions	IPv4 conditions
AX3650S-24T6XW AX3650S-20S6XW AX3650S-48T4XW	Ethernet	512	4096[#2]	4096 x *n*[#2, #3]
	VLAN	--	--	--

Legend: --: Not applicable, *n*: Number of member switches

#1

See #1 in *Table 3-36: Mode layer3-1: Maximum number of filter entries*.

#2

Entry limits differ according to the port range. For details, see *Table 3-39: Mode layer3-2: Maximum number of filter entries (per port range)*.

#3

In a stack configuration, the capacity limits increase according to the number of member switches.

The table below describes the maximum number of filter entries that can be set per switch for each range of port numbers. When an Ethernet interface is used with the models in this table, the entry limits differ for each port range. Make sure that you set the number of entries within the given range.

Table 3-39: Mode layer3-2: Maximum number of filter entries (per port range)

Model	Port range	Maximum number of filter entries on the receiving side[#]
		IPv4 conditions
AX3650S-24T6XW AX3650S-20S6XW	Ports 1-4	512
	Ports 5-8	512
	Ports 9-12	512
	Ports 13-16	512
	Ports 17-20	512
	Ports 21-24	512
	Ports 25-27	512
	Ports 28-30	512
AX3650S-48T4XW	Ports 1-8	512
	Ports 9-16	512
	Ports 17-24	512
	Ports 25-32	512

Model	Port range	Maximum number of filter entries on the receiving side#
		IPv4 conditions
	Ports 33-40	512
	Ports 41-48	512
	Ports 49, 50	512
	Ports 51, 52	512

#

See #1 in *Table 3-36: Mode layer3-1: Maximum number of filter entries*.

(c) Mode layer3-5: Maximum number of filter entries

The following table describes the maximum number of filter entries that can be set when you select the layer3-5 flow detection mode for the receiving side.

Table 3-40: Mode layer3-5: Maximum number of filter entries

Model	Interface type	Maximum number of filter entries on the receiving side#1					
		Per interface		Per switch		Per stack	
		IPv4 conditions	IPv6 conditions	IPv4 conditions	IPv6 conditions	IPv4 conditions	IPv6 conditions
AX3650S-24T6XW AX3650S-20S6XW AX3650S-48T4XW	Ethernet	512	256	2048#2	1024#2	2048 x *n* #2, #3	1024 x *n*#2, #3
	VLAN	--	--	--	--	--	--

Legend: --: Not applicable, *n*: Number of member switches

#1

See #1 in *Table 3-36: Mode layer3-1: Maximum number of filter entries*.

#2

Entry limits differ according to the port range. For details, see *Table 3-41: Mode layer3-5: Maximum number of filter entries (per port range)*.

#3

In a stack configuration, the capacity limits increase according to the number of member switches.

The table below describes the maximum number of filter entries that can be set per switch for each range of port numbers. When an Ethernet interface is used with the models in this table, the entry limits differ for each port range. Make sure that you set the number of entries within the given range.

Table 3-41: Mode layer3-5: Maximum number of filter entries (per port range)

Model	Port range	Maximum number of filter entries on the receiving side[#]	
		IPv4 conditions	IPv6 conditions
AX3650S-24T6XW	Ports 1-8	512	256
	Ports 9-16	512	256
	Ports 17-24	512	256
	Ports 25-30	512	256
AX3650S-20S6XW	Ports 1-10	512	256
	Ports 11-20	512	256
	Ports 21-24	512	256
	Ports 25-30	512	256
AX3650S-48T4XW	Ports 1-16	512	256
	Ports 17-32	512	256
	Ports 33-48	512	256
	Ports 49-52	512	256

#1

See #1 in *Table 3-36: Mode layer3-1: Maximum number of filter entries*.

(d) Mode layer3-6: Maximum number of filter entries

The following table describes the maximum number of filter entries that can be set when you select the layer3-6 flow detection mode for the receiving side.

Table 3-42: Mode layer3-6: Maximum number of filter entries

Model	Interface type	Maximum number of filter entries on the receiving side[#1]					
		Per interface		Per switch		Per stack	
		IPv4 conditions	IPv6 conditions	IPv4 conditions	IPv6 conditions	IPv4 conditions	IPv6 conditions
AX3650S-24T6XW AX3650S-20S6XW AX3650S-48T4XW	Ethernet	2048	1024	2048[#2]	1024[#2]	2048 x n[#2, #3]	1024 x n[#2, #3]
	VLAN					2048	1024

Legend: *n*: Number of member switches

#1

See #1 in *Table 3-36: Mode layer3-1: Maximum number of filter entries*.

#2

Entry limits do not differ depending on the port range.

#3

In a stack configuration, the capacity limits increase according to the number of member switches.

If a filter is set for VLAN, the number of entries that can be set for Ethernet decreases by the VLAN setting count x 2*n* entries.

(e) Mode layer3-dhcp-1: Maximum number of filter entries

The following table describes the maximum number of filter entries that can be set when you select the layer3-dhcp-1 flow detection mode for the receiving side.

Table 3-43: Mode layer3-dhcp-1: Maximum number of filter entries

Model	Interface type	Maximum number of filter entries on the receiving side[#1]	
		Per interface	Per switch
		IPv4 conditions	IPv4 conditions
AX3650S-24T6XW AX3650S-20S6XW AX3650S-48T4XW	Ethernet	512	1024[#2]
	VLAN	512	512

#1

See #1 in *Table 3-36: Mode layer3-1: Maximum number of filter entries*.

#2

Entry limits differ according to the port range. For details, see *Table 3-44: Mode layer3-dhcp-1: Maximum number of filter entries (per port range)*.

The table below describes the maximum number of filter entries that can be set per switch for each range of port numbers. When an Ethernet interface is used with the models in this table, the entry limits differ for each port range. Make sure that you set the number of entries within the given range.

Table 3-44: Mode layer3-dhcp-1: Maximum number of filter entries (per port range)

Model	Port range	Maximum number of filter entries on the receiving side[#]
		IPv4 conditions
AX3650S-24T6XW	Ports 1-24	512
	Ports 25-30	512
AX3650S-20S6XW	Ports 1-20	512
	Ports 21-30	512
AX3650S-48T4XW	Ports 1-48	512
	Ports 49-52	512

#1

See #1 in *Table 3-36: Mode layer3-1: Maximum number of filter entries*.

(2) Number of QoS entries on the receiving side

(a) Mode layer3-1: Maximum number of QoS entries

The following table describes the maximum number of QoS entries that can be set when you select the layer3-1 flow detection mode for the receiving side.

Table 3-45: Mode layer3-1: Maximum number of QoS entries

Model	Interface type	Maximum number of QoS entries on the receiving side					
		Per interface		Per switch		Per stack	
		MAC conditions	IPv4 conditions	MAC conditions	IPv4 conditions	MAC conditions	IPv4 conditions
AX3650S-24T6XW AX3650S-20S6XW AX3650S-48T4XW	Ethernet	256	256	256	256	256 x *n*#	256 x *n*#
	VLAN	256	256	256	256	256	256

Legend: *n*: Number of member switches

#

In a stack configuration, the capacity limits increase according to the number of member switches.

(b) Mode layer3-2: Maximum number of QoS entries

The following table describes the maximum number of QoS entries that can be set when you select the layer3-2 flow detection mode for the receiving side.

Table 3-46: Mode layer3-2: Maximum number of QoS entries

Model	Interface type	Maximum number of QoS entries on the receiving side		
		Per interface	Per switch	Per stack
		IPv4 conditions	IPv4 conditions	IPv4 conditions
AX3650S-24T6XW AX3650S-20S6XW AX3650S-48T4XW	Ethernet	256	1024#1	1024 x *n*#1, #2
	VLAN	--	--	--

Legend: --: Not applicable, *n*: Number of member switches

#1

Entry limits differ according to the port range. For details, see *Table 3-47: Mode layer3-2: Maximum number of QoS entries (per port range)*.

#2

In a stack configuration, the capacity limits increase according to the number of member switches.

The table below describes the maximum number of QoS entries that can be set per switch for each range of port numbers. When an Ethernet interface is used with the models in this table, the entry limits differ for each port range. Make sure that you set the number of entries within the given range.

Table 3-47: Mode layer3-2: Maximum number of QoS entries (per port range)

Model	Port range	Maximum number of QoS entries on the receiving side
		IPv4 conditions
AX3650S-24T6XW	Ports 1-8	256
	Ports 9-16	256
	Ports 17-24	256
	Ports 25-30	256
AX3650S-20S6XW	Ports 1-10	256
	Ports 11-20	256
	Ports 21-24	256
	Ports 25-30	256
AX3650S-48T4XW	Ports 1-16	256
	Ports 17-32	256
	Ports 33-48	256
	Ports 49-52	256

(c) Mode layer3-5: Maximum number of QoS entries

The following table describes the maximum number of QoS entries that can be set when you select the layer3-5 flow detection mode for the receiving side.

Table 3-48: Mode layer3-5: Maximum number of QoS entries

Model	Interface type	Maximum number of QoS entries on the receiving side					
		Per interface		Per switch		Per stack	
		IPv4 conditions	IPv6 conditions	IPv4 conditions	IPv6 conditions	IPv4 conditions	IPv6 conditions
AX3650S-24T6XW AX3650S-20S6XW AX3650S-48T4XW	Ethernet	256	256	512[#1]	512[#1]	512 x *n*[#1, #2]	512 x *n* [#1, #2]
	VLAN	--	--	--	--	--	--

Legend: --: Not applicable, *n*: Number of member switches

#1

Entry limits differ according to the port range. For details, see *Table 3-49: Mode layer3-5: Maximum number of QoS entries (per port range)*.

#2

In a stack configuration, the capacity limits increase according to the number of member switches.

The table below describes the maximum number of QoS entries that can be set per switch for each range of port numbers. When an Ethernet interface is used with the models in this table, the entry limits differ for each port range. Make sure that you set the number of entries within the given range.

Table 3-49: Mode layer3-5: Maximum number of QoS entries (per port range)

Model	Port range	Maximum number of QoS entries on the receiving side	
		IPv4 conditions	IPv6 conditions
AX3650S-24T6XW	Ports 1-24	256	256
	Ports 25-30	256	256
AX3650S-20S6XW	Ports 1-20	256	256
	Ports 21-30	256	256
AX3650S-48T4XW	Ports 1-48	256	256
	Ports 49-52	256	256

(d) Mode layer3-6: Maximum number of QoS entries

The following table describes the maximum number of QoS entries that can be set when you select the layer3-6 flow detection mode for the receiving side.

Table 3-50: Mode layer3-6: Maximum number of QoS entries

Model	Interface type	Maximum number of QoS entries on the receiving side					
		Per interface		Per switch		Per stack	
		IPv4 conditions	IPv6 conditions	IPv4 conditions	IPv6 conditions	IPv4 conditions	IPv6 conditions
AX3650S-24T6XW AX3650S-20S6XW AX3650S-48T4XW	Ethernet	512	512	512$^{\#1}$	512$^{\#1}$	512 x $n^{\#1, \#2}$	512 x $n^{\#1, \#2}$
	VLAN					512	512

Legend: *n*: Number of member switches

#1

Entry limits do not differ depending on the port range.

#2

In a stack configuration, the capacity limits increase according to the number of member switches.

If a filter is set for VLAN, the number of entries that can be set for Ethernet decreases by the VLAN setting count x 2*n* entries.

(e) Mode layer3-dhcp-1: Maximum number of QoS entries

The following table describes the maximum number of QoS entries that can be set when you select the layer3-dhcp-1 flow detection mode for the receiving side.

Table 3-51: Mode layer3-dhcp-1: Maximum number of QoS entries

Model	**Interface type**	**Maximum number of QoS entries on the receiving side**	
		Per interface	**Per switch**
		IPv4 conditions	**IPv4 conditions**
AX3650S-24T6XW AX3650S-20S6XW AX3650S-48T4XW	Ethernet	256	512#
	VLAN	256	256

#

Entry limits differ according to the port range. For details, see *Table 3-52: Mode layer3-dhcp-1: Maximum number of QoS entries (per port range)*.

The table below describes the maximum number of QoS entries that can be set per switch for each range of port numbers. When an Ethernet interface is used with the models in this table, the entry limits differ for each port range. Make sure that you set the number of entries within the given range.

Table 3-52: Mode layer3-dhcp-1: Maximum number of QoS entries (per port range)

Model	**Port range**	**Maximum number of QoS entries on the receiving side**
		IPv4 conditions
AX3650S-24T6XW	Ports 1-24	256
	Ports 25-30	256
AX3650S-20S6XW	Ports 1-20	256
	Ports 21-30	256
AX3650S-48T4XW	Ports 1-48	256
	Ports 49-52	256

(3) Number of filter entries on the sending side

(a) Mode layer3-1-out: Maximum number of filter entries

The following table describes the maximum number of filter entries that can be set when you select the layer3-1-out flow detection mode for the sending side.

Table 3-53: Mode layer3-1-out: Maximum number of filter entries

Model	**Interface type**	**Maximum number of filter entries on the sending side#1**		
		Per interface	**Per switch**	**Per stack**
		IPv4 conditions	**IPv4 conditions**	**IPv4 conditions**
AX3650S-24T6XW AX3650S-20S6XW AX3650S-48T4XW	Ethernet	256	1024#2	1024 x *n*#2, #3
	VLAN	--	--	--

Legend: --: Not applicable, *n*: Number of member switches

#1

When a filter entry is added, a discard entry, which is enabled when flow is undetected, is automatically applied to the interface. This means that the full number of filter entries is not available. Count the number of available filter entries as follows:

Example 1:

Entry condition: 1 entry is set for Ethernet interface 1/0/1.

Number of entries: 2 entries (the entry to be set and the discard entry for Ethernet interface 1/0/1) are used.

Number of remaining entries: 254

Example 2:

Entry condition: 2 entries are assigned to Ethernet interface 1/0/1 and 3 entries are assigned to Ethernet interface 1/0/2.

Number of entries: 7 entries (5 entries to be set, the discard entry for Ethernet interface 1/0/1, and the discard entry for Ethernet interface 1/0/2) are used.

Number of remaining entries: 249

#2

Entry limits differ according to the port range. For details, see *Table 3-54: Mode layer3-1-out: Maximum number of filter entries (per port range)*.

#3

In a stack configuration, the capacity limits increase according to the number of member switches.

The table below describes the maximum number of filter entries that can be set per switch for each range of port numbers. When an Ethernet interface is used with the models in this table, the entry limits differ for each port range. Make sure that you set the number of entries within the given range.

Table 3-54: Mode layer3-1-out: Maximum number of filter entries (per port range)

Model	Port range	Maximum number of filter entries on the sending side#
		IPv4 conditions
AX3650S-24T6XW	Ports 1-8	256
	Ports 9-16	256
	Ports 17-24	256
	Ports 25-30	256
AX3650S-20S6XW	Ports 1-10	256
	Ports 11-20	256
	Ports 21-24	256
	Ports 25-30	256
AX3650S-48T4XW	Ports 1-16	256
	Ports 17-32	256

Model	Port range	Maximum number of filter entries on the sending side#
		IPv4 conditions
	Ports 33-48	256
	Ports 49-52	256

#

See #1 in *Table 3-53: Mode layer3-1-out: Maximum number of filter entries*.

(b) Mode layer3-2-out: Maximum number of filter entries

The following table describes the maximum number of filter entries that can be set when you select the layer3-2-out flow detection mode for the sending side.

Table 3-55: Mode layer3-2-out: Maximum number of filter entries (1/2)

Model	Interface type	Maximum number of filter entries on the sending side#1					
		Per interface			Per switch		
		MAC conditions	IPv4 conditions	IPv6 conditions	MAC conditions	IPv4 conditions	IPv6 conditions
AX3650S-24T6XW AX3650S-20S6XW AX3650S-48T4XW	Ethernet	256	256	256	256	256	256
	VLAN	--	--	--	--	--	--

Table 3-56: Mode layer3-2-out: Maximum number of filter entries (2/2)

Model	Interface type	Maximum number of filter entries on the sending side#1		
		Per stack		
		MAC conditions	IPv4 conditions	IPv6 conditions
AX3650S-24T6XW AX3650S-20S6XW AX3650S-48T4XW	Ethernet	256 x *n*#2	256 x *n*#2	256 x *n*#2
	VLAN	--	--	--

Legend: --: Not applicable, *n*: Number of member switches

#1

See #1 in *Table 3-53: Mode layer3-1-out: Maximum number of filter entries*.

#2

In a stack configuration, the capacity limits increase according to the number of member switches.

(c) Mode layer3-3-out: Maximum number of filter entries

The following table describes the maximum number of filter entries that can be set when you select the layer3-3-out flow detection mode for the sending side.

Table 3-57: Mode layer3-3-out: Maximum number of filter entries (1/2)

Model	Interface type	Maximum number of filter entries on the sending side#					
		Per interface			Per switch		
		MAC conditions	IPv4 conditions	IPv6 conditions	MAC conditions	IPv4 conditions	IPv6 conditions
AX3650S-24T6XW AX3650S-20S6XW AX3650S-48T4XW	Ethernet	--	--	--	--	--	--
	VLAN	256	256	256	256	256	256

Table 3-58: Mode layer3-3-out: Maximum number of filter entries (2/2)

Model	Interface type	Maximum number of filter entries on the sending side#		
		Per stack		
		MAC conditions	IPv4 conditions	IPv6 conditions
AX3650S-24T6XW AX3650S-20S6XW AX3650S-48T4XW	Ethernet	--	--	--
	VLAN	256	256	256

Legend: --: Not applicable

#

See #1 in *Table 3-53: Mode layer3-1-out: Maximum number of filter entries*.

(4) Number of TCP/UDP port number detection patterns

The table below describes the capacity limits for the TCP/UDP port number detection patterns used in filter or QoS flow detection conditions. These patterns refer to hardware resources that are used with the port settings in a flow detection condition.

Table 3-59: Capacity limits for the TCP/UDP port number detection patterns

Model	Maximum number per switch
AX3650S models	64 x *n*# (Filters: 32 x *n*#, QoS: 32 x *n*#)

Legend: *n*: Number of member switches

#

In a stack configuration, the capacity limits increase according to the number of member switches.

The TCP/UDP port number detection patterns are used with the flow detection condition settings described in the table below. Patterns are not used only at creation of an access list (`access-list`) or QoS flow list (`qos-flow-list`). For the TCP/UDP port number detection patterns to be used, apply the created access list and QoS flow list to the interface by using the following configuration commands:

- ip access-group

- ipv6 traffic-filter
- ip qos-flow-group
- ipv6 qos-flow-group

Table 3-60: Flow detection condition parameters that use the TCP/UDP port number detection patterns

Flow detection condition parameter	Available specifications	Receiving-side flow detection mode	Sending-side flow detection mode
		All modes	All modes
Source port number	Single specification (`eq`)	--	--
	Range specification (`range`)	Y	Not applicable
Destination port number	Single specification (`eq`)	--	--
	Range specification (`range`)	Y	Not applicable

Legend:

Y: The TCP/UDP port number detection patterns are used.

--: The TCP/UDP port number detection patterns are not used.

The TCP/UDP port number detection patterns are shared in some cases for the Switch:

1. Filter entries and QoS entries are shared only among themselves.

   Filter and QoS entries are not shared with each other.
2. Patterns are shared between TCP and UDP.
3. Patterns are not shared between source and destination port numbers.
4. Patterns are shared between IPv4- and IPv6-based flow detection conditions.

The following table describes some examples of using the TCP/UDP port number detection patterns.

Table 3-61: Usage examples of the TCP/UDP port number detection patterns

Pattern usage example[#]	Number of parameters	Display from the show system operation command (Value for Used of Resources (Used/Max))
Filter entry: • Source port range (10-30) Filter entry: • Source port range (10-40)	A different range of source port numbers is specified in the two entries. Therefore, the following two patterns are used: • Source port range (10-30) • Source port range (10-40)	2

Pattern usage example[#]	Number of parameters	Display from the show system operation command (Value for Used of Resources (Used/Max))
Filter entry: • No source port number specified • Destination port range (10-20) Filter entry: • No source port number specified • Destination port range (10-20) QoS entry: • No source port number specified • Destination port range (10-20)	This is an example of the first type of shared pattern. Both filter entries share a pattern with the same destination port range (10-20). The pattern of destination port range (10-20) for QoS entries is not shared by filter entries. Therefore, the following two patterns are used: • Destination port range (10-20) for filter entries • Destination port range (10-20) for QoS entries	2
QoS entry: • TCP specified • Source port range (10-20) • No destination port number specified QoS entry: • UDP specified • Source port range (10-20) • No destination port number specified	This is an example of the second type of shared pattern. Both entries share a pattern with the same source port range (10-20). Therefore, the following one pattern is used: • Source port range (10-20)	1
QoS entry: • Source port range (10-20) • Destination port range (10-20)	This is an example of the third type of pattern, which is not shared. Although the same range is specified, a pattern is not shared between the source port range and the destination port range. Therefore, the following two patterns are used: • Source port range (10-20) • Destination port range (10-20)	2
QoS entry: • Source port range in an IPv4 condition (10-20) QoS entry: • Source port range in an IPv6 condition (10-20)	This is an example of the fourth type of shared pattern. Both entries share a pattern with the same source port range (10-20). Therefore, the following one pattern is used: • Source port range (10-20)	1

Note: The values in parentheses are the range of specifiable values when you specify the `eq` parameter or the `range` parameter.

3.2.6 Layer 2 authentication

(1) IEEE 802.1X

The following describes the capacity limits for IEEE 802.1X.

IEEE 802.1X of the Switch supports the following three authentication modes:

- Port-based authentication
- VLAN-based authentication (static)
- VLAN-based authentication (dynamic)

The following table describes the total number of IEEE 802.1X-enabled ports per switch when using VLAN-based authentication:

Table 3-62: Total number of IEEE 802.1X-enabled ports per switch

Model	Total number of IEEE 802.1X-enabled ports per switch#
All models	1024

#

The total number of IEEE 802.1X-enabled ports per switch is the maximum value of the sum of the VLAN ports in all VLANs for which VLAN-based authentication has been set. When a VLAN includes one or more channel groups, a channel group is counted as one port regardless of the number of physical ports in the channel group. Also, a port is counted for each of the tagged VLANs configured on the port. For example, when 10 VLANs are multiplexed to a single port using tags, a total of 10 ports are counted when VLAN-based authentication is enabled on those 10 VLANs.

The following table describes the maximum number of authenticated terminals for each authentication mode.

Table 3-63: Maximum number of authenticated terminals per authentication mode

Model	Authentication mode		
	Port-based authentication	VLAN-based authentication (static)	VLAN-based authentication (dynamic)
All models	64/port	256/VLAN	1024#/switch

#

When IEEE 802.1X authentication (VLAN-based (dynamic)) and Web authentication (dynamic VLAN mode) are both enabled, the total authenticated terminals allowed for the both authentication modes is 1024 per switch.

The following table describes the maximum number of authenticated terminals for the Switch.

Table 3-64: Maximum number of authenticated terminals for the Switch

Model	Maximum number of authenticated terminals summed over three modes
All models	1024#/switch

#

When IEEE 802.1X authentication (port-based and VLAN-based (static)), Web authentication (fixed VLAN mode), and MAC-based authentication are all enabled, the total authenticated terminals allowed among all the authentication modes is 1024 per switch.

(2) Web authentication

The following table describes the capacity limits for Web authentication.

Table 3-65: Capacity limits per switch for Web authentication

Item		Maximum number
Maximum number of authentications	Fixed VLAN mode	1024#1
	Dynamic VLAN mode	1024#2

Item		Maximum number
	Legacy mode	1024#3
Registered users in the internal Web authentication DB		300#4
Total size of files that can be specified in authentication page switching		1024 KB
Files that can be specified in authentication page switching		100
IPv4 access lists that can be set for unauthenticated terminals		1
Filter conditions that can be specified for the IPv4 access lists for unauthenticated terminals		20

#1

When Web authentication (fixed VLAN mode), IEEE 802.1X authentication (port-based and VLAN-based (static)), and MAC-based authentication are all enabled, the total authenticated terminals allowed among all the authentication modes is 1024 per switch.

#2

Web authentication (dynamic VLAN mode), MAC-based authentication (dynamic VLAN mode), and IEEE 802.1X authentication (VLAN-based (dynamic)) are all enabled, the total authenticated terminals allowed among all the authentication modes is 1024 per switch.

#3

When Web authentication (Legacy mode) and IEEE 802.1X authentication (VLAN-based (dynamic)) are both enabled, the total authenticated terminals allowed among all the authentication modes is 1024 per switch.

#4

When a user ID registered in the internal Web authentication DB is used on more than one terminal, terminals up to the maximum number of terminal authentications can be authenticated. If the number of user IDs that will need to be authenticated is greater than the maximum number of entries in the Web authentication DB, authenticate users remotely using a RADIUS server rather than the internal Web authentication DB.

(3) MAC-based authentication

The following table describes the capacity limits for MAC-based authentication.

Table 3-66: Capacity limits per switch for MAC-based authentication

Item		Maximum number
Maximum number of authentications	Fixed VLAN mode	1024#1
	Dynamic VLAN mode	1024#2
Number of users to be registered in the internal MAC-based authentication DB		1024

#1

When MAC-based authentication (fixed VLAN mode), IEEE 802.1X authentication (port-based and VLAN-based (static)), and Web authentication (fixed VLAN mode) are all enabled, the total authenticated terminals allowed among all the authentication modes is 1024.

#2

When MAC-based authentication (dynamic VLAN mode), Web authentication (dynamic VLAN mode), and IEEE 802.1X authentication (VLAN-based (dynamic)) are all enabled, the total authenticated terminals allowed among all the authentication modes is 1024 per switch.

(4) Authentication VLAN

The following table describes the capacity limits for configuring authentication VLANs.

Table 3-67: Capacity limits for authentication VLANs

Item	Maximum number
Maximum number of authenticated terminals per switch	1024
Number of VLANaccessAgents that can be configured per switch	10
Number of authenticated VLANs that can be configured per switch	4093

3.2.7 DHCP snooping

The following table describes the capacity limits for DHCP snooping for each model.

(1) AX3800S

Table 3-68: Maximum number of DHCP snooping entries

Receiving-side flow detection mode	Number of binding database entries[#1]		Number of terminal filter entries[#2]
	Total number of dynamic/static	Static	
layer3-dhcp-1	1022	256	1022
Other	1022	256	0

#1

Each terminal connected to an untrusted port takes up one entry.

#2

Each port belonging to a binding database entry takes up one entry.

For channel groups, the number of ports per channel group is calculated.

Table 3-69: Maximum number of VLANs for DHCP snooping

Model	Maximum number of VLANs
All models	1024

(2) AX3650S

Table 3-70: Maximum number of DHCP snooping entries (per switch)

Receiving-side flow detection mode	Model	Number of binding database entries[#1]		Number of terminal filter entries[#2]
		Total number of dynamic/ static	Static	
layer3-dhcp-1	All models	3070	256	3070

Receiving-side flow detection mode	Model	Number of binding database entries[#1]		Number of terminal filter entries[#2]
		Total number of dynamic/ static	Static	
Other	All models	3070	256	0

#1

Each terminal connected to an untrusted port takes up one entry.

#2

Each port belonging to a binding database entry takes up one entry.

For channel groups, the number of ports per channel group is calculated.

Table 3-71: Maximum number of DHCP snooping entries (per port range)

Receiving-side flow detection mode	Model	Port range	Number of terminal filter entries
layer3-dhcp-1	AX3650S-24T6XW AX3650S-20S6XW	Ports 1-30	3070
	AX3650S-48T4XW	Ports 1-52	3070

Table 3-72: Maximum number of VLANs for DHCP snooping

Model	Maximum number of VLANs
All models	1024

3.2.8 High reliability function based on redundant configurations

(1) GSRP

The following table describes the capacity limits for GSRP. When using Layer 3 redundancy switching, the total number of VLAN ports must not exceed 5000.

Table 3-73: Capacity limits for GSRP

Model	Maximum number of VLAN groups	Maximum number of VLANs per VLAN group
All models	64	1024

(2) VRRP

The following table describes the capacity limits for VRRP.

Table 3-74: Capacity limits for VRRP

Model	Maximum number of virtual routers		Maximum number of fault monitoring interfaces and VRRP polling instances	
	Per interface	Per switch	Per virtual router	Per switch
All models	255[#1]	255[#1]	16[#2]	255[#2]

#1: Total IPv4 and IPv6 virtual routers

#2: Sum of fault-monitoring interfaces and VRRP pollings

(3) Uplink redundancy

The following table describes the capacity limits for uplink redundancy.

Table 3-75: Capacity limits for uplink redundancy

Model	Number of uplink ports	Number of interfaces allowed per uplink port
All models	25	2

Table 3-76: Capacity limits for the MAC address update functionality

Model	Maximum number of outgoing MAC address entries
All models	3000

3.2.9 High reliability function based on network failure detection

(1) IEEE 802.3ah/UDLD

Operation on all physical ports except stack ports is enabled. In general, a single port has one connection. Therefore, even when a port receives data from multiple devices (prohibited configuration), only the data for one device will be stored. The following table describes the capacity limits for IEEE 802.3ah/UDLD.

Table 3-77: Maximum number of link monitoring information items

Model	Maximum number of link monitoring information items
All models	Maximum number of physical ports, except stack ports, for the switch

(2) L2 loop detection

The following table describes the transmission rates of L2 loop detection frames.

Table 3-78: L2 loop detection frame transmission rate

Model	L2 loop detection frame transmission rate (per switch)#1	
	When using Spanning Tree Protocols, GSRP, or Ring Protocol	When not using Spanning Tree Protocols, GSRP, or Ring Protocol
All models	30 pps (recommended)#2	200 pps (maximum)#3

- Formula for calculating L2 loop detection frame transmission rate:

  number-of-VLAN-ports-subject-to-L2-loop-detection / frame-transmission-rate-(pps) ≤ *sending-interval-(sec.)*

#1

The transmission rate is automatically adjusted to within 200 pps in accordance with the above equation.

#2

When using either Spanning Tree Protocols, GSRP, or Ring Protocol, set the transmission rate to no more than 30 pps. If the transmission rate is any higher, normal operation of the functionality is not guaranteed.

#3

Frames that exceed 200 pps will not be sent. Loop failures cannot be detected on target ports or VLANs from which frames have not been sent. Make sure that you set the sending interval to achieve a transmission rate of no more than 200 pps.

(3) CFM

The following table describes the capacity limits for CFM.

Table 3-79: Capacity limits for CFM

Model	Number of domains	Number of MAs	Number of MEPs	Number of MIPs	Total number of CFM ports#1, #2	Total number of remote MEPs#2, #3
All models	8/switch	32/switch	32/switch	32/switch	256/switch	2016/switch

#1

Total number of CFM ports is the total number of VLAN ports that send CFM frames in the primary VLAN associated with the MA.

When the MA contains only Down MEPs:

Total number of VLAN ports in Down MEP

When the MA contains both Down and Up MEPs:

Total number of VLAN ports on the primary VLAN

You can check the total number of CFM ports using the `show cfm summary` operation command.

#2

The total number of CFM ports and total number of remote MEPs are governed by the capacity limits when using the default CCM sending interval. The capacity limits of the total number of CFM ports and total number of remote MEPs change if you change the CCM sending interval. The following table describes the capacity limits for total CFM ports and total remote MEPs according to the set CCM sending interval.

Table 3-80: Capacity limits based on CCM sending interval

Model	Interval for sending CCMs	Total number of CFM ports	Total number of remote MEPs
All models	1 minute or longer	256/switch	2016/switch
	10 seconds	128/switch	2016/switch
	1 second	50/switch	200/switch

#3

Total number of remote MEPs is the sum of MEPs on other devices. This affects the CCM receiving performance from MEPs. You can check the total number of remote MEPs using the `show cfm remote-mep` operation command.

Table 3-81: Capacity limits for CFM physical ports and channel groups

Model	Total number of physical ports and channel groups to which MEPs or MIPs can be assigned#
All models	8/switch

#

Multiple MEPs or MIPs can be assigned to the same port. Each channel group is counted as one port.

Table 3-82: Capacity limits for the CFM database

Model	Number of MEP CCM database entries	Number of MIP CCM database entries	Number of linktrace database entries#
All models	63/MEP	2048/switch	1024/switch

#

If information for 256 devices is stored per route, the database can store information for a maximum of four routes (1024 / 256 devices = 4 routes).

3.2.10 Managing information about neighboring devices (LLDP/OADP)

The following table describes the capacity limits for storing neighboring device information (LLDP/OADP).

Table 3-83: Capacity limits for storing neighboring device information (LLDP/OADP)

Item	Maximum capacity
LLDP neighboring device information	52
OADP neighboring devices information	100

3.2.11 Forwarding IPv4 and IPv6 packets

In the Switch, you can assign IP addresses to VLANs. This section describes the maximum number of VLAN interfaces to which IP addresses can be assigned, the maximum number of assignable IP addresses, and the maximum number of remote devices that the Switch can communicate with. The capacity limits for DHCP relay and DHCP servers are also described.

(1) Number of interfaces to which IP addresses can be assigned

The table below describes the maximum number of interfaces supported by the Switch. This value is the total number of interfaces to which IPv4 addresses and IPv6 addresses can be assigned. IPv4 and IPv6 addresses can be configured on the same interface as well as separately on different interfaces.

Table 3-84: Maximum number of interfaces

Model	Number of interfaces (per switch)
All models	1024

(2) Maximum number of multihomed subnets

In a LAN multihomed connection, multiple IPv4 or IPv6 addresses are assigned to the same interface.

(a) For IPv4

The following table describes the maximum number of multihomed subnets for IPv4.

Table 3-85: Maximum number of multihomed subnets (for IPv4)

Model	Number of multihomed subnets (per interface)
All models	256

(b) For IPv6

The table below describes the maximum number of multihomed subnets for IPv6. This maximum includes the number of link-local addresses. An interface must always be assigned one link-local address. Therefore, if only IPv6 global addresses are assigned to all interfaces, the actual number of IPv6 addresses assigned on the switch will be 8, which is the sum of the value given in the table plus one automatically generated IPv6 link-local address.

Table 3-86: Maximum number of multihomed subnets (for IPv6)

Model	Number of multihomed subnets (per interface)
All models	7

(3) Maximum number of IP addresses

(a) IPv4 address

The table below describes the maximum number of IPv4 addresses that can be set per switch by the configuration. This value is the number of IPv4 addresses that can be configured for a communication interface.

Table 3-87: Maximum number of IPv4 addresses that can be assigned per switch by the configuration

Model	Number of IPv4 addresses (per switch)
All models	1024#

#: In IPv6 unicast priority mode, the maximum is 128 addresses.

(b) IPv6 address

The table below describes the maximum number of IPv6 addresses that can be set per switch by the configuration. This value is the number of IPv6 addresses that can be configured for a communication interface. This value also includes the number of IPv6 link-local addresses. An interface must always be assigned one IPv6 link-local address. Therefore, if IPv6 global addresses are assigned to all interfaces, an IPv6 link-local address will be automatically assigned to each interface. As a result, the actual number of IPv6 addresses that can be set per switch is as shown in *Table 3-89: Relationship between the number of IPv6 addresses that can be set by the configuration and the number of IPv6 addresses actually assigned to the switch*.

Table 3-88: Maximum number of IPv6 addresses that can be assigned per switch by the configuration

Model	Number of IPv6 addresses (per switch)
All models	128

Table 3-89: Relationship between the number of IPv6 addresses that can be set by the configuration and the number of IPv6 addresses actually assigned to the switch

Number of IPv6 addresses assigned by the configuration		Total number of IPv6 addresses set by the configuration	Number of automatically assigned IPv6 link-local addresses	Number of IPv6 addresses assigned to the switch
IPv6 link-local address	IPv6 global addresses			
128 (128 x 1)	0	128	0	128

Number of IPv6 addresses assigned by the configuration		Total number of IPv6 addresses set by the configuration	Number of automatically assigned IPv6 link-local addresses	Number of IPv6 addresses assigned to the switch
IPv6 link-local address	IPv6 global addresses			
0	128 (128 x 1)	128	128	256

Note: Meaning of the numbers in parentheses:

In the format (*A* x *B*), *A* is the number of interfaces, and *B* is the number of addresses assigned to each interface.

(4) Maximum number of remote devices

The following describes the maximum number of remote devices that the Switch can communicate with over a connected LAN. Remote devices here include terminals as well as routers.

(a) Number of ARP entries

For IPv4, the hardware address corresponding to the destination address of the packet to be sent is determined by ARP in the LAN. Thus, the number of ARP entries determines the maximum number of remote devices for an IPv4 LAN. For the maximum number of ARP entries supported by the Switch, see *3.2.1 Number of table entries*.

(b) Number of NDP entries

For IPv6, the hardware address corresponding to the destination address of the packet to be sent is determined by NDP address resolution in the LAN. Thus, the number of NDP entries determines the maximum number of remote devices. For the maximum number of NDP entries supported by the Switch, see *3.2.1 Number of table entries*.

(c) Maximum number of RA terminals

Using RA, terminals generate addresses based on the IPv6 address information received from the router. The following table describes the maximum number of RA terminals supported by the Switch.

Table 3-90: Maximum number of RA terminals

Model	Maximum number of RA terminals	
	Per interface	Per switch
All models	128	128

(5) Policy-based routing (IPv4) [OS-L3SA]

(a) Capacity limits for policy-based routing

Policy-based routing uses the filter functionality's flow detection to detect target flows for policy-based routing. Note that policy-based routing can be used when the flow detection mode of the receiving side is layer3-6.

The following table describes the number of entries for policy-based routing group per switch.

Table 3-91: Number of entries for policy-based routing group per switch

Item	IPv4 Policy-based routing group
Number of access list entries	For AX3800S series switches: See *Table 3-30: Maximum number of filter entries on the receiving side*#1. For AX3650S series switches: See *Table 3-42: Mode layer3-6: Maximum number of filter entries*#2.
Number of policy-based routing lists	256#3
Number of routes that can be set for policy-based routing list information	8
Number of routes that can be linked with the tracking functionality of policy-based routing	1024#4

#1

The number of entries is calculated by the same method as described in *3.2.4 Filters and QoS [AX3800S]*.

#2

The number of entries is calculated by the same method as described in *3.2.5 Filters and QoS [AX3650S]*.

#3

Each item of policy-based routing list information is registered as one list. Therefore, if the same policy-based routing list information is set for multiple access lists, the number of lists used is counted as 1.

#4

Each track ID is registered as one entry. Therefore, if the same track ID is set for multiple routes, the number of entries used is counted as 1.

(b) Capacity limits for tracking functionality

The following table describes the capacity limits for the tracking functionality of policy-based routing.

Table 3-92: Capacity limits for tracking functionality

Item	Capacity limits
Number of tracks	1024
Number of polling monitoring tracks#	1024

#: The number of tracks for which the `type icmp` configuration command is set.

(6) DHCP and BOOTP relays

The following table describes the number of interfaces and relay destination addresses that can be configured for DHCP and BOOTP relays.

Table 3-93: Capacity limits for DHCP and BOOTP relays

Item	Maximum number
Number of DHCP and BOOTP relay interfaces	1023

Item	Maximum number
Number of DHCP and BOOTP relay destination addresses (per global network and per VRF)	16
Number of DHCP and BOOTP relay destination addresses per switch when a VRF is used.	256

(7) IPv6 DHCP relays

The following table describes the capacity limits for IPv6 DHCP relays.

Table 3-94: Capacity limits for IPv6 DHCP relay

Item	Maximum number per switch
Number of distributed prefixes#	1024
Number of interfaces	127

#

The number of PD prefixes distributed by the IPv6 DHCP server when clients are connected directly to a switch. Packets sent through other relays and information other than PD prefixes can be relayed regardless of this condition.

(8) DHCP server

The following table describes the number of interfaces and distributable IP addresses that can be configured for the DHCP server.

Table 3-95: Capacity limits for the DHCP server

Item	Maximum number per switch
Number of DHCP server interfaces	1024
Number of subnets managed by the DHCP server	1024
Number of distributable IP addresses#1	2000
Number of distributable fixed IP addresses	160
Number of IP address ranges that are excluded from distribution#2	4096

#1: Includes the number of distributable fixed IP addresses.

#2: Up to 1024 per subnet

(9) IPv6 DHCP servers

The following table describes the number of interfaces and distributable IP addresses that can be configured for the IPv6 DHCP server.

Table 3-96: Capacity limits for the IPv6 DHCP server

Item	Maximum number per switch
Number of interfaces	128
Maximum number of distributable prefixes	1024

3.2.12 IPv4 and IPv6 routing protocols

(1) Maximum number of neighboring routers

The following table describes the maximum number of neighboring routers.

Table 3-97: Maximum number of neighboring routers

Routing protocol	Maximum number of neighboring routers	
	The tracking functionality of policy-based routing is not used	The tracking functionality of policy-based routing is used
Static routing (total of IPv4 and IPv6)	128#	128#
Sum of RIP, OSPF, BGP4, RIPng, OSPFv3, and BGP4+	50	25

#

The number of neighboring routers that can be monitored by the dynamic monitoring functionality is limited by the polling interval. For details, see the following table.

Table 3-98: Maximum number of neighboring routers that support the dynamic monitoring functionality for static routes

Polling interval	Maximum number of neighboring routers that support the dynamic monitoring functionality
1 second	60
2 seconds	120
3 seconds	128

The following table describes the maximum number of neighboring routers for each routing protocol.

Table 3-99: Definition of "maximum number of neighboring routers"

Routing protocol	Definition
Static routing	Number of next hop addresses
RIP	Number of interfaces on which RIP operates
RIPng	Number of interfaces on which RIPng operates
OSPF	Sum of routers on each interface on which OSPF operates 1. If the interface is the designated router or designated backup router: The number of other OSPF routers connected to the interface 2. If the interface is not the designated router or designated backup router: The number of designated routers and designated backup routers connected to the interface These two conditions effectively mean the number of neighboring routers in `Full` status displayed by the `show ip ospf neighbor` operation command.

Routing protocol	Definition
OSPFv3	Sum of routers on each interface on which OSPFv3 operates 1. If the interface is the designated router or designated backup router: The number of other OSPFv3 routers connected to the interface 2. If the interface is not the designated router or designated backup router: The number of designated routers and designated backup routers connected to the interface These two conditions effectively mean the number of neighboring routers in `Full` status displayed by the `show ipv6 ospf neighbor` operation command.
BGP4	Number of BGP4 peers
BGP4+	Number of BGP4+ peers

(2) Relationship between the number of route entries and the maximum number of neighboring routers

The following three tables describe the relationship between the maximum number of route entries and the maximum number of neighboring routers for IPv4 mode, IPv4/IPv6 mode, and IPv6 unicast priority mode.

Table 3-100: Relationship between the number of route entries and the maximum neighboring routers (RIP, OSPF, and BGP4) in IPv4 mode

Routing protocol	Maximum number of route entries[#1]	Maximum number of neighboring routers[#2]	
		The tracking functionality of policy-based routing is not used	The tracking functionality of policy-based routing is used
RIP	1000	50	25
OSPF[#3, #4]	2000	50	25
	10000	10	5
BGP4	13312 **[AX3800S]** 16384 **[AX3650S]**	50	25

#1: The maximum number of route entries includes alternate routes.

#2: When all the routing protocols (RIP, OSPF, and BGP4) are used in conjunction, the maximum number of neighboring routers for each protocol is 1/*n*, where *n* is the number of routing protocols being used.

#3: The maximum number of OSPF route entries is equivalent to the number of LSAs.

#4: If OSPF is used on VRFs, the maximum number of neighboring routers in the switch is 50. Make sure that the total number of neighboring routers (calculated by multiplying the number of LSAs in each VRF by the number of neighboring routers) does not exceed 100000.

Table 3-101: Relationship between the number of route entries and the maximum neighboring routers (RIP/RIPng, OSPF/OSPFv3, and BGP4/BGP4+) in IPv4/IPv6 mode

Routing protocol	**Maximum number of route entries**[#1]	**Maximum number of neighboring routers**[#2]	
		The tracking functionality of policy-based routing is not used	**The tracking functionality of policy-based routing is used**
RIP	1000	50	25
RIPng	1000	50	25
OSPF[#3, #4]	2000	50	25
	8000	12	6
OSPFv3[#3, #5]	1000	50	25
	2000	25	13
	4000 **[AX3650S]**	12 **[AX3650S]**	6 **[AX3650S]**
BGP4	8192	50	25
BGP4+	2048 **[AX3800S]** 4096 **[AX3650S]**	50	25

#1: The maximum number of route entries includes alternate routes.

#2: When all the routing protocols (RIP, RIPng, OSPF, OSPFv3, BGP4, and BGP4+) are used in conjunction, the maximum number of neighboring routers for each protocol is 1/*n*, where *n* is the number of routing protocols being used.

#3: The maximum number of OSPF/OSPFv3 route entries is equivalent to the number of LSAs.

#4: If OSPF is used on VRFs, the maximum number of neighboring routers in the switch is 50. Make sure that the total number of neighboring routers (calculated by multiplying the number of LSAs in each VRF by the number of neighboring routers) does not exceed 100000.

#5: If OSPFv3 is used on VRFs, the maximum number of neighboring routers in the switch is 50. Make sure that the total number of neighboring routers (calculated by multiplying the number of LSAs in each VRF by the number of neighboring routers) does not exceed 50000.

Table 3-102: Relationship between the number of route entries and the maximum neighboring routers (RIP/RIPng, OSPF/OSPFv3, and BGP4/BGP4+) in IPv6 unicast priority mode

Routing protocol	**Maximum number of route entries**[#1]	**Maximum number of neighboring routers**[#2]	
		The tracking functionality of policy-based routing is not used	**The tracking functionality of policy-based routing is used**
RIP	1000	50	25
RIPng	1000	50	25
OSPF[#3]	1000	50	25

Routing protocol	Maximum number of route entries[#1]	Maximum number of neighboring routers[#2]	
		The tracking functionality of policy-based routing is not used	The tracking functionality of policy-based routing is used
OSPFv3[#3, #4]	1000	50	25
	5000	10	5
	7000	7	4
BGP4	1024	50	25
BGP4+	7560 **[AX3800S]** 7680 **[AX3650S]**	50	25

#1: The maximum number of route entries includes alternate routes.

#2: When all the routing protocols (RIP, RIPng, OSPF, OSPFv3, BGP4, and BGP4+) are used in conjunction, the maximum number of neighboring routers for each protocol is 1/*n*, where *n* is the number of routing protocols being used.

#3: The maximum number of OSPF/OSPFv3 route entries is equivalent to the number of LSAs.

#4: If OSPFv3 is used on VRFs, the maximum number of neighboring routers in the switch is 50. Make sure that the total number of neighboring routers (calculated by multiplying the number of LSAs in each VRF by the number of neighboring routers) does not exceed 50000.

(3) Maximum number of configuration settings for the Switch

The table below describes the maximum number of route configurations that can be set for each routing protocol.

The numbers shown in this table are the maximum numbers that can be specified by the configuration. Make sure to stay within all capacity limits shown in this chapter during operation.

Table 3-103: Maximum number of configurations that can be set

Category	Configuration commands	Definition of "maximum number"	Maximum number of settings
IPv4 static	ip route	Number of lines	12288
IPv6 static	ipv6 route	Number of lines	2048
IPv4 summarized route	ip summary-address	Number of lines	1024
IPv6 summarized route	ipv6 summary-address	Number of lines	1024
RIP	network	Number of lines	128
	ip rip authentication key	Number of lines	512
OSPF	area range	Number of lines	1024

Category	Configuration commands	Definition of "maximum number"	Maximum number of settings
	area virtual-link	Total number of lines for which parameters `authentication-key` and `message-digest-key` have been specified	512
	ip ospf authentication-key ip ospf message-digest-key	Total number of lines for each command	512
	network	Number of lines	256
	router ospf	Number of lines	64
BGP4	network	Number of lines	1024
OSPFv3	area range	Number of lines	1024
	ipv6 router ospf	Number of lines	64
BGP4+	network	Number of lines	1024
Route filtering	distribute-list in (RIP) distribute-list out (RIP) redistribute (RIP)	Total number of lines for each command	500
	distribute-list in (OSPF) distribute-list out (OSPF) redistribute (OSPF)	Total number of lines for each command	500
	distribute-list in (BGP4) distribute-list out (BGP4) redistribute (BGP4)	Total number of lines for each command	500
	distribute-list in (RIPng) distribute-list out (RIPng) redistribute (RIPng)	Total number of lines for each command	500
	distribute-list in (OSPFv3) distribute-list out (OSPFv3) redistribute (OSPFv3)	Total number of lines for each command	500
	distribute-list in (BGP4+) distribute-list out (BGP4+) redistribute (BGP4+)	Total number of lines for each command	500
	ip as-path access-list	Number of setting <*Id*> types	200
		Number of lines	1024
	ip community-list	Number of setting <*Id*> types	100
		Number of lines with the `standard` setting	100
		Number of lines with the `expanded` setting	100
	ip prefix-list	Number of setting <*Id*> types	1024
		Number of lines	4096
	ipv6 prefix-list	Number of setting <*Id*> types	1024

Category	Configuration commands	Definition of "maximum number"	Maximum number of settings
		Number of lines	4096
	neighbor in (BGP4) neighbor out (BGP4)	Total number of lines with the <*IPv4-Address*> setting	500
		Total number of lines with the <*Peer-Group*> setting	500
	neighbor in (BGP4+) neighbor out (BGP4+)	Total number of lines with the <*IPv6-Address*> setting	500
		Total number of lines with the <*Peer-Group*> setting	500
	route-map	Number of setting <*Id*> types	256
		Number of <*Id*> and <*Seq*> combinations	4096
	match as-path	Total number of parameters specified for each line	2048
	match community	Total number of parameters specified for each line	2048
	match interface	Total number of parameters specified for each line	2048
	match ip address match ipv6 address	Total number of parameters specified for each line	2048
	match ip route-source match ipv6 route-source	Total number of parameters specified for each line	2048
	match origin	Number of lines	2048
	match protocol	Total number of parameters specified for each line	2048
	match route-type	Number of lines	2048
	match tag	Total number of parameters specified for each line	2048
	match vrf	Total number of parameters specified for each line	1024
	set as-path prepend count set distance set local-preference set metric set metric-type set origin set tag	Number of <*Id*> and <*Seq*> combinations for `route-map` in which any one of these parameters is specified	2048
	set community	Total number of parameters specified for each line	2048
	set community-delete	Total number of parameters specified for each line	2048

3.2.13 IPv4 and IPv6 multicast routing protocols

(1) IPv4 multicasting

The table below describes the number of interfaces for which IPv4 multicasting can be specified and the number of entries in the routing tables. The Switch supports PIM-SM or PIM-SSM as IPv4 multicast routing protocols. PIM-SM and PIM-SSM can operate simultaneously.

If IPv4 multicasting is used on multiple VRFs, include the total of all VRFs and the global network within the capacity limitations.

Table 3-104: Maximum number of IPv4 multicast

Item	Maximum number
PIM-SM or PIM-SSM multicast interfaces#1	63/switch
IGMP operating interfaces	127/switch
Multicast sources	128/group
PIM-SM or PIM-SSM multicast routing information entries ((S,G) entries, (*,G) entries, and negative cache)#2 S: Source IP address G: Group address	1024/switch
Settings (source and group pairs) to enable PIM-SSM interoperability with IGMPv2/IGMPv3 (EXCLUDE mode)#3	256/switch
Record information that can be processed per report in IGMPv3#4	32 records/message 32 sources/record
IGMP subscription groups#5	256/switch
Multicast neighboring routers	64/switch
Rendezvous points	2/group
Groups that can be assigned to rendezvous points per switch	128/switch
Total number of groups that can be assigned to rendezvous points per network (VPN)	128/network (VPN) 128/switch#6
BSR candidates per network (VPN)	16/network (VPN) 32/switch#6
Static subscription groups#7	256/switch
Static rendezvous point (RP) router addresses	16/switch
IGMP subscription groups per interface#5	256/interface
Source addresses per IGMP group	128/group
VRFs to which multicast can be set	31/switch
Multicast filters for the extranet#8	64/switch
`route-map` to be used for an extranet	32/switch 32/VRF
Number of multicasting addresses of PIM-SM VRF Gateway operation#9	32/switch 32/VRF

#1

The number of interfaces adjacent to other routers in PIM-SM or PIM-SSM mode.

#2

The maximum number depends on the table entries allocation pattern. For details, see *3.2.1 Number of table entries*. When PIM-SM is used in an environment that satisfies the following conditions, the maximum number of entries is 128 even if a mode in which the maximum number of entries is 128 or more selected.

- Multicast broadband communication is used.
- The Switch acts as a first-hop router or rendezvous point.

The number of entries also depends on the number of IP interfaces (not multicast interfaces) configured in the Switch. Make sure that the total number of I/O ports per entry summed over all entries falls within the range specified in *Table 3-105: Number of multicast I/O ports per number of configured IP interfaces*.

When both IPv4 and IPv6 are enabled, the number of entries is the sum of the IPv4 and IPv6 entries.

When a port is shared by the Input and Output interfaces, the number of I/O ports in an entry is counted as 1. For example, if the input interface uses ports 1/0/1 and 1/0/2, output interface 1 uses ports 1/0/2, 1/0/3, and 1/0/4, and output interface 2 uses ports 1/0/3, 1/0/4, and 1/0/5, there will be five I/O ports for that entry.

#3

The number of source and group pairs depends on the number of interfaces and subscription groups used in the multicast. Make sure that the number of source and group pairs specified is within the range shown in *Table 3-106: Number of used interfaces and number of settings to enable PIM-SSM interoperability with IGMPv2/IGMPv3 (EXCLUDE mode)* and *Table 3-107: Total number of subscription groups and number of settings to enable PIM-SSM interoperability with IGMPv2/IGMPv3 (EXCLUDE mode)*. The number of subscription groups is sum of the dynamic and static subscription groups. If a group address subscribes to multiple interfaces, the number of subscription groups is not one but the number of the interfaces to which the group address subscribes.

#4

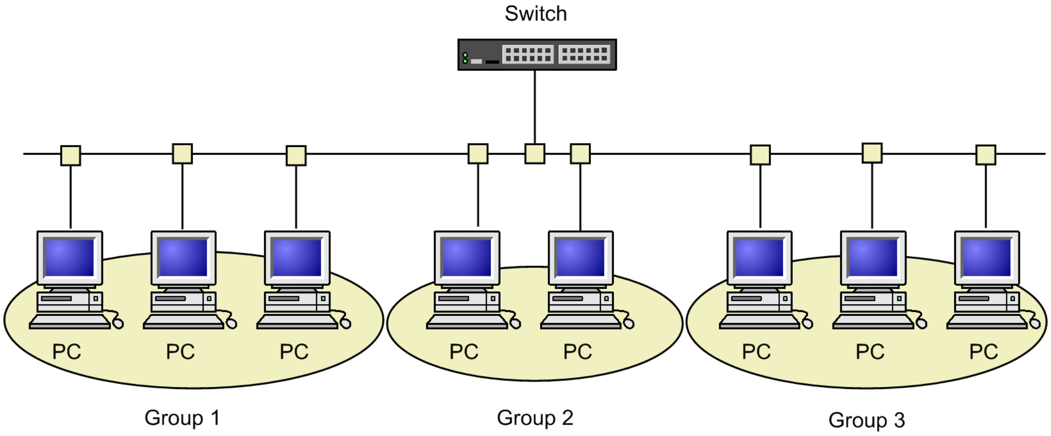
A maximum of 256 sources can be processed in a Report message. A record that does not contain source information is also counted as one source.

When PIM-SSM is configured to interoperate with IGMPv3 (EXCLUDE mode), the number of sources defined in the EXCLUDE record that matches that setting are counted. If there are multiple EXCLUDE records in the received Report message, and if more than 256 sources were added when configuring PIM-SSM interoperability with IGMPv3 (EXCLUDE mode), no multicast relay information will be created for any subsequent EXCLUDE records in that Report message that match the PIM-SSM setting.

#5

The number of groups that connect directly to the Switch. When the source is specified in IGMPv3 mode, the number of groups is the number of source-and-group combinations. For example, there are three groups in total in *Figure 3-1: Example of multicast groups*. For the number of groups that can subscribe to a single interface, see *Table 3-108: Number of possible subscription groups per interface in IPv4*.

Figure 3-1: Example of multicast groups



#6

The total number of networks (VPN) that are connected to the global network and all VRFs of this Switch.

#7

The number of static subscription groups is the total number of group addresses that statically subscribe to each multicast interface. If a group address statically subscribes to several different interfaces, the number of the static subscription groups is not one but the number of interfaces to which the group address statically subscribes. A maximum of 256 static subscription groups can be set for a single interface.

#8

The total number of addresses in the access lists (`access-list`) specified for all `route-map` instances.

#9

Uses `route-map` specified in the extranet. This applies to multicast addresses that are specified as host addresses (32-bit mask) in the access lists (`access-list`) specified for `route-map`.

The maximum number for each switch is the total number of all group addresses of the PIM-SM VRF gateways specified on VRFs.

This number is added to the number of group addresses specified as static subscription groups.

Table 3-105: Number of multicast I/O ports per number of configured IP interfaces

Number of IP interfaces set for the Switch	Number of I/O ports per entry summed for all entries
No more than 64	8191
65-128	4095
129-192	2730
193-256	2047
257-320	1638
321-384	1365
385-448	1170
449-512	1023

Number of IP interfaces set for the Switch	Number of I/O ports per entry summed for all entries
513-576	910
577-640	819
641-704	744
705-768	682
769-832	630
833-896	585
897-960	546
961-1024	511

Table 3-106: Number of used interfaces and number of settings to enable PIM-SSM interoperability with IGMPv2/IGMPv3 (EXCLUDE mode)

Number of used interfaces	Number of settings to enable PIM-SSM interoperability with IGMPv2/IGMPv3 (EXCLUDE mode)
31	256
63	128
127	64

Table 3-107: Total number of subscription groups and number of settings to enable PIM-SSM interoperability with IGMPv2/IGMPv3 (EXCLUDE mode)

Total number of subscription groups	Number of settings to enable PIM-SSM interoperability with IGMPv2/IGMPv3 (EXCLUDE mode)
64	256
128	128
256	64
512	32
1024	16
2048	8
4096	4
8128	2

Table 3-108: Number of possible subscription groups per interface in IPv4

Number of used interfaces	Possible number of subscription groups per interface
31	256
63	128
127	64

(2) IPv6 multicasting

The table below describes the number of interfaces for which IPv6 multicasting can be specified and the number of entries in the routing tables. The Switch supports PIM-SM and PIM-SSM as IPv6 multicast routing protocols. PIM-SM and PIM-SSM can operate simultaneously.

If IPv6 multicasting is used on multiple VRFs, include the total of all VRFs and the global network within the capacity limitations.

Table 3-109: Maximum number of IPv6 multicast entries

Item	**Maximum number**	
	AX3830S	**AX3650S**
PIM-SM or PIM-SSM multicast interfaces#1	63/switch	63/switch
MLD operating interfaces	127/switch	127/switch
Multicast sources	128/group	128/group
PIM-SM or PIM-SSM multicast routing information entries ((S,G) entries, (*,G) entries, and negative cache)#2 S: Source IP address G: Group address	128/switch	768/switch
Settings to enable PIM-SSM interoperability with MLDv1/MLDv2 (EXCLUDE mode)#3	256/switch	256/switch
Record information that can be processed per report in MLDv2#4	32 records/ message 32 sources/ record	32 records/ message 32 sources/ record
MLD subscription groups#5	256/switch	256/switch
Multicast neighboring routers	64/switch	64/switch
Rendezvous points	1/group	1/group
Groups that can be assigned to rendezvous points per switch	128/switch	128/switch
Total number of groups that can be assigned to rendezvous points per network (VPN)	128/ network(VPN) 128/switch#6	128/ network(VPN) 128/switch#6
BSR candidates per network (VPN)	16/network (VPN) 32/switch#6	16/network (VPN) 32/switch#6
Static subscription groups#7	256/switch	256/switch
Static rendezvous point (RP) router addresses	16/switch	16/switch
MLD subscription groups per interface#5	256/interface	256/interface
Source addresses per MLD group	256/group	256/group
Remote multicast server addresses to be used as direct connecting servers	256/switch 128/interface	256/switch 128/interface
VRFs to which multicast can be set	31/switch	31/switch
Multicast filters for the extranet#8	64/switch	64/switch
`route-map` to be used for an extranet	32/switch 32/VRF	32/switch 32/VRF

Item	Maximum number	
	AX3830S	AX3650S
Multicasting addresses of PIM-SM VRF Gateway operation#9	32/switch 32/VRF	32/switch 32/VRF

#1

The number of interfaces adjacent to other routers in PIM-SM or PIM-SSM mode.

#2

The maximum number depends on the table entries allocation pattern. For details, see *3.2.1 Number of table entries*. When PIM-SM is used in an environment that satisfies the following conditions, the maximum number of entries is 128 even if a mode in which the maximum number of entries is 128 or more selected.

- Multicast broadband communication is used.
- The Switch acts as a first-hop router or rendezvous point.

The number of entries also depends on the number of IP interfaces (not multicast interfaces) configured in the Switch. Make sure that the total number of I/O ports per entry summed over all entries falls within the range specified in *Table 3-105: Number of multicast I/O ports per number of configured IP interfaces*.

When both IPv4 and IPv6 are enabled, the number of entries is the sum of the IPv4 and IPv6 entries.

When a port is shared by the Input and Output interfaces, the number of I/O ports in an entry is counted as 1. For example, if the input interface uses ports 1/0/1 and 1/0/2, output interface 1 uses ports 1/0/2, 1/0/3, and 1/0/4, and output interface 2 uses ports 1/0/3, 1/0/4, and 1/0/5, there will be five I/O ports for that entry.

#3

The number of source and group pairs depends on the number of interfaces and subscription groups used in the multicast. Make sure that the number of source and group pairs specified is within the range shown in *Table 3-110: Number of used interfaces and number of settings to enable PIM-SSM interoperability with MLDv1/MLDv2 (EXCLUDE mode)* and *Table 3-111: Total number of subscription groups and number of settings to enable PIM-SSM interoperability with MLDv1/MLDv2 (EXCLUDE mode)*. The number of subscription groups is sum of the dynamic and static subscription groups. If a group address subscribes to multiple interfaces, the number of subscription groups is not one but the number of the interfaces to which the group address subscribes.

#4

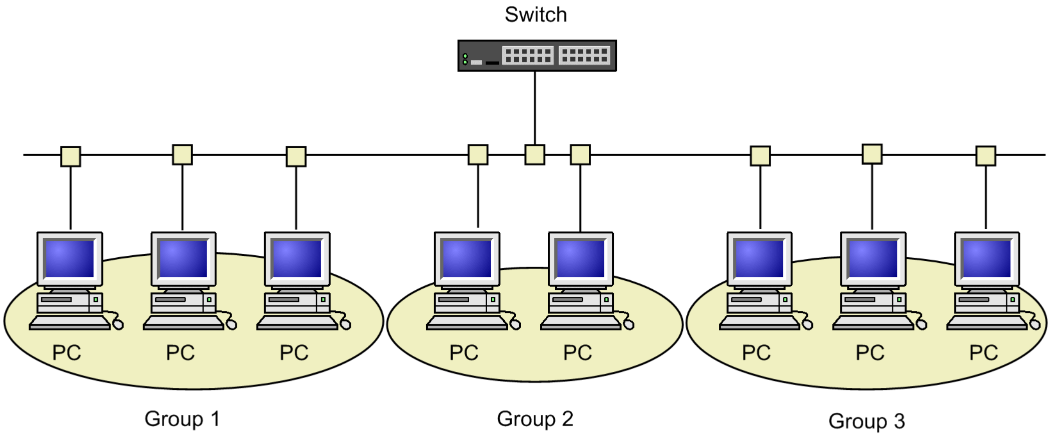
A maximum of 1024 sources can be processed in a Report message. A record that does not contain source information is also counted as one source.

When PIM-SSM is configured to interoperate with MLDv2 (EXCLUDE mode), the number of sources defined in the EXCLUDE record that matches that setting are counted. If there are multiple EXCLUDE records in the received Report message, and if more than 1024 sources were added when configuring PIM-SSM interoperability with MLDv2 (EXCLUDE mode), no multicast relay information will be created for any subsequent EXCLUDE records in that Report message that match the PIM-SSM setting.

#5

The number of groups that connect directly to the Switch. When the source is specified in MLDv2 mode, the number of groups is the number of source-and-group combinations. For example, there are three groups in total in *Figure 3-2: Example of multicast groups*. For details about the number of IPv6 groups that can subscribe per interface, see *Table 3-112: Number of possible subscription groups per interface in IPv6*.

Figure 3-2: Example of multicast groups



#6

The total number of networks (VPN) that are connected to the global network and all VRFs of this Switch.

#7

The number of static subscription groups is the total number of group addresses that statically subscribe to each multicast interface. If a group address statically subscribes to several different interfaces, the number of the static subscription groups is not one but the number of interfaces to which the group address statically subscribes. A maximum of 256 static subscription groups can be set for a single interface.

#8

The total number of addresses in the access lists (`access-list`) specified for all `route-map` instances.

#9

Uses `route-map` specified for the extranet. This applies to multicast addresses that are specified as host addresses (128-bit mask) in the access lists (`access-list`) specified for `route-map`.

The maximum number for each switch is the total number of all group addresses of the PIM-SM VRF gateways specified on VRFs.

This number is added to the number of group addresses specified as static subscription groups.

Table 3-110: Number of used interfaces and number of settings to enable PIM-SSM interoperability with MLDv1/MLDv2 (EXCLUDE mode)

Number of used interfaces	Number of settings to enable PIM-SSM interoperability with MLDv1 or MLDv2 (EXCLUDE mode)
31	256
63	128
127	64

Table 3-111: Total number of subscription groups and number of settings to enable PIM-SSM interoperability with MLDv1/MLDv2 (EXCLUDE mode)

Total number of subscription groups	Number of settings to enable PIM-SSM interoperability with MLDv1/MLDv2 (EXCLUDE mode)
64	256
128	128
256	64
512	32
1024	16
2048	8
4096	4
8128	2

Table 3-112: Number of possible subscription groups per interface in IPv6

Number of used interfaces	Possible number of subscription groups per interface
31	256
63	128
127	64

3.2.14 VRF [OS-L3SA]

The following table describes the number of VRFs that can be set. Note that the global network is not included in the number.

Table 3-113: Number of VRFs that can be set

Item	Number per switch
Number of VRFs that can be set	31

Chapter

4. Login Procedures

This chapter describes how to start and stop the Switches, and how to log in and log out. This chapter also provides an overview of management tasks, and describes operation terminals and their configuration in a network.

4.1 Operation terminal-based management

4.1.1 Operation terminals

A console or remote operation terminal is required to operate the Switch. A console is a terminal connected via RS232C, and a remote operation terminal is a terminal connected via an IP network. The Switch also supports network management by an SNMP manager over an IP network. *Figure 4-1: Connection topology of operation terminals* shows a connection topology of operation terminals and *Table 4-1: Functional requirements of operation terminals* describes their functional requirements.

Figure 4-1: Connection topology of operation terminals

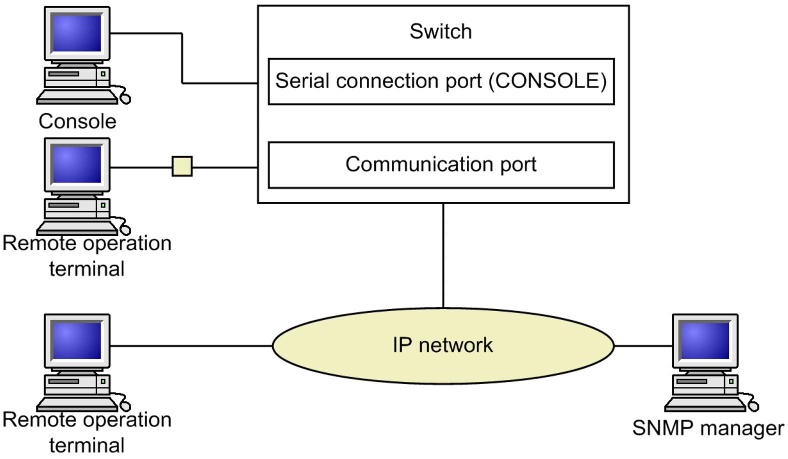

Switch
Serial connection port (CONSOLE)
Communication port
Console
Remote operation terminal
IP network
Remote operation terminal
SNMP manager

Table 4-1: Functional requirements of operation terminals

Terminal type	Connection method	Required specifications
Console	Serial port (RS232C)	RS232C (transmission speed of 19200, 9600, 4800, 2400, or 1200 bit/s) ZMODEM protocol
Remote operation terminal	Communication port	TCP/IP Telnet FTP

(1) Console

The console connects via RS232C and runs general communications software. To enable communication between the console and the Switch, make sure that the following standard VT-100 settings (Switch defaults) are defined in the communication software:

- Communication speed: 9600 bit/s
- Data size: 8 bits
- Parity bit: None
- Stop bit: 1 bit
- Flow control: None

If you want to use the console with a communication speed other than 9600 bit/s (1200, 2400, 4800, or 19200 bit/s), change the communication speed on the Switch side using the `speed` configuration command. The new setting takes effect after you log out from the console.

Figure 4-2: Example of setting the console's communication speed

```
(config)# line console 0
(config-line)# speed 19200
```

To log in from the console to the switch being operated in stack mode, log in to a serially connected member switch. Log in to the master switch if serially connected to it. Log in to the backup switch if serially connected to it.

Note:

Keep the following in mind when using the console.

- When you log in from the console, the Switch automatically acquires and sets the screen size using the VT-100 control characters. If the console does not support VT-100 emulation, the screen size cannot be obtained or set. Invalid character strings might appear or the first CLI prompt might be displayed incorrectly.

  Note that the same problem occurs when you press a key as soon as you log in. This is because display results cannot be acquired for VT-100 control characters. If this happens, log in again.
- The communication speed settings are enabled after logging out. Change the communication speed settings of the communication terminal and communication software you are using after logging out from the console. Until they are changed, some characters are displayed incorrectly (e.g. login prompt).
- If the communication speed is set to settings other than 9600 bit/s, invalid characters appear after starting (or restarting) the device until the new configuration is enabled in the system.

(2) Remote operation terminal

Remote operation terminals connect to the Switch via an IP network and perform command operations. Any terminal that has Telnet client functionality can be used as a remote operation terminal.

Note:

The Telnet server in the Switch recognizes `CR` as the line feed code. Some clients send `CR` and `LF` as the line feed code. If you connect to a switch from this type of terminal, problems will occur: Blank lines might appear, or nothing happens when you press the **Y** or **N** key in response to a prompt. If this is the case, check the client settings.

4.1.2 Connection topology of operation terminals

The following table describes the characteristics of connections from the two types of operation terminal.

Table 4-2: Connection features of operation terminals

Functionality	Serial connection	Communication port
Connected operation terminal	Console	Remote operation terminal
Remote login	Not supported	Supported
Login from the Switch to an operation terminal	Not supported	Supported
Access control	None	Provided
Command input	Supported	Supported
File transfer protocol	ZMODEM protocol	FTP

Functionality	Serial connection	Communication port
IP communication	Not supported	IPv4 and IPv6
SNMP manager connection	Not supported	Supported
Configuration settings	Not required	Required

(1) Serial port

The serial port is for console connections. Because you can log in via this port without performing any configuration settings, you can log in to the Switch immediately after deployment, and then enter the initial settings.

(2) Communication port

Using the communication port, you can log in to the Switch from a remote operation terminal or manage the network via an SNMP manager. To log in to the Switch via this port using Telnet or FTP, you must first register the IP address of the Switch and permit remote access using configuration commands.

4.1.3 Overview of operation management functionality

To begin using the Switch, complete the setup tasks and then power on the Switch. From an operation terminal connected to the Switch, you can execute operation commands and configuration commands to check the device status or to change the configuration as the connected network changes. The following table describes the Switch management operations you can perform.

Table 4-3: Operation management functionality

Functionality	Overview
Command input	Accepts input from the command line.
Login control	Blocks unauthorized access and performs password checks.
Configuration editing	Sets the running configuration. The settings apply immediately.
Network commands	Supports remote operation commands.
Logs and statistics	Shows information such as past failures and statistics about line usage.
LED display and fault reporting	Shows the status of the Switch using LEDs.
MIB information gathering	Manages the network via an SNMP manager.
Switch maintenance	Provides commands such as displaying statuses for maintaining the switch, and line diagnostics for tracking switch and network failures.
Memory card tools	Perform tasks such as formatting memory cards.

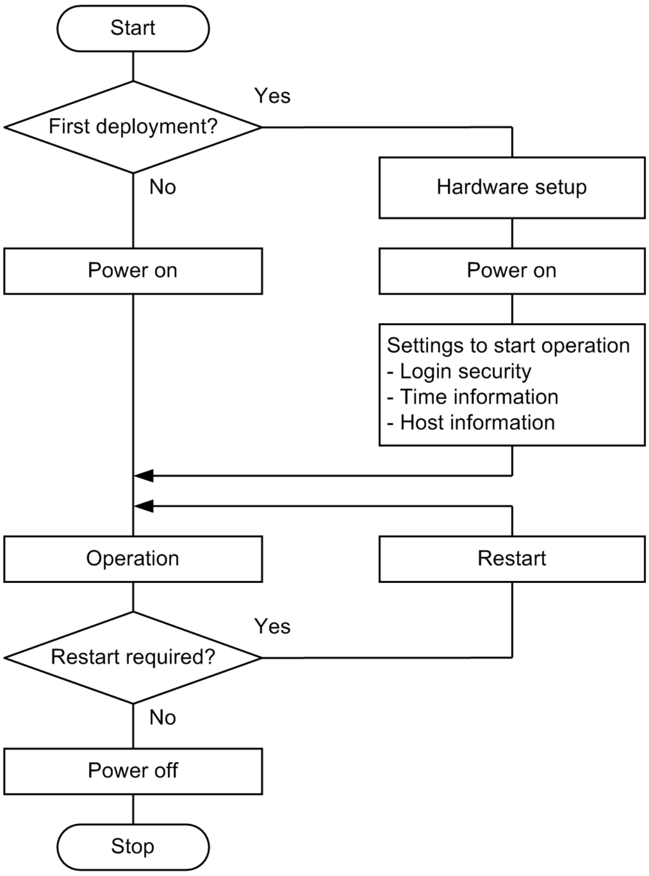
4.2 Starting the switch

This section describes how to start and stop a Switch.

4.2.1 Workflow from starting to stopping a switch

The figure below shows the workflow from starting to stopping the Switch. For the hardware setup procedure, see the *Hardware Instruction Manual*.

Figure 4-3: Workflow from starting to stopping the device



4.2.2 Start procedures

The following table describes the procedures for starting and restarting the Switch.

Table 4-4: Start and restart procedures

Start method	Description	Procedure
Power on	Starts the Switch from the powered-off status.	Turn the power switch on.
Manual restart	Resets the Switch after a failure.	Press the RESET button.
Command restart	Resets the Switch after a failure.	Execute the `reload` command.

Start method	Description	Procedure
Default restart	Restarts a Switch if you cannot log in because you forgot your password, or if you cannot execute commands from the console for some reason such as an error in configuring command authorization. Take care when performing a default restart. This method does not perform authentication by password, authentication when changing to administrator mode (`enable` command), or command authorization. A default restart uses the existing account and configuration information. Note that if you have forgotten your login user name, you will not be able to log in after a default restart. The new password set at a default restart takes effect after the Switch is restarted.	Push and hold the RESET button for at least five seconds.

If the STATUS lamp turns red when you start or restart the Switch, see the *Troubleshooting Guide*. For details about the LED lamp indications, see the *Hardware Instruction Manual*.

The Switch boots from the memory card if you start or restart the Switch from an inserted memory card that contains the software image file `k.img`. When you use this method, the account and configuration information reverts to the factory defaults and you cannot save your own settings. Avoid using this method under normal circumstances.

4.2.3 Stop procedure

Powering off the Switch while files are being accessed might corrupt the files. Make sure that no users are logged in before you power off the Switch. We recommend that you first stop the switch by using the `reload stop` operation command, and then turn off the power.

4.3 Login and logout

This section describes login and logout procedures.

(1) Login

When a switch starts, a login page appears. Enter your user name and password. If authentication is successful, a command prompt appears. If authentication fails, the message `Login incorrect` appears and you cannot log in. The figure below shows the login page.

For the initial deployment, you can log in with the user name `operator`, without needing a password.

Figure 4-4: Login page

```
login: operator

Password: *******                                                       ...1

Copyright (c) 20XX ALAXALA Networks Corporation. All rights reserved.

>                                                                       ...2
```

1. Not displayed unless a password has been set.

   The actual characters in the password are not shown.
2. The command prompt appears.

(2) Logout

To log out after completing operations via the CLI, execute the `logout` command or the `exit` command. The figure below shows the logout page.

Figure 4-5: Logout page

```
> logout
login:
```

(3) Auto-logout

You are automatically logged out if there is no key input for a set duration (default: 60 minutes). You can change the auto-logout time using the `username` configuration command or the `set exec-timeout` operation command.

Chapter

5. Command Operations

This chapter describes how to specify commands on the Switch.

5.1 Command input mode

5.1.1 List of operation commands

The following table describes the operation commands for input mode transitions and utilities.

Table 5-1: List of operation commands

Command name	Description
enable	Changes the command input mode from user mode to administrator mode.
disable	Changes the command input mode from administrator mode to user mode.
quit	Ends the current command input mode.
exit	Ends the current command input mode.
logout	Logs out from the device.
configure (configure terminal)	Changes the command input mode from administrator mode to configuration command mode, and starts configuration editing.
diff#	Compares two specified files and displays their differences.
grep#	Retrieves a specified file and outputs lines containing a specified pattern.
more#	Shows one page of the contents of a specified file.
less#	Shows one page of the contents of a specified file.
tail#	Outputs the contents of a specified file from a specified point.
hexdump#	Shows a hexadecimal dump.

#

For details, see *8. Utilities* in the manual *Operation Command Reference Vol.1 For Version 11.10*.

5.1.2 Command input mode

To change the configuration or check the status of the Switch, you must move to the appropriate command input mode, and then enter a configuration command or operation command. From the CLI prompt, you can tell which command input mode you are in.

The following table describes the correspondences between command input modes and CLI prompts.

Table 5-2: Correspondences between command input modes and CLI prompts

Command input mode	Executable command	Prompt
User mode	Operation commands (Some commands, such as `configure` and `adduser`, can only be executed in administrator mode.)	>
Administrator mode		#
Configuration command mode	Configuration commands#	(config)#

#

You can execute an operation command while editing a configuration entry without changing the command input mode to administrator mode by using commands such as the `quit` command and the `exit` command. To do so, enter the operation command preceded by a dollar sign (`$`).

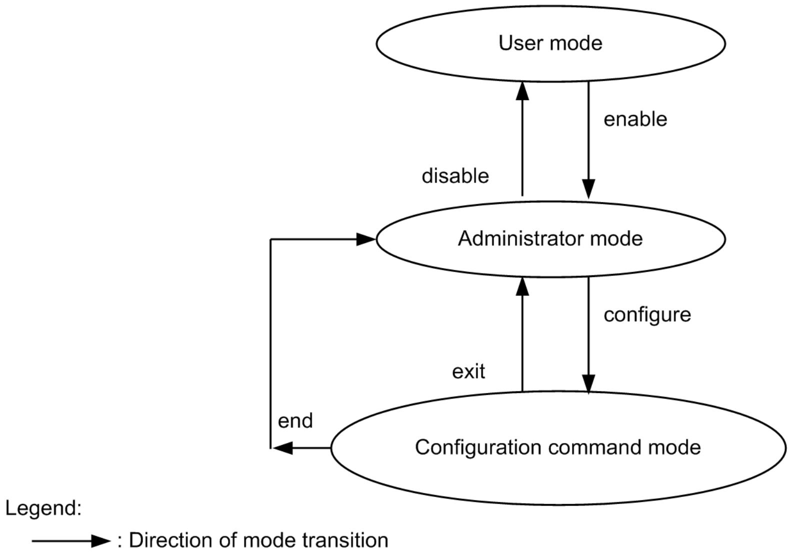
Example

To execute the `show ip arp` operation command in configuration command mode:

```
(config)# $show ip arp
```

The following figure provides an overview of mode transitions.

Figure 5-1: Overview of mode transitions



In the following situations, letters appear in front of the CLI prompt to show you where you are:

1. When you set a host name using the `hostname` configuration command, the first 20 characters of the host name appear in the prompt.
2. If you edit the running configuration but do not save it as the startup configuration, an exclamation mark (!) appears in front of the prompt.

The following figure shows an example of these two situations.

Figure 5-2: Example of displaying prompts

```
> enable
# configure
(config)# hostname "OFFICE1"
!OFFICE1(config)# save
OFFICE1(config)# quit
OFFICE1# quit
OFFICE1>
```

5.2 CLI operations

5.2.1 Command line completion

By pressing the **Tab** key on the command line, you can complete a partially entered command name or file name, which simplifies command input. The following figure shows an example of simplified command input using this functionality.

Figure 5-3: Simplified command input using command line completion

```
(config)# in[Tab]
(config)# interface
```

By pressing the **Tab** key here, a list of parameters and file names that can be specified appears:

```
(config)# interface [Tab]
gigabitethernet     port-channel        tengigabitethernet
loopback            range               vlan
(config)# interface
```

5.2.2 Help functionality

By typing a question mark (?) on the command line, you can search for a specifiable command or parameter. You can also find out what the command or parameter means. The following figure shows an example of the Help display when you enter a question mark.

Figure 5-4: Example of Help display by entering a question mark

```
> show vlan ?
  <vlan id list>        1 to 4094 ex. "5", "10-20" or "30,40"
  channel-group-number  Display the VLAN information specified by
                        channel-group-number
  detail                Display the detailed VLAN information
  list                  Display the list of VLAN information
  mac-vlan              Display the MAC VLAN information
  port                  Display the VLAN information specified by port number
  summary               Display the summary of VLAN information
  <cr>
> show vlan
```

If you type a question mark in a parameter without entering a preceding space, command line completion will activate. To use a question mark (?) in a command parameter, press **Ctrl** + **V**, and then type the question mark.

5.2.3 Entry-error location detection functionality

If you enter a command or parameter incorrectly, the error is marked by a caret (^) and an error message appears on the next line. For details on error messages, see *Error messages displayed by the entry-error location detection functionality* in the manual *Operation Command Reference Vol.1 For Version 11.10*. Input errors when you press the **Tab** key or type a question mark are indicated in the same manner.

Check and re-enter the command or parameter, referring to the marked location and error message. *Figure 5-5: Display example for a spelling mistake* and *Figure 5-6: Display example for a missing parameter* show display examples of entry errors.

Figure 5-5: Display example for a spelling mistake

```
(config)# interface gigabitehternet 1/0/1
interface gigabitehternet 1/0/1
                  ^
% illegal parameter at '^' marker
(config)# interface gigabitehternet 1/0/1
```

Figure 5-6: Display example for a missing parameter

```
(config)# interface gigabitethernet 1/0/1
(config-if)# speed
speed
      ^
% Incomplete command at '^' marker
(config-if)#
```

5.2.4 Abbreviated-command execution

A command or parameter entered in abbreviated form will be executed if the entered characters are recognized as a unique command or parameter. The following figure shows an example of abbreviated-command execution.

Figure 5-7: Example of abbreviated-command execution (show ip arp command)

```
> sh ip ar
Date 20XX/11/15 19:37:02 UTC
Total: 1 entries
 IP Address       Linklayer Address  Netif             Expire     Type
 192.168.0.1      0012.e2d0.e9f5     VLAN0010          3h44m57s   arpa
>
```

The commands related to configuration editing and operation listed in *Table 6-1: List of configuration commands* cannot be abbreviated except in level-1 configuration mode.

Parameters following a parameter containing an asterisk (*) cannot be abbreviated.

5.2.5 History functionality

The history functionality allows you to easily re-execute a command entered in the past, and to change part of the command before execution. The following figure shows some examples of using the history functionality.

Figure 5-8: Simplified command input using the history functionality

```
> ping 192.168.0.1 numeric count 1                          ...1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=31 time=1.329 ms

--- 192.168.0.1 PING Statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max = 1.329/1.329/1.329 ms
>                                                           ...2
> ping 192.168.0.1 numeric count 1                          ...3
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=31 time=1.225 ms

--- 192.168.0.1 PING Statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max = 1.225/1.225/1.225 ms
>                                                           ...4
> ping 192.168.0.2 numeric count 1                          ...5
PING 192.168.0.2 (192.168.0.2): 56 data bytes

--- 192.168.0.2 PING Statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
>
```

1. Execute the `ping` command on 192.168.0.1.
2. Press the up arrow key (↑) to call the preceding command.

In this example, pressing the up arrow key once displays the line ping 192.168.0.1 numeric count 1. Simply press Enter to re-execute this command.

3. Execute the `ping` command on 192.168.0.1.

4. Press the up arrow key (↑) to call the preceding command, and then use the left arrow key (<-) and the Backspace key to edit the command string.

   In this example, pressing the up arrow key (↑) once displays the line ping 192.168.0.1 numeric count 1. Change 1 in the IP address to 2, and then press the Enter key.

5. Execute the `ping` command on 192.168.0.2.

Using the history functionality and the character strings in the table below, you can call or change a previously executed command string, and then execute the command. Command string conversion is not supported for configuration commands.

Table 5-3: Characters supported by command string conversion

No.	Specification	Description
1	!!	Calls and executes the last executed command.
2	!*n*	Calls and executes the command that has history number *n*#.
3	!-*n*	Calls and executes the *n*th previous command.
4	!str	Calls and executes the last executed command beginning with the character string `str`.
5	^str1^str2	Executes the last executed command, replacing `str1` with `str2`.

#

The array number displayed by the `show history` operation command.

After you call a previously executed command, and then edit the command string or delete the command using the **Backspace** key or the **Ctrl** + **C** keys, you can call the command again and edit or erase its history.

Notes

Depending on the communication software you are using, the arrow keys (↑, ↓, <-, ->) might not call a command. If so, check the settings in your communication software manual.

5.2.6 Pipe function

Using the pipe function, you can pass command execution results to another command. Passing the results to the `grep` command can make them easier to understand. However, response messages, such as those indicating that command execution failed, are not passed, and are displayed when a command is executed. *Figure 5-9: Results of executing the show sessions command* shows the execution results of the `show sessions` command, and *Figure 5-10: Results of executing the show sessions command filtered by the grep command* shows the same results when filtered by the `grep` command.

Figure 5-9: Results of executing the show sessions command

```
> show sessions
Date 20XX/01/07 12:00:00 UTC
operator console  -----  0   Jan  6 14:16
operator ttyp0    -----  2   Jan  6 14:16 (192.168.3.7)
operator ttyp1    -----  3   Jan  6 14:16 (192.168.3.7)
operator ttyp2    admin  4   Jan  6 14:16 (192.168.3.7)
```

Figure 5-10: Results of executing the show sessions command filtered by the grep command

```
> show sessions | grep admin
operator ttyp2    admin  4   Jan  6 14:16 (192.168.3.7)
>
```

5.2.7 Redirection

Using the redirection functionality, you can output command execution results to a file. However, response messages, such as those indicating that command execution failed, are not output to a file, and are displayed on a page when a command is executed. The following figure shows an example of outputting the execution result of the `show ip interface` command to a file.

Figure 5-11: File output of the show ip interface command execution result

```
> show ip interface > show_interface.log
>
```

5.2.8 Paging

When the information you want to view in the command execution results extends outside the viewable area, you can scroll the information page by page, by input from the keyboard. Paging is not performed when redirection is used. Paging can be enabled or disabled by executing the `username` configuration command or the `set terminal pager` operation command.

5.2.9 Customizing CLI settings

The behavior of part of the auto-logout and CLI functionality can be customized on a user basis as CLI environment information. The following table describes the CLI functions and CLI environment information that can be customized.

Table 5-4: Customizable CLI functionality and CLI environment information

Functionality	Customizable contents and defaults
Auto-logout	Time until the user is automatically logged out. Default: 60 minutes
Paging	Whether to enable paging. Default: Paging enabled
Help functionality	List of commands displayed in Help messages. Default: When you display a Help message for operation commands, a list of all specifiable operation commands appears.

This CLI environment information can be set for each user by executing the `username` configuration command or the following operation commands:

- set exec-timeout
- set terminal pager
- set terminal help

Settings entered by the `username` configuration command take priority over settings entered by the operation commands. When any one of the three items of CLI environment information is set for a user by the `username` configuration command, values set by the three operation commands do not apply to that user. The customizable CLI functions behave as specified in the `username` configuration command, and the defaults apply to omitted items of CLI environment information.

The operation command settings apply when there are no username settings. When no CLI environment information is set for a user by the `username` configuration command, the operation command settings apply to that user. Note that you cannot view these settings. Instead, check each function's activity status.

In a session during which an operation command is executed, operation command settings are applied to the behavior of the CLI immediately after the command is executed. For other sessions, the settings are applied at the next login, even if the same user executed the commands. For operations using configuration command settings, the CLI behavior of a temporarily executed session can be changed.

If operation command settings are being used, and you add a user account by the `adduser` command with the `no-flash` parameter specified, the CLI environment information for that user reverts to the defaults when the switch is restarted.

5.3 Notes on CLI operation

(1) If an operation terminal crashes after logging in

If an operation terminal crashes, the user's login status is sometimes retained in the Switch. If this occurs, either wait for the user to be automatically logged out, or log in again and delete the login user by using the `killuser` operation command.

(2) Notes on CLI operations with special keys

Pressing **Ctrl** + **C**, **Ctrl** + **Z** or **Ctrl** + \ might cause you to log out. In such a case, log in again.

Chapter

6. Configuration

The configuration and operating conditions of the Switch must be set to match the network environment. This chapter describes what you need to know when setting the configuration.

6.1 Configuration

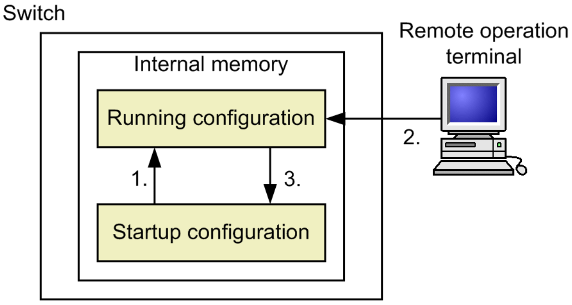
Both at deployment and during operation, the administrator will need to perform configuration settings relating to the connected network and the operating conditions of the Switch. The switch configuration is not predefined at initial deployment.

6.1.1 Configuration at startup

When you power on the Switch, the startup configuration file in internal memory is read and operation commences according to the file contents. The configuration used during operation is referred to as the running configuration.

You cannot directly edit the startup configuration. It is updated automatically when you edit the running configuration and then execute the `save` (`write`) command. The following figure provides an overview of the configuration at startup and during operation.

Figure 6-1: Overview of the configuration at startup and during operation



1. At startup, the startup configuration is read and loaded as the running configuration. Operation starts according to the running configuration contents.
2. Any changes to the configuration are reflected in the running configuration.
3. The new running configuration is saved as the startup configuration.

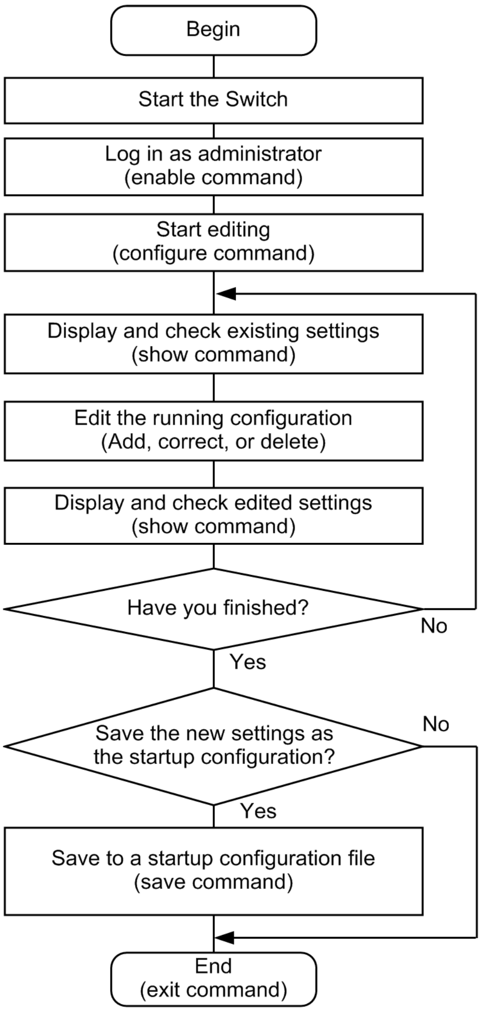
6.1.2 Configuration during operation

When you edit a configuration during operation, the edited contents are immediately applied as the running configuration. By executing the `save` (`write`) command, you can save the running configuration as the startup configuration in the switch's internal memory. Note that the edited contents will be lost if you restart a switch without first saving the running configuration.

6.2 Overview of editing a running configuration

You will need to edit the running configuration at initial deployment and after changing the network configuration. Editing at deployment must be performed on the console. The figure below shows the workflow. For details, see *6.4 Configuration editing procedures*.

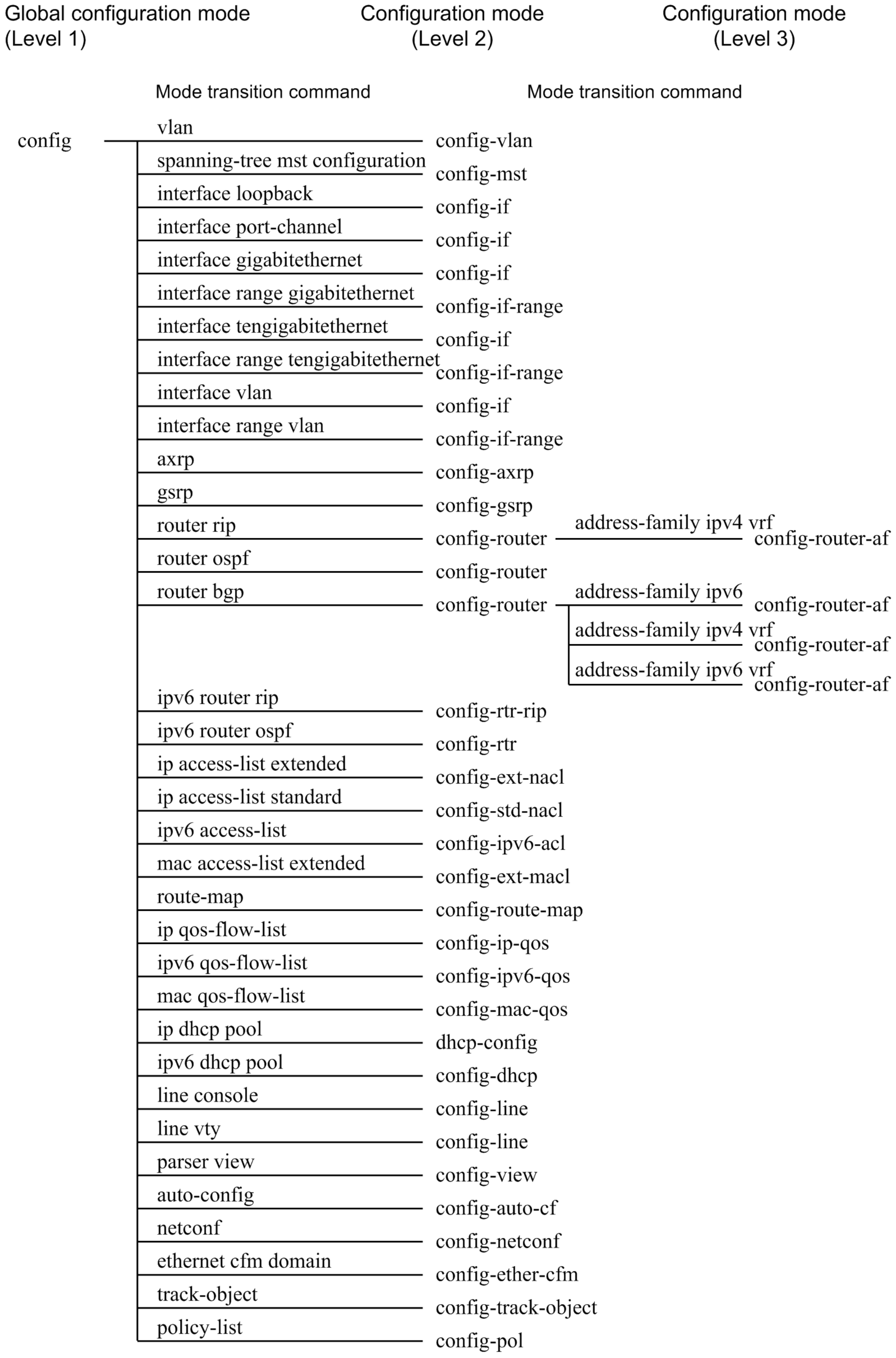
Figure 6-2: Workflow when editing a running configuration



6.3 Mode transitions when entering configuration commands

Edit configurations in the appropriate executable configuration mode. To edit a level-2 configuration, you must first switch from global configuration mode to a level-2 configuration mode using a mode transition command. You can then execute the required configuration commands. The following figure provides an overview of transition between configuration modes.

Figure 6-3: Overview of configuration mode transition



6.4 Configuration editing procedures

6.4.1 Lists of configuration commands and operation commands

The following table describes the configuration commands for editing and working with configurations.

Table 6-1: List of configuration commands

Command name	Description
end	Ends configuration command mode and returns you to administrator mode.
quit (exit)	Returns to the previous mode. If you are editing a configuration in global configuration mode, the command ends configuration command mode and returns you to administrator mode.
save (write)	Saves the edited configuration as the startup configuration.
show	Shows the configuration being edited.
status	Shows the status of the configuration being edited.
top	Returns you from a level-2 or level-3 configuration command mode to global configuration mode (level 1).

The following table describes the operation commands for editing and working with configurations.

Table 6-2: List of operation commands

Command name	Description
show running-config	Shows the running configuration.
show startup-config	Shows the startup configuration.
copy	Copies a configuration.
erase configuration	Resets a running configuration to the defaults.
show file	Shows the contents and line numbers of a local or remote server file.
cd	Changes the directory.
pwd	Shows the path to the present working directory.
ls	Lists files and directories.
dir	Lists recoverably deleted files used by the Switch.
cat	Shows the contents of a specified file.
cp	Copies a file.
mkdir	Creates a new directory.
mv	Moves or renames a file.
rm	Deletes a specified file.
rmdir	Deletes a specified directory.
delete	Recoverably deletes files used by the Switch.
undelete	Restores recoverably deleted files used by the Switch.

Command name	Description
squeeze	Completely erases files used by the Switch that have been recoverably deleted.
zmodem	Transfers files between the Switch and console connected by RS232C.

6.4.2 Starting configuration editing (configure command and configure terminal command)

To edit a configuration, first execute the `enable` command to switch to administrator mode. Then enter the `configure` command or the `configure terminal` command. The prompt changes to `(config)#`, allowing you to edit the running configuration. The following figure shows an example of starting editing of a running configuration.

Figure 6-4: Example of starting editing of a running configuration

```
> enable               ...1
# configure            ...2
(config)#
```

1. Execute the `enable` command to enter administrator mode.
2. Start editing the running configuration.

6.4.3 Displaying and checking configuration entries (show command)

(1) Displaying and checking the running configuration or startup configuration

You can display and check the running configuration or startup configuration by using the `show running-config` or `show startup-config` operation command in administrator mode. The following figure shows an example of displaying a running configuration.

Figure 6-5: Example of displaying a running configuration

```
OFFICE01# show running-config                 ...1
#default configuration file for XXXXXX-XX
!
hostname "OFFICE01"
!
vlan 1
  name "VLAN0001"
!
vlan 100
  state active
!
vlan 200
  state active
!
interface gigabitethernet 1/0/1
  switchport mode access
  switchport access vlan 100
!
interface gigabitethernet 1/0/2
  switchport mode access
  switchport access vlan 200
!
OFFICE01#
```

1. Display the running configuration.

(2) Displaying and checking configuration entries

Using the `show` command in configuration mode, you can display and check configuration entries before or after they have been edited. *Figure 6-6: Displaying all configuration entries* to *Figure 6-9: Displaying information for a specified interface in interface mode* show examples of displayed configuration entries.

Figure 6-6: Displaying all configuration entries

```
OFFICE01(config)# show                 ...1
#default configuration file for XXXXXX-XX
!
hostname "OFFICE01"
!
vlan 1
  name "VLAN0001"
!
vlan 100
  state active
!
vlan 200
  state active
!
interface gigabitethernet 1/0/1
  switchport mode access
  switchport access vlan 100
!
interface gigabitethernet 1/0/2
  switchport mode access
  switchport access vlan 200
!
OFFICE01(config)#
```

1. Display the entire running configuration when you omit all parameters.

Figure 6-7: Displaying information for all configured interfaces

```
OFFICE01(config)# show interface gigabitethernet        ...1
interface gigabitethernet 1/0/1
  switchport mode access
  switchport access vlan 100
!
interface gigabitethernet 1/0/2
  switchport mode access
  switchport access vlan 200
!
OFFICE01(config)#
```

1. Display all the configured interfaces in the running configuration.

Figure 6-8: Displaying information for a specified interface

```
OFFICE01(config)# show interface gigabitethernet 1/0/1       ...1
interface gigabitethernet 1/0/1
  switchport mode access
  switchport access vlan 100
!
OFFICE01(config)#
```

1. Display interface 1/0/1 in the running configuration.

Figure 6-9: Displaying information for a specified interface in interface mode

```
OFFICE01(config)# interface gigabitethernet 1/0/1
OFFICE01(config-if)# show                               ...1
interface gigabitethernet 1/0/1
  switchport mode access
  switchport access vlan 100
!
OFFICE01(config-if)#
```

1. Display interface 1/0/1 in the running configuration.

6.4.4 Adding, changing, and deleting configuration entries

(1) Configuration command input

Configuration commands are used for editing configuration entries. You can also negate a configuration command by specifying `no` at the beginning.

To disable functionality using this method, specify `no` at the beginning of the command string. To reinstate the functionality, enter the same command without the preceding `no`.

Figure 6-10: Example of editing a configuration shows an example of editing a configuration, and *Figure 6-11: Example of disabling and reinstating functionality* shows an example of disabling functionality and later reinstating it.

Figure 6-10: Example of editing a configuration

```
(config)# vlan 100                                    ...1
(config-vlan)# state active                           ...2
(config-vlan)# exit
(config)# interface gigabitethernet 1/0/1             ...3
(config-if)# switchport mode access                   ...4
(config-if)# switchport access vlan 100               ...5
(config-if)# exit
(config)#
(config)# vlan 100                                    ...6
(config-vlan)# state suspend                          ...7
(config-vlan)# exit
(config)#
(config)# interface gigabitethernet 1/0/1             ...8
(config-if)# no switchport access vlan                ...9
```

1. Configure VLAN 100 as a port VLAN.
2. Activate VLAN 100.
3. Move to Ethernet interface 1/0/1 configuration mode.
4. Set the access mode for port 1/0/1.
5. Configure VLAN 100 as an accessed VLAN.
6. Move to VLAN 100 configuration mode.
7. Change VLAN 100 from the active status to the inactive status.
8. Move to Ethernet interface 1/0/1 configuration mode.
9. Remove VLAN ID 100 from the defined accessed VLANs.

Figure 6-11: Example of disabling and reinstating functionality

```
(config)# no ip domain lookup                         ...1
(config)# ip domain name router.example.com           ...2
(config)# ip name-server 192.168.0.1                  ...3
(config)# ip domain lookup                            ...4
```

1. Disable the DNS resolver functionality.
2. Set the domain name as `router.example.com`.

3. Set the name server as 192.168.0.1.
4. Activate the DNS resolver functionality.

(2) Command syntax check

When you enter a configuration command, the system immediately checks whether the input configuration contains any errors. If there are no errors, the prompt shown in *Figure 6-12: Output for a correct configuration* appears, ready for command input. If you are editing a running configuration, the edited contents take effect immediately.

If an error is found in the input configuration, an error message indicating the nature of the error appears in the line below the entered command, as shown in *Figure 6-13: Error message output for an incorrect configuration*. In this case, the edited configuration does not take effect. Correct the error and re-enter the configuration command.

Figure 6-12: Output for a correct configuration

```
(config)# interface gigabitethernet 1/0/1
(config-if)# description TokyoOsaka
(config-if)#
```

Figure 6-13: Error message output for an incorrect configuration

```
(config)# interface tengigabitethernet 1/0/1
(config-if)# description
description
            ^
% Incomplete command at '^' marker
(config-if)#
```

6.4.5 Applying an edited configuration

When you change a configuration, it takes effect as soon as you enter the configuration command. If you have edited the BGP filter settings, however, you must instead execute the `clear ip bgp` operation command to apply the changes to the switch operation.

On execution of the `clear ip bgp` operation command, changes made to the configuration by the following commands take effect automatically:

- access-list command
- prefix-list command
- route-map command
- distribute-list in command
- distribute-list out command
- redistribute command
- neighbor in command
- neighbor out command

A command input example is shown below.

Figure 6-14: Example of command input

```
(config)# ip access-list standard 1  .............................(1)
(config-std-nacl)# permit 10.0.0.0 0.255.255.255  ................(2)
(config-std-nacl)# permit 172.16.0.0 0.0.255.255  ................(3)
(config-std-nacl)# exit
(config)# ip prefix-list PEER-OUT seq 10 permit 172.16.1.0/24  ...(4)
(config)# route-map SET-COMM 10  .................................(5)
(config-route-map)# match ip address prefix-list PEER-OUT  .......(6)
(config-route-map)# set community no-export  .....................(7)
(config-route-map)# exit
(config)# router bgp 65530
(config-router)# distribute-list 1 in  ...........................(8)
```

```
(config-router)# redistribute static  ..........................(9)
(config-router)# neighbor 192.168.1.1 remote-as 65531
(config-router)# neighbor 192.168.1.2 remote-as 65532
(config-router)# neighbor 192.168.1.2 send-community
(config-router)# neighbor 192.168.1.2 route-map SET-COMM out  ....(10)
(config-router)# exit
(config)# save
(config)# exit
# clear ip bgp * both                                            ...1
```

1. The changes in (1) to (10) are used in the switch operation.

6.4.6 Saving configuration entries to a file (save command)

Using the `save` (`write`) command, you can save the edited running configuration to the startup configuration file. The following figure shows an example of saving a configuration.

Figure 6-15: Example of saving a configuration

```
# configure                 ...1
(config)#
       :
       :                    ...2
       :
!(config)# save             ...3
(config)#
```

1. Start editing the running configuration.
2. Change the configuration.
3. Save to the startup configuration file.

6.4.7 Ending configuration editing (exit command)

When you have finished editing the running configuration, execute the `exit` command in global configuration mode. If you execute the `exit` command without saving the changes to the startup configuration file via the `save` command, a confirmation message appears. To exit configuration command mode without saving your changes, type `y`. If you type any other letter, you will remain in configuration command mode. *Figure 6-16: Example of ending configuration editing* and *Figure 6-17: Example of ending configuration editing without saving your changes* show examples of ending configuration editing.

Figure 6-16: Example of ending configuration editing

```
!(config)# save
(config)# exit             ...1
```

1. End configuration editing.

Figure 6-17: Example of ending configuration editing without saving your changes

```
# configure                                                    ...1
(config)#
       :
       :                                                       ...2
       :
!(config)# exit
Unsaved changes found! Do you exit "configure" without save ? (y/n): y ...3
!#
```

1. Start configuration editing.
2. Change the configuration.

3. A confirmation message appears.

6.4.8 Notes on configuration editing

(1) Limits on the number of configuration commands

Because user configurations are stored in memory, the number of commands you can enter in configuration entries depends on the amount of available memory. If there is insufficient memory for the entries, or if the number of entries you have edited exceeds the switch capacity, either of the following messages appears: `Maximum number of entries is already defined (config memory shortage).` *<IP>* or `Maximum number of entries are already defined.` *<IP>*. If such a message appears, check whether any unnecessary entries exist.

(2) Copying and pasting configuration entries

You can copy and paste configuration entries up to a maximum of 1000 characters per line, and less than 4000 characters total (including spaces and line feed codes) per operation. Note that the configurations will not be set correctly if you attempt to paste 4000 characters or more at one time.

If the configuration entries exceed 4000 characters, copy and paste them in multiple operations, each time keeping the number of characters to no more than 1000 per line and less than 4000 total.

6.5 Configuration operations

This section describes operations such as configuration backups and file transfers.

6.5.1 Backing up configurations

Using the `copy` operation command, you can back up a configuration to a remote server or to the Switch itself. Note that when saving a backup configuration file to the Switch, you cannot specify the directory for the startup configuration file (`/config`). Create your own backup configuration files in your home directory.

You can back up both the startup configuration and running configuration. If you change a configuration entry during operation but do not save the changes, the contents of the backed-up configuration file (startup configuration) will differ from the running configuration. The following figures show examples of backing up the startup and running configurations.

Figure 6-18: Example of backing up the startup configuration

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

Authentication for 2001:240:400::101.
User: staff
Password: xxx                              ...1
transferring...

Data transfer succeeded.
#
```

1. Enter the password stored on the remote server for the user account staff.

Figure 6-19: Example of backing up the running configuration

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

Authentication for 2001:240:400::101.
User: staff
Password: xxx                              ...1
transferring...

Data transfer succeeded.
#
```

1. Enter the password stored on the remote server for the user account staff.

6.5.2 Copying backup configuration files to the Switch

Use the `copy` operation command to apply a backup configuration file as the startup or running configuration. The following figures show examples of replacing the startup and running configuration with a backup file.

Figure 6-20: Example of replacing the startup configuration with a backup file

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

```
Authentication for 2001:240:400::101.
User: staff
Password: xxx                             ...1
transferring...

Data transfer succeeded.
#
```

1. Enter the password stored on the remote server for the user account staff.

Figure 6-21: Example of replacing the running configuration with a backup file

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

Authentication for 2001:240:400::101.
User: staff
Password: xxx                             ...1
transferring...

Data transfer succeeded.
#
```

1. Enter the password stored on the remote server for the user account staff.

6.5.3 Transferring files using the zmodem command

Use the `zmodem` command to transfer files between the Switch and the console connected by an RS232C cable.

(1) Transferring a backup configuration file to the Switch

After transferring the backup configuration file to your home directory on a Switch (`/usr/home/operator`), copy it to the startup configuration by using the `copy` operation command. The following figure shows an example of transferring a backup configuration file to the Switch by using the `zmodem` command.

Figure 6-22: Example of transferring a backup configuration file to the Switch (zmodem command)

```
> cd /usr/home/operator
> zmodem get backup.cnf                                 ...1
**B000000027fed4
**B000000027fed4
> enable
# copy /usr/home/operator/backup.cnf startup-config     ...2
Configuration file copy to startup-config ? (y/n): y    ...3
#
```

1. Transfer the backup configuration file. The file name after transfer is the same as the specified source file name.
2. Use the backup configuration file (`backup.cnf`) as the startup configuration.
3. Confirm that you want to replace the existing startup configuration.

(2) Transferring a backup configuration file to the console

The following figure shows an example of transferring a backup configuration file stored in the Switch to the console.

Figure 6-23: Example of transferring a backup configuration file to the console

```
> cd /usr/home/operator
> enable
# copy running-config backup.cnf                   ...1
Configuration file copy to /usr/home/operator/backup.cnf? (y/n) : y
# exit
> zmodem put backup.cnf                            ...2
**000000000000
>
```

1. Copy the running configuration file to the backup configuration file.
2. Transfer the backup configuration file.

6.5.4 Transferring files using the ftp command

Use the `ftp` command to transfer files between the Switch and a remote operation terminal.

(1) Transferring a backup configuration file to the Switch

After transferring the backup configuration file to your home directory on a Switch (`/usr/home/operator`), copy it to the startup configuration by using the `copy` operation command. The following figure shows an example of transferring a backup configuration file to the Switch by using the `ftp` command.

Figure 6-24: Example of transferring a backup configuration file to the Switch (ftp command)

```
> cd /usr/home/operator
> ftp 192.168.0.1
Connect to 192.168.0.1.
220  FTP server (Version wn-2.4(4) Wed Jan 1 00:00:00 JST 1999) ready.
Name (192.168.0.1:operator): test
331 Password required for test.
Password:xxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp> get backup.cnf                                         ...1
local: backup.cnf remote: backup.cnf
200 PORT command successful.
150 Opening BINARY mode data connection for backup.cnf (12,345 bytes)
226 Transfer complete.
ftp> bye
221 Goodby
> enable
# copy /usr/home/operator/backup.cnf startup-config         ...2
Configuration file copy to startup-config ? (y/n): y        ...3
#
```

1. Transfer the backup configuration file.
2. Use the backup configuration file (`backup.cnf`) as the startup configuration.
3. Confirm that you want to replace the existing startup configuration.

(2) Transferring a backup configuration file to a remote operation terminal

The following figure shows an example of transferring a backup configuration file stored in the Switch to a remote operation terminal.

Figure 6-25: Example of transferring a backup configuration file to a remote operation terminal

```
> cd /usr/home/operator
> enable
# copy running-config backup.cnf                          ...1
Configuration file copy to /usr/home/operator/backup.cnf? (y/n) : y
```

```
# exit
> ftp 192.168.0.1
Connect to 192.168.0.1.
220  FTP server (Version wn-2.4(4) Fri Jan 1 00:00:00 JST 1999) ready.
Name (192.168.0.1:operator): test
331 Password required for test.
Password:xxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp> put backup.cnf                                       ...2
local: backup.cnf remote: backup.cnf
200 PORT command successful.
150 Opening BINARY mode data connection for backup.cnf (12,345 bytes)
226 Transfer complete.
ftp> bye
221 Goodby
>
```

1. Copy the running configuration file to the backup configuration file.
2. Transfer the backup configuration file.

6.5.5 Transferring files using a memory card

Use the `cp` command to transfer files to a memory card.

(1) Transferring a backup configuration file to the Switch

After transferring the backup configuration file from a memory card to your home directory (`/usr/home/operator`), copy it to the startup configuration by using the `copy` operation command. The following figure shows an example of transferring a backup configuration file to the Switch by using the `cp` command.

Figure 6-26: Example of transferring a backup configuration file on a memory card to the Switch (cp command)

```
> cd /usr/home/operator
> cp mc-file backup.cnf backup.cnf                           ...1
> enable
# copy /usr/home/operator/backup.cnf startup-config          ...2
Configuration file copy to startup-config? (y/n): y          ...3
#
```

1. Transfer the backup configuration file from the memory card.
2. Use the backup configuration file (`backup.cnf`) as the startup configuration.
3. A confirmation message asking whether you want to replace the existing startup configuration appears.

(2) Transferring a backup configuration file to a memory card

The following figure shows an example of transferring a backup configuration file stored in the Switch to a memory card.

Figure 6-27: Example of transferring a backup configuration file to a memory card

```
> cd /usr/home/operator
> enable
# copy running-config backup.cnf                          ...1
Configuration file copy to /usr/home/operator/backup.cnf? (y/n) : y
# exit
> cp backup.cnf mc-file backup.cnf                        ...2
>
```

1. Copy the running configuration file to the backup configuration file.
2. Transfer the backup configuration file to the memory card.

6.5.6 Notes on applying a backup configuration file

When you copy a backup configuration file to the Switch's running configuration by using the `copy` operation command, the port being used is restarted. Be careful if you are logged in over a network.

If the contents of the backup configuration file are inconsistent with the Switch's actual configuration, amend the file and then use the `copy` operation command. If you execute the `copy` command on an inconsistent backup configuration file, the command will either return an error, or it might complete successfully but the file contents will not be applied properly. Amend the file, and then re-execute the `copy` command.

Chapter

7. Description of Stack Functionality

This chapter describes the stack functionality.

7.1 Overview of stack functionality

7.1.1 Overview

In a stack configuration, multiple switches are connected to logically run as one switch. The functionality to manage multiple switches as one logical switch is called the stack functionality. Stack configurations have the following features:

- Consolidated management

  Allows you to run multiple switches as one switch.

- Redundancy

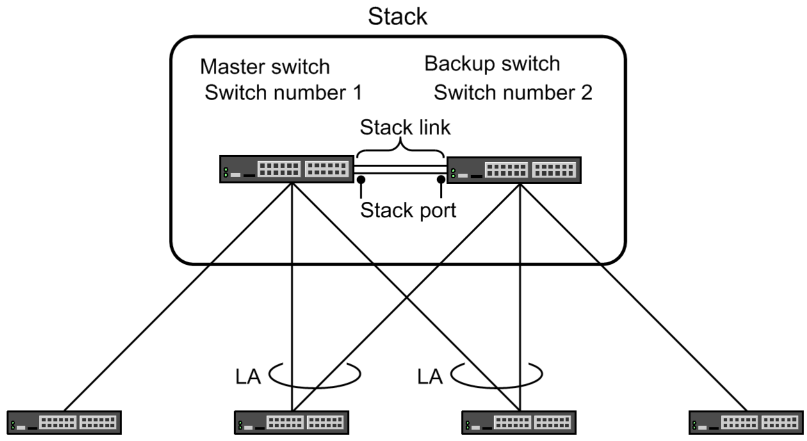
  Ensures that communication can continue in the event of a fault in part of the configuration.

- Expansion

  Allows you to add switches to increase the number of ports.

The stack is configured by connecting switches running the stack functionality via an Ethernet interface. The following figure shows an example of a stack configuration.

Figure 7-1: Example of stack configuration



Legend: LA: Link aggregation

Each switch that configures the stack is called a member switch. The number that identifies a member switch is called a switch number. One of the member switches is called the master switch, and the other is called the backup switch. The port that connects these member switches is called a stack port. The line that connects two member switches with a stack port is called a stack link.

A stack can be configured with one or two member switches. Up to two stack ports can be configured to a member switch.

The master switch controls the member switches that make up the stack. In the event of a fault in the master switch, the backup switch runs as the new master switch.

7.1.2 Stack and standalone configuration

The status where a switch is not running the stack functionality is called the standalone status. A standalone switch does not make up a stack, and always runs alone.

This Switch becomes part of a stack by running the stack functionality. To run the stack functionality, you must set the `stack enable` configuration command, save the configuration to the startup configuration, and then restart the Switch.

To return the Switch running the stack functionality to the standalone status, you must delete the setting with the `no stack enable` configuration command, save the configuration to the startup configuration, and then restart the Switch.

If any functionality that is not supported by the stack is required, use the Switch in the standalone status.

7.1.3 Support functionality

The following table describes the support status of each functionality in the stack.

Table 7-1: Support status in the stack

Item		Support status	Remark
Operation management	Login from the console	Y	None
	Login from a remote operation terminal	Y	
	Configuration operations and editing	Y	
	Login Security and RADIUS or TACACS+	Y	
	Time Settings and NTP	Y	
	Host Names and DNS	Y	
	Power saving functionality	P	Power OFF to ports for which the `shutdown` configuration command is supported.
	Open Autonomic Networking (OAN)	--	None
Network interface	Ethernet	P	A line test is not supported.
	Link aggregation	P	The LACP functionality is not supported.
Layer 2 switching	MAC address learning	P	MAC address learning is not supported.
	VLAN	P	MAC VLANs are not supported. Also, VLAN ID 4094 cannot be used.
	VLAN tunneling	Y	None
	Tag translation	Y	
	Inter-port relay blocking functionality	Y	
	Layer 2 relay blocking functionality	Y	
	Spanning Tree Protocol	--	
	Ring Protocol	--	
	IGMP snooping	--	
	MLD snooping	--	
Filters	Flow detection mode	Y	None

Item		Support status	Remark
	Access lists	Y	
	QoS	Y	
Layer 2 authentication	IEEE 802.1X	--	None
	Web authentication	--	
	MAC-based authentication	--	
	Authentication VLAN	--	
Security	DHCP snooping	--	None
High reliability based on redundant configurations	GSRP	--	Can run as GSRP aware.
	VRRP	--	None
	Uplink redundancy	--	
High reliability based on network failure detection	IEEE 802.3ah/UDLD	Y	None
	Storm control	--	
	Layer 2 loop detection	Y	
	CFM	--	
Remote network management	SNMP	P	RMON is not supported. Some MIBs are not supported. For details, see *MIB Reference For Version 11.10*.
	Log output functionality	Y	None
	sFlow statistics	--	
Management of neighboring device information	LLDP	--	None
	OADP	--	
Port mirroring	Port mirroring	Y	None
Forwarding IPv4 packets	IPv4, ARP, and ICMP	Y	None
	Loopback interface	Y	
	Null interface	Y	
	Policy-based routing	--	
	DHCP relay functionality	Y	
	DHCP server functionality	--	
IPv4 routing protocols	Routing options	Y	None
	Route summarization	Y	
	Static routing	Y	
	RIP	Y	
	OSPF	Y	
	BGP4	Y	

Item		Support status	Remark
	Route filtering	Y	
	IPv4 multicast	Y	
Forwarding IPv6 packets	IPv6, NDP, and ICMPv6	Y	None
	Loopback interface	Y	
	Null interface	Y	
	RA	Y	
	IPv6 DHCP relay	--	
	IPv6 DHCP server functionality	--	
IPv6 routing protocols	Routing options	Y	None
	Route summarization	Y	
	Static routing	Y	
	RIPng	Y	
	OSPFv3	Y	
	BGP4+	Y	
	Route filtering	Y	
	IPv6 multicast	--	
Network partitioning	VRF	Y	None

Legend: Y: Supported, P: Partially supported, N: Not supported

7.2 Stack configurations

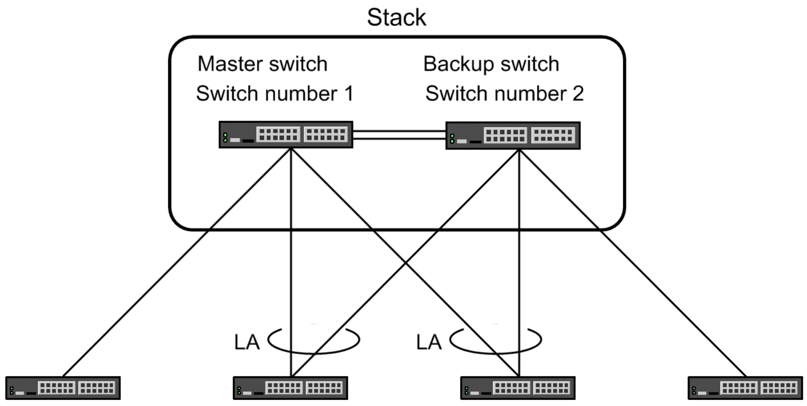
7.2.1 Stack configurations

Up to two member switches are allowed to make up a stack.

(1) Stack configuration with two member switches

The following figure shows an example of the stack configuration with two member switches.

Figure 7-2: Example of a stack configuration with two member switches



Legend: LA: Link aggregation

In a stack configuration, the master switch controls the other associated member switch to function as one virtual device.

We recommend configuring the link aggregation setting concerning the stack configuration for the respective member switches, which are the constituents of the configuration. The setting enables communication to be secured in case of a failure of a member switch.

If a failure takes place on a stack link and the failure disturbs communication between the member switches, the stack is separated and both the switches start functioning as a master switch. In that case, the switches might not be able to communicate with each other. To prevent the case, we recommend that you configure two stack links to make the stack line redundant.

(2) Stack configuration with one member switch

A stack is also configurable with only one member switch.

Even in the case where two member switches are used to configure a stack, a stack configuration with one member switch is expandable to that with two by first establishing a stack configuration with one member switch and then making a connection between the stack ports of the member switch and the associated member switch.

When a stack configuration with one member switch is employed from the beginning of system operation, it is possible to increase the number of available ports by adding devices without stopping communication during system operation.

7.2.2 Member switch models

The member switch configured as the master switch needs to be a model for member switches in which a stack configuration can be established. A model different from that of the master switch is also usable. However, the AX3800S does not allow the AX3650S to be configured as a member switch, and the AX3650S does not allow the AX3800S to be configured as a member switch.

The model of the local member switch is automatically configured at the time of startup. Concerning the other models of member switches, use the `switch provision` configuration command to configure them.

7.2.3 Conditions to configure the stack

When configuring the stack, all the following conditions need to be satisfied between the member switches:

- The switch numbers to be different.
- The optional licenses to be the same.
- The software types and versions to be the same.

If the optional licenses, software types, or software versions are not the same, the non-master member switch might repeatedly restart. After that, the member switch starts up with the default settings.

Even if the software types or software versions are inconsistent, a stack is configured when the configuration is the same. However, the configuration is not modifiable.

7.3 Basic stack functionality

7.3.1 Switch number

The switch number is used to identify the member switch in a stack configuration. The switch number is specific to the member switch and remains unchanged even after a stack configuration is established. For the switch number, 1 and 2 are specifiable.

To set a switch number, use the `set switch` operation command. The specified switch number is applied after the member switch restarts.

In a standalone configuration, the switch number is fixed at 1. Therefore, when a value other than 1 is specified by using the `set switch` operation command, the switch number is set to 1 after the switch restarts, if the stack functionality is not enabled.

7.3.2 Stack port and stack link

The stack port connects the member switches in a stack configuration, and two stack ports are available per member switch. On AX3800S switches, the SFP/SFP+ shared ports 37 to 44 and QSFP+ port are usable as the stack port.

The stack link connects the stack ports of the two member switches. The stack link must be a direct connection. Do not connect any network devices on the stack line connecting the stack ports of the two member switches.

The stack link is used for communication between the member switches. In order to secure a sufficient communication bandwidth between the member switches, we recommend that you use an interface that is capable of a bandwidth of 10 gigabits or more for the stack port. Note that AX3800S switches make the stack port functional only when a transceiver supporting a bandwidth of 10 gigabits or greater is used.

In a two-member-switch stack configuration, a stack link is required. We recommend using two stack links. With a redundant implementation of two stack links, the two member switches can guarantee operation through either link even if a failure occurs on one of the stack links.

While two stack links are operating normally, communication between the member switches are load-balanced on the stack links. In this case, if the stack links do not have the same communication performance, load balancing will likely cause packets to be discarded. When two stack links are routed, secure the same line speed by using a direct attachment cable and transceiver type (SFP/SFP+/QSFP+) of the same type for the stack ports.

To configure a stack port, use the `stack` parameter of the `switchport mode` configuration command.

For the Ethernet interface used for the stack port, only the following configuration commands are usable:

- bandwidth
- description
- no snmp trap link-status
- shutdown

Configuration commands other than those mentioned above will result in operations being performed when commands are omitted. However, be cautious that the following configuration commands do not result in operations being performed when commands are omitted:

- flowcontrol

  Both the send/receive operations are turned off.

- mtu

For the MTU, a stack-specific value is set. It is independent of the value set by the `system mtu` configuration command.

7.3.3 Switch states

This section describes switch states and the switch-state change process that occurs after a switch state transition.

(1) List of switch states

The following table describes a list of switch states. The letters indicate logs and command prompts and show the switch states.

Table 7-2: List of switch states

Switch states	Alphabet letter	Description
Initial state	I	State in which the device is in during which the switch state is determined to one of the following after it starts up: • Standalone • Master • Backup
Standalone	S	State in which the device is not in a stack configuration
Master	M	State in which the member switch is functioning for a stack configuration and controlling the other member switch.
Backup	B	State in which the member switch is functioning for a stack configuration and switches to the master switch if the current master switch becomes faulty.

(2) Change process after a switch state transition

When the switch state changes, the member switch performs either of the following processes to secure the correct operation of the switch after state transition:

- Initialization
- Switching

These processes are called change processes. The required change process type is different depending on the switch states before and after a transition. Change processing takes a while to run.

(a) Change processing when transitioning from the initial state to the master state

For a switch state transition from the initial state to the master state, the change process starts initialization for transmissions. The master switch being initialized does not connect to the associated member switch immediately after its stack port is connected to the member switch. It connects to the associated member switch after initialization finishes.

(b) Change process when transitioning from the initial state to the backup state

For a switch state transition from the initial state to the backup state, change processing starts initialization for transmissions. The backup switch being initialized restarts when the connection to the master switch is lost. Therefore, if the master switch stops or restarts while the backup switch is being initialized, transmission of packets is not guaranteed. A fully initialized backup switch replaces the master switch when the connection to the master switch is lost. Therefore, even when the connection to the master switch is lost after initialization is completed, the transmission of packets is guaranteed if the port of the backup switch is active.

For the backup switch being initialized, no operation commands can be executed from the master switch by using the `remote command` command. Execute operation commands after backup switch initialization ends.

(c) Change process when transitioning from the backup state to the master state

For a switch state transition from the backup state to the master state, change processing makes the switch ready for master switch option. The switch being switched to the master does not connect it to the associated member switch immediately after its stack port is connected to the member switch. It connects to the associated member switch after switching finishes.

7.3.4 Role and selection of the master switch

The master switch is a switch that controls the entire stack, and it is selected by its switch status, its master selection priority, and the chassis MAC address of the member switch.

The following describes the role of the master switch and how to select it.

(1) Role of the master switch

The master switch will control all the member switches that make up the stack and their functionality. The member switches making up the stack are used according to the configuration of and instructions from the master switch.

The master switch is the representative of the member switches, and the master switch is always logged in to when a remote terminal logs in to the stack.

The master switch that is logged in can perform following operations:

- Edit the configuration
- Operate all the member switches
- Check operation messages and operation logs for all member switches

(2) Selection of the master switch

The master switch is selected by the following conditions.

(a) If there is already a master switch

The existing master switch is selected as the master switch.

Even if a new member switch is connected to an operating stack via the stack port and booted, the existing master switch maintains the master status. By doing this, the new member switch can be added and the transfer functionality of the stack can be maintained.

As an exception, when the master selection priority of the master switch is 1, and if there is a member switch that has a master selection priority of 2 or higher, the member switch with master selection priority of 2 or higher will be selected as the master switch.

(b) If there is no master switch

The backup switch will be selected as the master switch.

(c) If there is no master switch and no backup switch

The member switch with the highest master selection priority will be selected as the master switch. If the master selection priority is same, the member switch with the lowest chassis MAC address will be selected as the master switch.

(d) If there are two master switches

The member switch with the highest master selection priority will be selected as the master switch. If the master selection priority is same, the member switch with the lowest chassis MAC address will be selected as the master switch.

(3) Example of selecting the master switch

The following are examples of selecting the master switch.

(Example 1) A member switch is added to the stack with one member switch

If there is only one member switch operating in the stack and it is operating as the master switch, the master status of the original master switch will be maintained when another member switch is started. Selection criterion (a) applies.

However, if the master selection priority of the original master switch is 1 and the master selection priority of the added member switch is 2 or higher, the added member switch will be selected as the master switch. The original master switch will be restarted, and it will become a member switch that is not the master switch of the stack.

(Example 2) When two member switches are started up simultaneously

When two member switches that are already connected via a stack port are simultaneously started up, the master switch is selected by comparing the master selection priorities and then the chassis MAC addresses. Selection criterion (c) applies.

(Example 3) When a master switch is connected to another master switch

When two stacks configured with one member switch each are connected, the master switch is selected by comparing the master selection priorities and then the chassis MAC addresses. Selection criterion (d) applies.

The member switch that was not selected as a master switch will restart, and gets added into the stack of the member switch that was selected as the master switch.

(4) Method to fix the selection of the master switch in a stack made up of two devices

There are the following two methods to set the selected member switch as a master switch when starting up all the member switches in a stack configured with two devices.

- Set the master selection priority of the member switch that is planned to become the master switch to 2 or higher, and set the master selection priority of the member switch that is not planned to become the master switch to 1.
- Start up the member switch planned to become the master switch first. Once it starts up as a master switch, start up the member switch that is not planned to become the master switch.

(5) Master selection priority

Master selection priority is a value used to select the master switch from the member switches making up a stack. Values from 1 to 31 can be set for the master selection priority using the `switch priority` configuration command.

The member switch with the higher master selection priority will be selected as the master switch when all the member switches making up the stack are started up simultaneously. However, if the member switch with the higher master selection priority is added to the stack with a master switch operating already, the existing master switch will maintain the master status if the master selection priority of the existing master switch is set to anything other than 1.

The master selection priority 1 is a special priority. When there are two members switches operating, and the master selection priority of one member switch is set to 1 and the master selection priority for the other member switch is set to 2 or higher, the member switch with the master selection priority of 2 or higher will always be selected as the master switch.

As an example, when a member switch with the master selection priority 2 or higher is added and started up in a stack configured with the master switch with the master selection priority 1, the added member switch will be selected as the master switch.

When the master switch is changed over, both the original master switch (the switch with master selection priority 1) and the added member switch will restart, meaning that communication will temporarily stop.

The member switch with the master selection priority set to 1 will not be selected as a master switch except for the following cases:

- When there is only one member switch configuring the stack

- When the master selection priority for all the member switches configuring the stack is set to 1

When adding a member switch to an existing stack, set the master selection priority of the member switch to be added to 1. This prevents the added member switch from becoming the master switch when the existing master switch is restarted due to a fault, and the configuration of the old master switch getting replaced by the configuration of the added member switch. When the stack is created, the master selection priority of the backup switch will be changed to the master selection priority set by the master switch.

7.3.5 Device MAC address of the stack

The chassis MAC address of the member switch that was selected as the master switch when the stack is first configured will be used as the device MAC address of the stack. If the backup switch becomes the new master switch due to fault in the master switch, the device MAC address of the stack will not change and the original device MAC address will be maintained.

If all the member switches are restarted simultaneously, the chassis MAC address of the member switch newly selected as the master switch will become the device MAC address of the stack.

7.4 Operation management of stack

(1) Configuration

(a) Member switch configuration

When using a stack, all the member switches making up the stack operate in the same configuration. Each member switch includes a startup configuration and a running configuration. A stack operates with the running configuration in the same state among all the member switches.

(b) Editing of running configuration

The running configuration in the stack configuration can be edited only in the master switch. The running configuration cannot be edited from a switch other than the master switch. The running configuration edited in the master switch is synchronized with the running configuration in the other member switch. When the `save` command is executed on the master switch, the running configurations of all the member switches are saved in each startup configuration.

(c) Flow up to synchronization with a member switch started later

If a member switch starts after a stack configuration is started, the system checks if the running configuration in the master switch matches the startup configuration in the member switch started after.

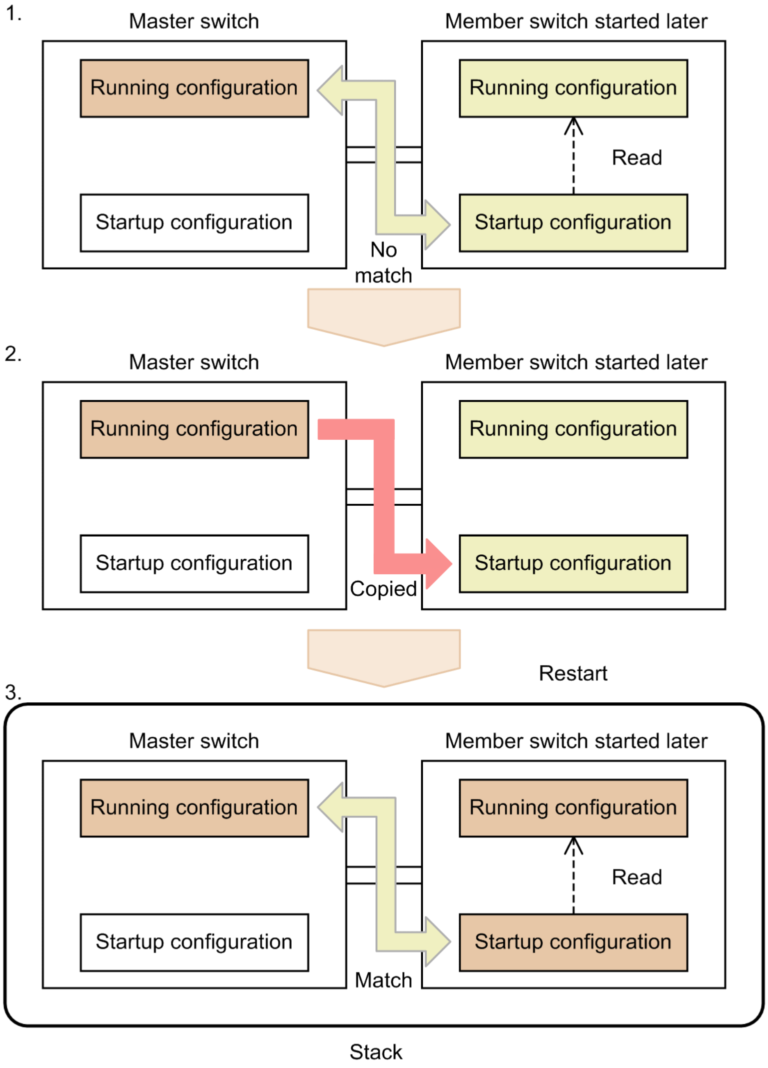
- If the configurations are the same

  The member switch started after will become part of the stack.

- If the configurations are different from each other

  The configurations are made to be matched in the procedure shown in the following figure, so that the member switch becomes part of the stack.

Figure 7-3: Flow for the configurations to match each other



1. The running configuration in the master switch does not match the startup configuration of the member switched started after.
2. The running configuration in the master switch is copied to the startup configuration in the member switch, and then the member switch is restarted.
3. The running configuration in the master switch matches the startup configuration in the restarted member switch, so the member switch operates with a running configuration synchronized with the running configuration in the master switch.

(2) Execution of operation commands

When using stack, users can use the `remote command` operation command to execute an operation command for the member switch specified from the master switch.

For example, in the case of the functionality that aggregates information into the master switch, executing the `show` command, which displays information, on the master switch displays the information of all the member switches. However, in the case of functionality that has information per member switch, executing the `show` command in the master switch displays the information of only the master switch. To display the information of member switches other than the master switch, use the `remote command` operation command to specify the switch number of the target member switch and the `show` command.

Note the following points when you execute the `remote command` operation command:

- A member switch other than the master switch cannot execute the operation command for the other member switches.
- The `remote command` operation command can be executed for the member switches whose initialization has been completed. The execution is unavailable for the member switch being initialized. In such a case, execute the command again after the initialization is completed.
- To continuously execute an operation command containing the `remote command` operation command, wait for a prompt to appear after the `remote command` operation command is finished, and then execute the next operation command. If you enter the operation command containing the `remote command` operation command by copying and pasting it, and then execute it, the operation commands following the `remote command` operation command might not be executed. In such a case, re-enter the ignored operation commands for execution.

(3) User account

When using a stack, the user account of a member switch other than the master switch synchronizes with the user account of the master switch. Therefore, the user accounts in member switches other than the master switch will be deleted when a stack is configured. Note that the files under the home directory are not synchronized.

(4) Login to a member switch

When using a stack, a console is connected in order to log in to a member switch.

You can identify the member switch logged in to by checking the command prompt. For example, if `OFFICE1` has been set by the `hostname` configuration command and if switch No. 1 and No. 2 are the master switch and the backup switch, respectively, the command prompts are as follows:

- The master switch's command prompt: `OFFICE1>`
- The backup switch's command prompt: `OFFICE1-02B>`

The characters after the hyphen (`-`) of the backup switch's command prompt represent the switch number (two characters) and the switch status (one character).

Note that you cannot log in to the member switch started later until the master switch is connected to the started member switch. If you cannot log in to the member switched started later, wait for the command prompt for logging in to appear.

To log in from a remote operation terminal, log in to the master switch.

(5) Time of a member switch

The time of member switches other than the master switch synchronizes with the time of the master switch. However, the time is synchronized by seconds, so difference between member switches might occur.

Executing the `set clock` operation command in the master switch causes the time of the other member switches to be synchronized within a minute.

(6) Software management

(a) Software updates

For software updates, update the member switch of either the backup or the master switch and wait for its port to be up, and then update the other. We recommend updating the backup switch first, and then the master switch.

Execute the `show switch` operation command to check that the update is completed. If the initialization of the updated member switch is completed, the update is also completed. Also, execute the `show port` operation command to check that the port is up.

(b) Software upgrades

When changing the member switch of L3S Light Software to that of L3S Advanced Software, upgrade the member switch of either the backup or the master switch and wait for its port to be up, and then upgrade the other. We recommend updating the backup switch first, and then the master switch.

Execute the `show switch` operation command to check that the upgrade is completed. If the initialization of the upgraded member switch is completed, the upgrade is also completed. Also, execute the `show port` operation command to check that the port is up.

(c) Optional license

When setting the optional license and then applying it by restarting the switches, we recommend restarting the backup switch first and then the master switch.

Note that if it takes long time from the backup switch restart time to the master switch restart time, a stack might not be able to be configured.

(7) Backup and restoration of operating information

The target of backups and restorations includes information called the stack information file specific to each member switch.

(8) Operation messages and logs

The event information that has occurred in member switches is displayed as operation messages on the operation terminal of each member switch, and also saved as the operation logs in each member switch.

Among the information, failure and event information (log type ERR and EVT) related to the switches are also notified to the master switch. That is, the information about switch-related failures and events that have occurred in all the member switches is displayed as operation messages on the operation terminal of each member switch, and also saved as the operation logs in the master switch. In addition, these logs can be output to a server on the network by using the `syslog` interface.

Note that the formats of the operation message and the log include the switch number and the switch status. This enables users to identify the member switch with the event and its status.

(9) MIB and traps

When using a stack, like a standalone configuration, users can set SNMP to obtain or set MIB and output traps.

7.5 Stack operation at the time of fault and recovery

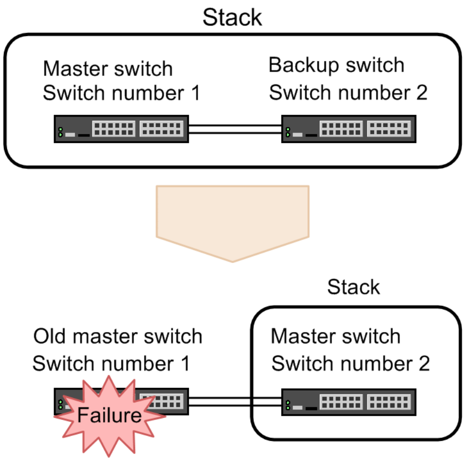
This section describes the stack operation at the time of a fault and recovery.

7.5.1 Failure and recovery of member switch

(1) Master switch fault

The following figure shows the operation when a fault occurs in the master switch.

Figure 7-4: Master switch fault

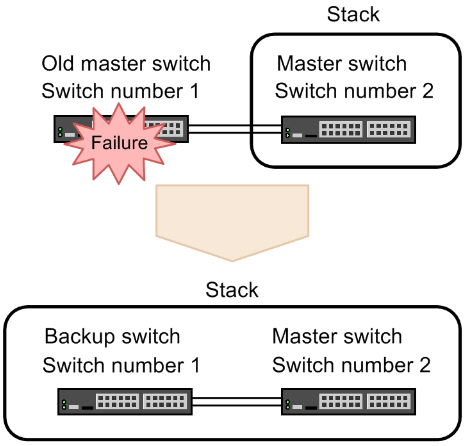


If the master switch stops due to a fault, the backup switch serves as a new master switch and operates in the stack with one master switch. In this case, the MAC address of the switch is not changed.

(2) Recovery of an old master switch

The following figure shows the operation when the old master switch is recovered from the fault.

Figure 7-5: Recovery of the old master switch

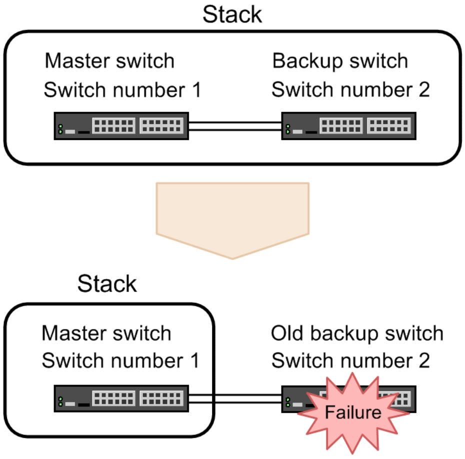


When the old master switch is recovered from the fault, this member switch serves as the backup switch and the switches operate in the stack with two member switches. In this case, the MAC address of the switch is not changed.

(3) Backup switch fault

The following figure shows the operation when a fault occurs in the backup switch.

Figure 7-6: Backup switch fault

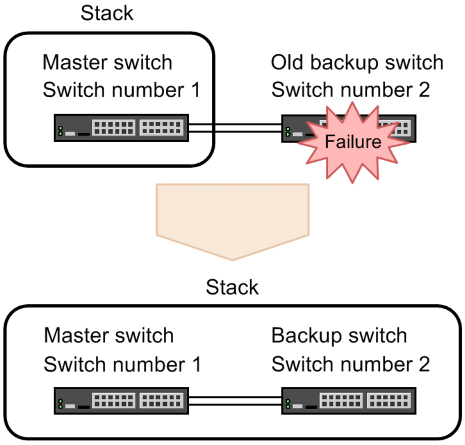


If the backup switch stops due to a fault, the switch operates in the stack with one master switch. In this case, the MAC address of the switch is not changed.

(4) Recovery of an old backup switch

The following figure shows the operation when the old backup switch is recovered from the fault.

Figure 7-7: Recovery of the old backup switch



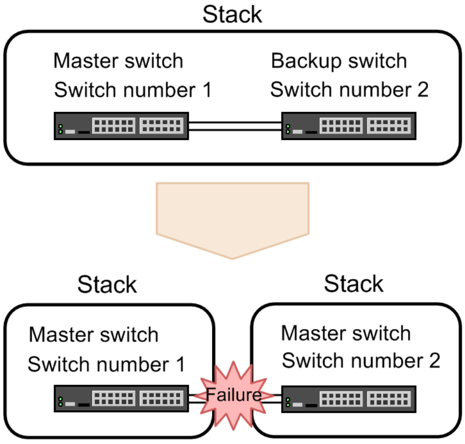
When the old backup switch is recovered from the fault, this member switch serves as the backup switch and the switches operate in the stack with two member switches. In this case, the MAC address of the switch is not changed.

7.5.2 Fault and recovery of stack link

(1) Stack link fault

The following figure shows the operation when a fault occurs in all stack links.

Figure 7-8: Fault in the stack link



If a fault occurs in all the stack links, the master switch and the backup switch cannot recognize the member switches adjacent to each other. As a result, one stack divides into two stacks, and the switches operate under the situation where the master switch remains as the master switch and the backup switch serves as a new master switch.

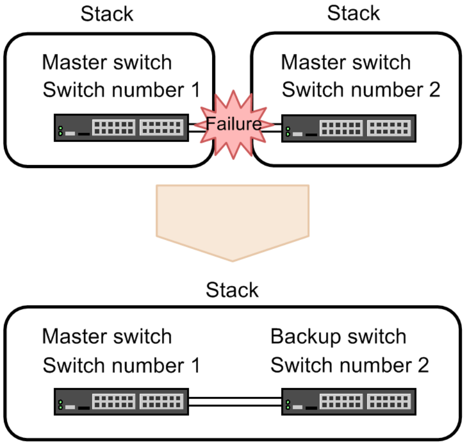
In this case, these two stacks use the same IP address and the switch MAC address, resulting in a communication failure due to address duplication.

When there are two stack links, even if either of the stacks fails, operation continues with the other. However, a fault in the remaining stack link causes the stack to divide into two stacks. Therefore, if a fault occurs in either of the stack links, immediately recover it from the fault.

(2) Recovery of stack link

The following figure shows the operation when the stack link is recovered from the fault.

Figure 7-9: Recovery of the stack link



When the stack link is recovered from the fault, the member switches divided into two stacks recognize each other and operate as one stack.

7.5.3 Switching communication between member switches

By configuring a stack, you can switch the communication in a short time in the case of a fault or recovery of a member switch. To switch the communication in a short time, use the function that supports the short-time communication switching in the stack. The following table describes the support status of short-time communication switching in the stack by using functionality.

Table 7-3: Support status of short-time communication switching in the stack

Category	Functionality	Supported
Network interfaces	Ethernet	Y
Link aggregation	Static	Y
	Standby link link-down mode	N
	Standby link non-link-down mode	Y
	Mixed-speed mode	N
Layer 2 forwarding	MAC address learning	Y
	Port VLAN	Y
	Protocol VLAN	Y
	Tag translation	Y
	VLAN tunneling	Y
Filters and QoS	Filters	Y
	QoS	Y
High-reliability functionality	IEEE 802.3ah/UDLD	Y
	Layer 2 loop detection	Y
IPv4 packet forwarding#	IPv4, ARP	Y
	DHCP relay	Y
IPv4 unicast routing protocol	Static routing	Y
	RIP	N
	OSPF	N
	BGP4	N
IPv4 multicast routing protocol	PIM-SM	N
	PIM-SSM	N
IPv6 packet forwarding#	IPv6, NDP	Y
IPv6 unicast routing protocol	Static routing	Y
	RIPng	N
	OSPFv3	N
	BGP4+	N

Legend: Y: Supported; N: Not supported

#

The software forwarding of the IPv4/IPv6 packets and IPv4/IPv6 communication with the Switch do not support short-time communication switching.

Note that the following cases take time to switch communication:

- The link-down or link-up detection time of a line connected to the stack is not 0 seconds.

In this case, the detection times of both of the stack and the partner switch are affected.

- For connection with other switches, link aggregation connected to multiple member switches is not used. Examples are as follows:
    - Only one member switch is connected to other switches.
    - Multiple lines connected to other switches are not aggregated by using link aggregation.

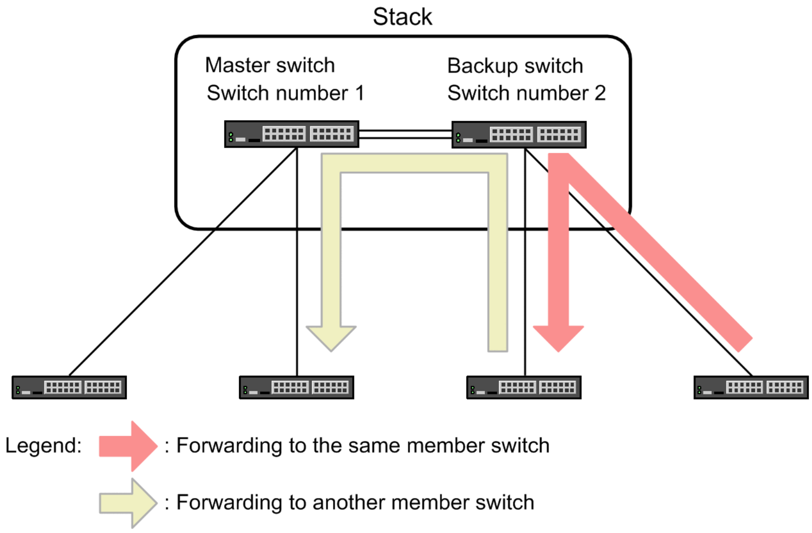
7.6 Stack forwarding

7.6.1 Physical port forwarding

(1) Forwarding under normal conditions

If the received port and the forwarding destination port are in the same member switch, the port is forwarded within the member switch. If each of the received port and the forwarding destination port is in different member switches, the port is forwarded via a stack link. The following figure shows the forwarding operation under normal conditions at the physical port.

Figure 7-10: Forwarding under normal conditions (physical port)


Stack
Master switch
Switch number 1
Backup switch
Switch number 2
Legend:
: Forwarding to the same member switch
: Forwarding to another member switch

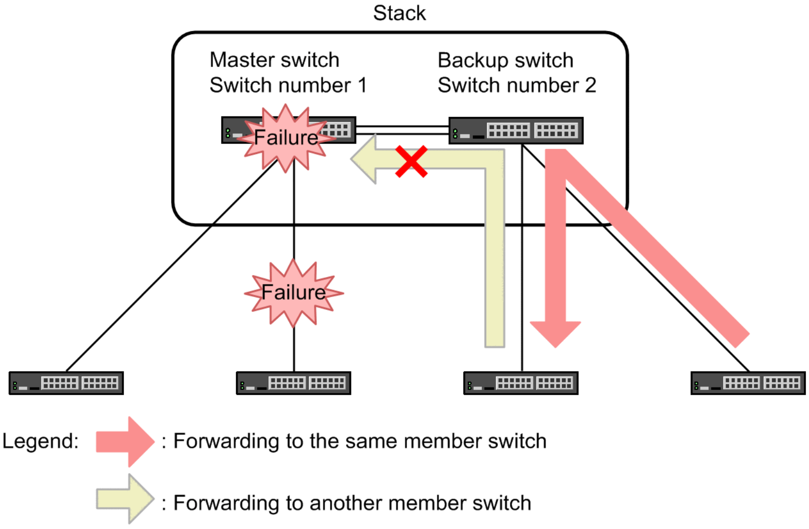
(2) Forwarding in the case of a fault

In this configuration, the paths have not been made redundant. Therefore, if each of the received port and the forwarding destination port is in different member switches, forwarding cannot continue in the following situations:

- A fault occurs in the path to the forwarding destination of the other member switch.
- A fault occurs in the other member switch.

The following figure shows the forwarding operation in the case of a fault at the physical port.

Figure 7-11: Forwarding in the case of a fault (physical port)



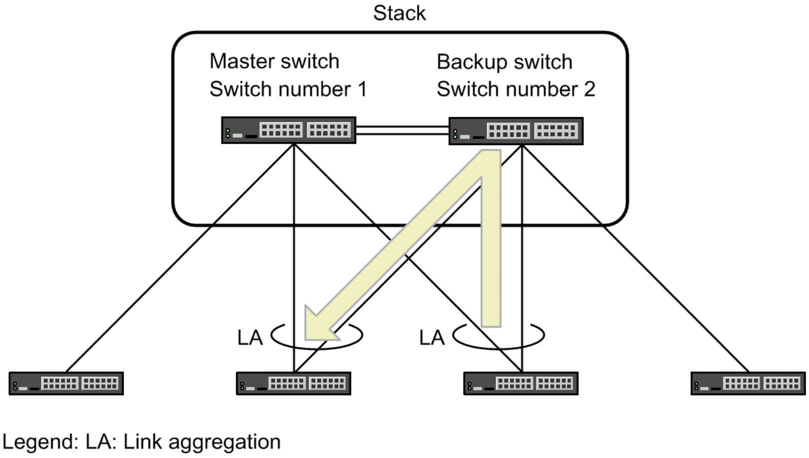
To continue the forwarding operation in such a case, we recommend using link aggregation in the stack.

7.6.2 Link aggregation forwarding

(1) Forwarding under normal conditions

If the link aggregation connected to multiple member switches is the forwarding destination, the received port of a member switch is given priority as the forwarding destination. The following figure shows the forwarding operation under normal conditions with link aggregation.

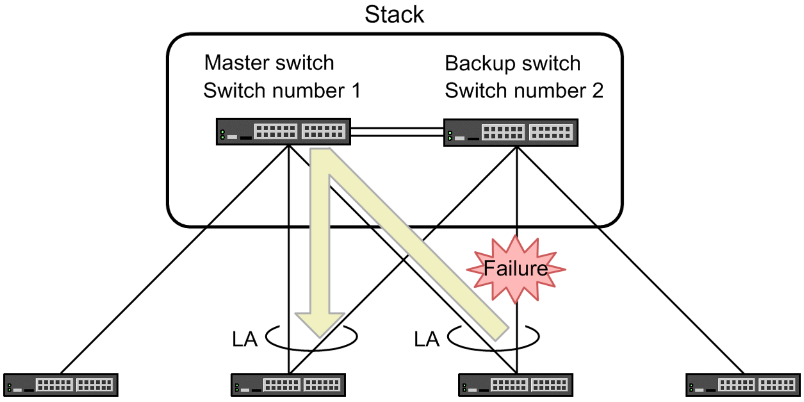
Figure 7-12: Forwarding under normal conditions (link aggregation)



(2) Forwarding in the case of a fault at the source port

With link aggregation, if the member switch to be received is changed due to a fault at the source port, the port of the received member switch is given priority as the forwarding destination. The following figure shows the forwarding operation under normal conditions with link aggregation.

Figure 7-13: Forwarding in the case of a fault at the source port (link aggregation)

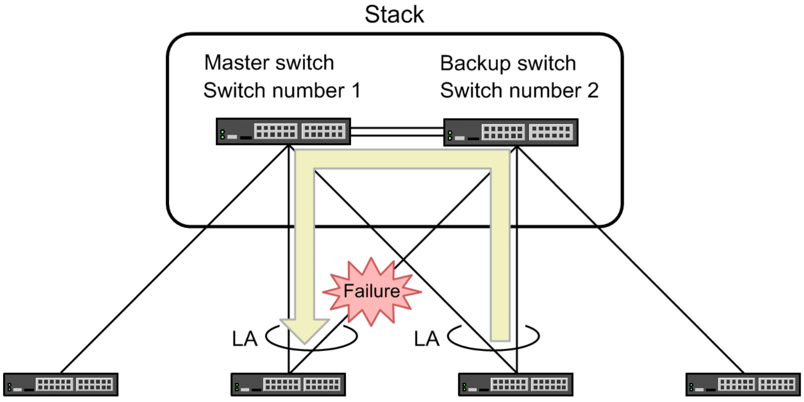


Legend: LA: Link aggregation

(3) Forwarding in the case of a fault at the destination port

When using link aggregation, if the received member switch has no port due to a fault at the destination port, the forward destination is switched to the port of the other member switch via the stack link. The following figure shows the forwarding operation in the case of a fault at the destination port with link aggregation.

Figure 7-14: Forwarding in the case of a fault at destination port (link aggregation)



Legend: LA: Link aggregation

7.7 Prohibited configuration and notes on the stacks

7.7.1 Prohibited stack configurations

(1) Number of member switches

Up to two member switches can be configured for a stack.

A stack cannot be configured with three or more member switches. Also, do not connect two different member switches to one member switch via a stack port.

(2) Stack link

Directly connect the stack link via a line. Do not connect other network devices between the stack ports connecting two member switches. Operation of the stack is not guaranteed when network devices such as Layer 2 switches, hubs, media converters, etc., are connected to the stack port.

7.7.2 Notes on stacks

(1) Operation of the configuration file

- The `erase configuration` operation command cannot be executed.

  To reset the configuration to the default, perform the procedure detailed in *8.1.7 Switching the operating mode to standalone*, and then execute the `erase configuration` command.

- The `copy` operation command cannot be used to copy the running configuration file.

  To change the running configuration file, use the `copy` command to copy the startup configuration, and then restart the member switch.

- When operating in standalone mode, the configuration file with the `stack enable` configuration command set cannot be copied to the running configuration file with the `copy` operation command.

  To copy the configuration file to the running configuration file, perform the procedure detailed in *8.1.2 Configuring a stack with standalone switches*, and then execute the `copy` command.

- The configuration cannot be edited when the software type and version do not match between member switches.

(2) Configurations that require the restarting of the device or the VLAN program

When a configuration is edited that requires a restart of the device or the VLAN program to apply the changes, all member switches must be restarted for a stack as well. Edit the configuration, save the changes to the startup configuration using the `save` command, and then restart all the member switches. For details on how to restart member switches, see *8.2.5 Restarting a stack*.

This applies to following configuration commands:

- ip route static maximum-paths
- ipv6 route static maximum-paths
- limit-queue-length
- maximum-paths
- swrt_table_resource
- system flowcontrol off
- system l2-table mode

Out of these commands, the `ip route static maximum-paths`, `ipv6 route static maximum-paths`, and `maximum-paths` commands require the restarting of all member switches only when a warning level operation message is output after editing the configuration. For details, see *7.4.2 Load balancing specifications* in the manual *Configuration Guide Vol. 3 For Version 11.10*.

When all the member switches are not restarted and only the member switch that the change was made to is restarted, the new configuration is applied to only the restarted member switch.

As an example, when the configuration is changed in a table entry with the following configuration command, member switches will operate with different table entries when only the member switch with the changed configuration is restarted:

- ip route static maximum-paths
- ipv6 route static maximum-paths
- maximum-paths
- swrt_table_resource
- system l2-table mode

When this happens, the number of table entries that operation is guaranteed for is the limit of the switch with the smallest limit. To confirm the table entries of each member switch, execute the `show system` operation command.

(3) Packet transfers when IPv4 multicasting is used

When IPv4 multicasting is used with a stack, the packets targeted for forwarding at a corresponding forwarding entry might be discarded instead of executing a Layer 2 transfer during the change of a multicasting forwarding entry. Also, when the negative cache of multicast forwarding is changed, the packets targeted for Layer 3 discarding might be discarded instead of executing a Layer 2 transfer for the corresponding negative cache.

(4) Flow control

Flow control does not work for stack ports.

Even if the reception buffer is depleted on a particular member switch in a stack using flow control, the buffer in other member switch might not be depleted. So, even if the reception buffer is depleted due to an outgoing packet being held in the member switch, a pause packet will not be transmitted from other member switches.

(5) MAC address learning

In a stack, each member switch will learn MAC addresses individually. It may take up to 180 seconds for an AX3800S series switch, and up to 160 seconds for an AX3650S series switch to apply the results of MAC address learning to a particular member switch. To make the operation of MAC address learning stable, we recommend that you not set the aging time of the MAC address learning shorter than the default 300 seconds.

There are the following two restrictions for each member switch to perform MAC address learning individually.

(a) Restriction regarding detecting a move for MAC address learning

When a terminal such as a PC is moved from the port of a particular member switch to a different port, the member switch at the PC destination will detect the movement, and the MAC address that was learned after the movement will be reflected in the MAC address table of each member switch. However, the following restrictions might apply depending on the number of moved terminals or the frequency of movement:

- When many terminals are moved at once, the MAC address port that was known before the movement might remain in the MAC address table of the member switch (with the exception of the destination). In such conditions, communication might not be performed correctly because the frame is sent to the port before the move.

- When the MAC address is learned close to the capacity of the MAC address table for AX3800S series switches, and a large number of terminals are moved in sequence, the MAC addresses learned by each member switch might not be applied to other member switches within the above time, causing a flooding of frames with MAC addresses not being applied at the destination.

In such cases, wait until the MAC addresses newly learned by each member switch are applied to the other member switches.

(b) Restrictions regarding unicast transmissions

When there are two terminals connected to separate member switches performing unicast transmissions between these two terminals, flooding of unicast transmissions from either terminal into the VLAN might occur. In such cases, wait until one of following conditions is met:

- Multicast packets or broadcast packets are sent from the terminal that was the destination of the frame that was flooded.
- The MAC addresses learned at each member switch are applied to the other member switches.

(6) Diverting a member switch that was used in a stack

The chassis MAC address of the master switch at the time of configuring the stack for the first time will become the device MAC address of the stack. The device MAC address will not change even if there is a fault in the master switch.

Therefore, when removing the member switch that was used in the stack from the stack and connecting this device to the same network with the corresponding stack, confirm that the chassis MAC address of the removed member switch is different from the device MAC address of the stack. If it is the same, change the device MAC address of the stack by restarting the stack after removing the corresponding member switch from the stack.

For details about the device MAC address of the stack, see *7.3.5 Device MAC address of the stack*. For details about restarting the stack, see *8.2.5 Restarting a stack*.

(7) When downgrading the software version

When downgrading the version of a member switch that was used in the stack to a version that does not support the stack function (ver. 11.10 or earlier for AX3800S series switches, and ver. 11.8 or earlier for AX3650S series switches), return the switch to a standalone configuration before downgrading the version. This is because the configuration might not be possible to edit after downgrading the version.

For details on how to return the switch to a standalone configuration, see *8.1.7 Switching the operating mode to standalone*.

If the version is downgraded to a previous version (ver. 11.10 or earlier for AX3800S series switches, and ver. 11.8 or earlier for AX3650S series switches) with the stack configuration still set, execute the `erase configuration` operation command to return to configuration to its initial state.

(8) Switching over the master switch

When switching over the master switch with packet transfers continuing, perform the switchover after confirming both of following are met:

- Initialization of the backup switch is completed.
- The port of the backup switch is running.

When the master switch is switched over during the initialization of the backup switch, the backup switch that is initializing will restart, so the transferring of the packets will not be able to continue.

Whether initialization of the backup switch is completed or not can be confirmed with the `show switch` operation command. Whether the port is running can be confirmed with the `show port` operation command.

(9) Using the master selection priority 1

When a stack configured with one member switch with the master selection priority set to 2 or higher is connected to a stack configured with one member switch with a master selection priority of 1, the member switch with the master selection priority set to 2 or higher will be selected as the master switch. The member switch with the master selection priority set to 1 will restart, and will be added to the stack as the backup switch. The member switch with the master selection priority set to 2 or higher will continue to keep the master status without restarting, so the transfer function of the stack will be maintained.

However, if the member switch with the master selection priority set to 2 or higher is connected to the stack configured with one member switch with a master selection priority of 1 and started, the member switch with the master selection priority set to 2 or higher will detect the master switch, and wait for backup transfer instructions from the master switch in the default status. At the same time, the member switch with the master selection priority 1 will detect the member switch with the master selection priority set to 2 or higher, and will restart. The member switch waiting for the backup transfer instructions will detect the absence of the master switch, so it will restart. Communication will be disconnected until the member switch with the master selection priority set to 2 or higher completes initialization as the master switch.

As shown above, the time of a communication disconnection might become longer at the time of a switchover of the master switch when a master selection priority of 1 is used.

Only use the master selection priority 1 temporarily to prevent the unintended replacement of the configuration when a member switch is added to an existing stack. We do not recommend fixing the selection of a master switch using the master selection priority 1 during normal operation. We recommend that you operate with a master selection priority of 2 or higher after configuring the stack.

Chapter

8. Settings and Operation for Stack Functionality

This chapter describes stack operations.

8.1 Configuring a stack

This section describes how to use configuration commands and operation commands to configure a stack, and how to switch the operating mode from stack mode to standalone mode.

8.1.1 List of configuration commands and operation commands

The following table describes the configuration commands for a stack.

Table 8-1: List of configuration commands

Command name	Description
stack enable	Enables the stack functionality.
switch priority	Sets the master selection priority.
switch provision	Sets the model of a member switch that configures a stack.
switchport mode#	Sets a port used for connecting the member switches that configure a stack.

#

For details, see *13. VLANs* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.

The following table describes the operation commands used to configure a stack.

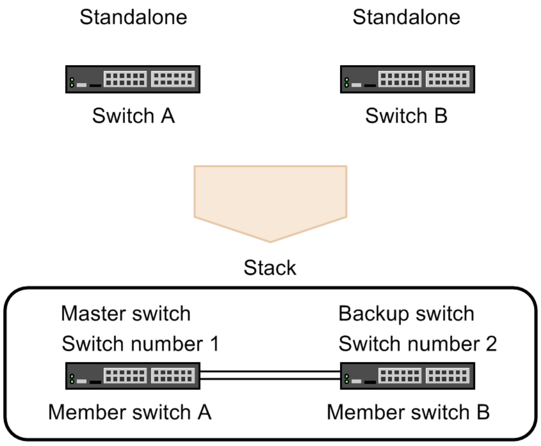
Table 8-2: List of operation commands (for configuring a stack)

Command name	Description
set switch	Sets the switch number of a member switch.

8.1.2 Configuring a stack with standalone switches

As shown in the following figure, a stack is configured with Switches A and B, which operate in standalone mode.

Figure 8-1: Configuring a stack with standalone switches



The following table describes how to configure a stack with standalone switches.

Table 8-3: Flow for configuring a stack with standalone switches

Operational flow and description	Target switch
(1) Checking the optional licenses and software installed on Switch A and Switch B • Checking the optional licenses • Checking the software	Switch A (member switch A) Switch B (member switch B)
(2) Switching Switch A to operate as the member switch with switch number 1 in a stack with one member switch • Enabling the stack functionality • Restarting the switch	Switch A (member switch A)
(3) Setting the configurations of member switch A and member switch B • Setting the stack ports of member switch A • Setting the master selection priority of member switch A • Setting the model of member switch B • Setting the stack ports of member switch B • Setting the master selection priority of member switch B	Switch A (member switch A)
(4) Switching Switch B to operate as the member switch with switch number 2 in a stack with one member switch • Setting the switch number • Enabling the stack functionality • Restarting the switch	Switch B (member switch B)
(5) Setting the configuration of member switch B to connect with member switch A • Setting stack ports • Setting the master selection priority to 1	Switch B (member switch B)
(6) Switching member switch A and member switch B to operate in a stack with two member switches • Connecting the switches through stack ports	--

Legend: --: Not applicable

(1) Checking the optional licenses and software installed on Switch A and Switch B

Check the optional licenses and the type and version of the software on Switch A and Switch B.

If the optional licenses differ between Switch A and Switch B, add or delete optional licenses so that the optional licenses are the same. If the type and version of the software differ between Switch A and Switch B, update the software so that the type and version are the same.

Procedure

1. `# show license`

   ```
   Date 20XX/10/26 12:00:00 UTC
     Available: -----
       ----------------
   ```

   On Switch A, check the optional licenses.

2. `# show version software`

   ```
   Date 20XX/10/26 12:01:00 UTC
   S/W: OS-L3SA Ver. 11.8
   ```

   On Switch A, check the software type and version.

3. `# show license`

   ```
   Date 20XX/10/26 13:00:00 UTC
   ```

```
  Available: -----
    ----------------
```

On Switch B, check the optional licenses. Check that the optional licenses are the same as those for Switch A that were checked in step 1.

4.
```
# show version software
Date 20XX/10/26 13:01:00 UTC
S/W: OS-L3SA Ver. 11.8
```

Check the software type and version on Switch B. Check that the software type and version are the same as those for Switch A that were checked in step 2.

(2) Switching Switch A to operate as the member switch with switch number 1 in a stack with one member switch

Enable the stack functionality on Switch A.

Points to note

Use the `stack enable` command to enable stack operations. You must restart the Switch to apply the settings configured by using the `stack enable` command. Because of this, set the `stack enable` command before starting system operation. In addition, you cannot edit any configurations from the time when the `stack enable` command is set until the Switch restarts.

Note that the following configurations are automatically set when the `stack enable` command is set:

- spanning-tree disable
- no service ipv6 dhcp

Therefore, before setting the `stack enable` command, check that the Switch does not use functionality that is not supported in stack mode (such as Spanning Tree Protocols and the IPv6 DHCP server functionality).

Command examples

1.
```
(config)# stack enable
After this command execute, please save configuration editing
now in startup-config, and please reboot a device.
Do you wish to continue ? (y/n):
```

Switches the operation mode of the Switch to stack mode. When a message confirming the configuration change appears, enter `y`.

2.
```
(config)# save
(config)# exit
```

Saves the configuration, and then returns to administrator mode from configuration command mode.

3.
```
# reload
```

Restarts the Switch. After the Switch restarts, it operates as the member switch of a stack with one member switch.

(3) Setting the configurations of member switch A and member switch B

On member switch A, set the configurations of all switches to be operated in a stack as member switches.

Points to note

The configuration of member switch B, which operates as the backup switch, is synchronized with that of member switch A, which operates as the master switch. Therefore, you must configure the following on member switch A:

- Stack ports of member switch A
- The master selection priority of member switch A
- The model of member switch B
- Stack ports of member switch B
- The master selection priority of member switch B

When you set the model of member switch B, the configurations of the Ethernet interfaces associated with the specified model are established automatically. Set the master selection priority of member switch A to a value larger than the master selection priority set for member switch B.

Command examples

1.
   ```
   (config)# interface tengigabitethernet 1/0/25
   (config-if)# switchport mode stack
   (config-if)# exit
   (config)# interface tengigabitethernet 1/0/26
   (config-if)# switchport mode stack
   (config-if)# exit
   ```
   Configures stack ports for an Ethernet interface of member switch A (switch number 1).

2.
   ```
   (config)# switch 1 priority 20
   ```
   Sets the master selection priority of member switch A (switch number 1) to 20.

3.
   ```
   (config)# switch 2 provision 3650-24t6xw
   ```
   Sets the model of the Switch to be used as member switch B. Here, the model is AX3650S-24T6XW.

4.
   ```
   (config)# interface tengigabitethernet 2/0/25
   (config-if)# switchport mode stack
   (config-if)# exit
   (config)# interface tengigabitethernet 2/0/26
   (config-if)# switchport mode stack
   (config-if)# exit
   ```
   Configures stack ports for an Ethernet interface of member switch B (switch number 2).

5.
   ```
   (config)# switch 2 priority 10
   ```
   Sets the master selection priority of member switch B (switch number 2) to 10.

6.
   ```
   (config)# save
   (config)# exit
   ```
   Saves the configuration, and then returns to administrator mode from configuration command mode.

(4) Switching Switch B to operate as the member switch with switch number 2 in a stack with one member switch

Set the switch number of Switch B to 2, and then enable the stack functionality.

Points to note

Set the switch number of Switch B to 2. Then, use the `stack enable` command to enable stack operations, and restart the Switch.

Command examples

1.
```
# set switch 2
```
Sets the switch number to 2.

2.
```
(config)# stack enable
After this command execute, please save configuration editing
now in startup-config, and please reboot a device.
Do you wish to continue ? (y/n):
```
Switches the operation mode of the Switch to stack mode. When a message confirming the configuration change appears, enter `y`.

3.
```
(config)# save
(config)# exit
```
Saves the configuration, and then returns to administrator mode from configuration command mode.

4.
```
# reload
```
Restarts the Switch. After the Switch restarts, it operates as the member switch of a stack with one member switch.

(5) Setting the configuration of member switch B to connect with member switch A

Configure the settings that are essential for member switch B to connect with member switch A in a stack.

Points to note

Set the master selection priority of member switch B to 1. This means that member switch B will not operate as the master switch, even if member switch A restarts because of a failure when member switch B is connected with member switch A.

Note that the configuration set here is overwritten by that in member switch A, which operates as the master switch.

Command examples

1.
```
(config)# interface tengigabitethernet 2/0/25
(config-if)# switchport mode stack
(config-if)# exit
(config)# interface tengigabitethernet 2/0/26
(config-if)# switchport mode stack
(config-if)# exit
```
Configures stack ports for an Ethernet interface of member switch B (switch number 2).

2.
```
(config)# switch 2 priority 1
```
Sets the master selection priority of member switch B (switch number 2) to 1.

3.
```
(config)# save
(config)# exit
```
Saves the configuration, and then returns to administrator mode from configuration command mode.

(6) Switching member switch A and member switch B to operate in a stack with two member switches

Connect member switch A and member switch B, each of which is operating as the member switch in a stack with one member switch, to configure a stack with two member switches.

Because the master selection priority of member switch B is 1 here, member switch A continues to operate as the master switch, and member switch B automatically restarts.

After restarting, member switch B automatically restarts again to synchronize its configurations with those of member switch A. Member switch A then operates as the master switch and member switch B as the backup switch in a stack.

Procedure

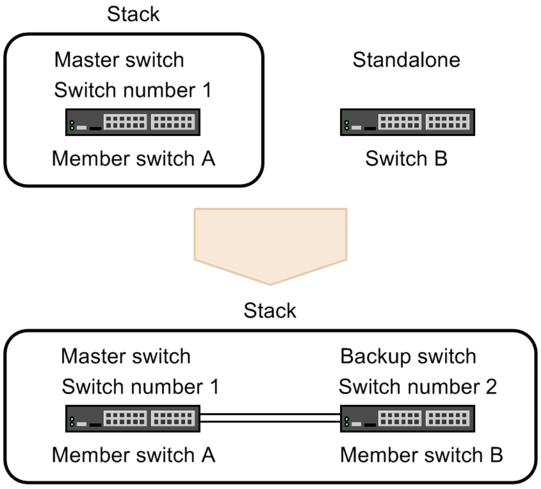
1. Connect member switch A and member switch B through their stack ports.

2.
```
# show switch detail
```
Execute the `show switch detail` operation command to check that member switch A operates as the master switch and that member switch B operates as the backup switch in a stack.

8.1.3 Adding a member switch

As shown in the following figure, Switch B operating in standalone mode is added to the stack configured by member switch A only.

Figure 8-2: Adding a member switch



The following table describes how to add a member switch.

Table 8-4: Flow for adding a member switch

Operational flow and description	Target switch
(1) Checking the optional licenses and software installed on member switch A and Switch B • Checking the optional licenses • Checking the software	Member switch A Switch B (member switch B)

Operational flow and description	Target switch
(2) Setting the configuration of member switch B • Setting the model of member switch B • Setting the stack ports of member switch B • Setting the master selection priority of member switch B	Member switch A
(3) Switching Switch B to operate as the member switch with switch number 2 in a stack with one member switch • Setting the switch number • Enabling the stack functionality • Restarting the switch	Switch B (member switch B)
(4) Setting the configuration of member switch B to connect with member switch A • Setting stack ports • Setting the master selection priority to 1	Switch B (member switch B)
(5) Switching member switch A and member switch B to operate in a stack with two member switches • Connecting the switches through stack ports	--

Legend: --: Not applicable

(1) Checking the optional licenses and software installed on member switch A and Switch B

Check the optional licenses and the type and version of the software on member switch A, which is operating in a stack, and Switch B, which is to be added to the stack.

If the optional licenses differ between Switch A and Switch B, add or delete optional licenses so that the optional licenses are the same. If the type and version of the software differ between Switch A and Switch B, update the software so that the type and version are the same.

Procedure

1.
```
# show license
Date 20XX/10/26 12:00:00 UTC
  Available: -----
    ----------------
```
On member switch A, check the optional licenses.

2.
```
# show version software
Date 20XX/10/26 12:01:00 UTC
S/W: OS-L3SA Ver. 11.8
```
On member switch A, check the software type and version.

3.
```
# show license
Date 20XX/10/26 13:00:00 UTC
  Available: -----
    ----------------
```
On Switch B, check the optional licenses. Check that the option licenses are the same as those for member Switch A in step 1.

4.
```
# show version software
Date 20XX/10/26 13:01:00 UTC
S/W: OS-L3SA Ver. 11.8
```

On Switch B, check the software type and version. Check that the software type and version are the same as those checked for member switch A in step 2.

(2) Setting the configuration of member switch B

On member switch A, set the configuration of member switch B, which is to be added. Here, the master selection priority and stack ports have been set for member switch A as shown below.

```
switch 1 priority 20
!
interface tengigabitethernet 1/0/25
  switchport mode stack
!
interface tengigabitethernet 1/0/26
  switchport mode stack
```

Points to note

The configuration of member switch B, which operates as the backup switch, is synchronized with that of member switch A, which operates as the master switch. Therefore, you must configure the following on member switch A:

- The model of member switch B
- Stack ports of member switch B
- The master selection priority of member switch B

When you set the model of member switch B, the configurations of the Ethernet interfaces associated with the specified model are established automatically. Set the master selection priority of member switch A to a value larger than the master selection priority set for member switch B.

Command examples

1. `(config)# switch 2 provision 3650-24t6xw`

   Sets the model of the Switch to be used as member switch B. Here, the model is AX3650S-24T6XW.

2.
   ```
   (config)# interface tengigabitethernet 2/0/25
   (config-if)# switchport mode stack
   (config-if)# exit
   (config)# interface tengigabitethernet 2/0/26
   (config-if)# switchport mode stack
   (config-if)# exit
   ```

   Configures stack ports for an Ethernet interface of member switch B (switch number 2).

3. `(config)# switch 2 priority 10`

   Sets the master selection priority of member switch B (switch number 2) to 10.

4.
   ```
   (config)# save
   (config)# exit
   ```

   Saves the configuration, and then returns to administrator mode from configuration command mode.

(3) Switching Switch B to operate as the member switch with switch number 2 in a stack with one member switch

Set the switch number of Switch B to 2, and then enable the stack functionality.

Points to note

Set the switch number of Switch B to 2. Then, use the `stack enable` command to enable stack operations. You must then restart the Switch, so set the `stack enable` command before starting system operation. You cannot change any configurations from the time when the `stack enable` command is set until the Switch restarts.

Note that the following configurations are automatically set when the `stack enable` command is set:

- spanning-tree disable
- no service ipv6 dhcp

Command examples

1.
```
# set switch 2
```
Sets the switch number to 2.

2.
```
(config)# stack enable
After this command execute, please save configuration editing
now in startup-config, and please reboot a device.
Do you wish to continue ? (y/n):
```
Switches the operation mode of the Switch to stack mode. When a message confirming the configuration change appears, enter `y`.

3.
```
(config)# save
(config)# exit
```
Saves the configuration, and then returns to administrator mode from configuration command mode.

4.
```
# reload
```
Restarts the Switch. After the Switch restarts, it operates as the member switch of a stack with one member switch.

(4) Setting the configuration of member switch B to connect with member switch A

Configure the settings that are essential for member switch B to connect with member switch A in a stack.

Points to note

Set the master selection priority of member switch B to 1. This means that member switch B will not operate as the master switch, even if member switch A restarts because of a failure when member switch B is connected with member switch A.

Note that the configuration set here is overwritten by that in member switch A, which operates as the master switch.

Command examples

1.
```
(config)# interface tengigabitethernet 2/0/25
(config-if)# switchport mode stack
(config-if)# exit
(config)# interface tengigabitethernet 2/0/26
(config-if)# switchport mode stack
(config-if)# exit
```
Configures stack ports for an Ethernet interface of member switch B (switch number 2).

2. `(config)# switch 2 priority 1`

   Sets the master selection priority of member switch B (switch number 2) to 1.

3. `(config)# save`

   `(config)# exit`

   Saves the configuration, and then returns to administrator mode from configuration command mode.

(5) Switching member switch A and member switch B to operate in a stack with two member switches

Connect member switch A and member switch B, each of which is operating as the member switch in a stack with one member switch, to configure a stack with two member switches.

Because the master selection priority of member switch B is 1 here, member switch A continues to operate as the master switch, and member switch B automatically restarts.

After restarting, member switch B automatically restarts again to synchronize its configurations with those of member switch A. Member switch A then operates as the master switch and member switch B as the backup switch in a stack.

Procedure

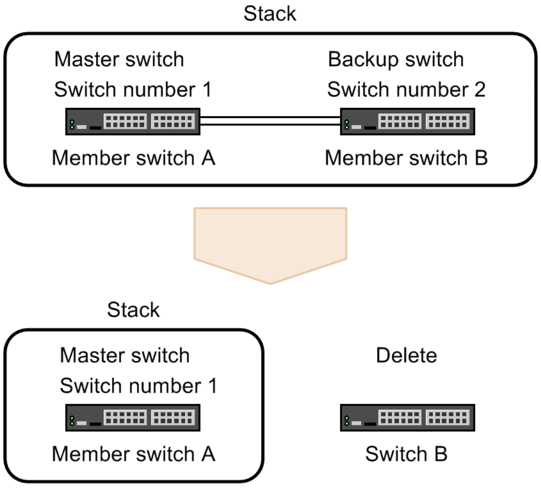
1. Connect member switch A and member switch B through their stack ports.
2. `# show switch detail`

   Execute the `show switch detail` operation command to check that member switch A operates as the master switch and that member switch B operates as the backup switch in a stack.

8.1.4 Deleting a member switch (backup switch)

As shown in the following figure, member switch B is deleted from the stack that is configured with member switch A operating as the master switch and member switch B operating as the backup switch.

Figure 8-3: Deleting a member switch (backup switch)



The following table describes how to delete a member switch (backup switch).

Table 8-5: Flow for deleting a member switch (backup switch)

Operational flow and description	Target switch
(1) Terminating member switch B	Switch B (member switch B)
(2) Deleting the configuration of member switch B • Deleting the model • Deleting the master selection priority	Member switch A

(1) Terminating member switch B

Log in to member switch B, and then terminate the switch.

Procedure

1. `# reload stop`

   Terminate member switch B.

   You can also terminate member switch B on member switch A, which is operating as the master switch. To do so, log in to member switch A and execute the following command:

   ```
   # remote command 2 reload stop
   ```

2. Turn off the power of member switch B to delete the switch from a stack configuration.

(2) Deleting the configuration of member switch B

From the configurations in member switch A, which is operating as the master switch, delete the configuration of the deleted member switch B.

Points to note

When the model of member switch B is deleted from the configurations in member switch A, the configurations of the Ethernet interfaces associated with the model are also deleted.

Command examples

1. `(config)# no switch 2 provision`

   Deletes the model of the member switch with switch number 2. When the model is deleted, the configurations of the Ethernet interfaces associated with the specified model are also deleted.

2. `(config)# no switch 2 priority`

   Deletes the master selection priority of the member switch with switch number 2.

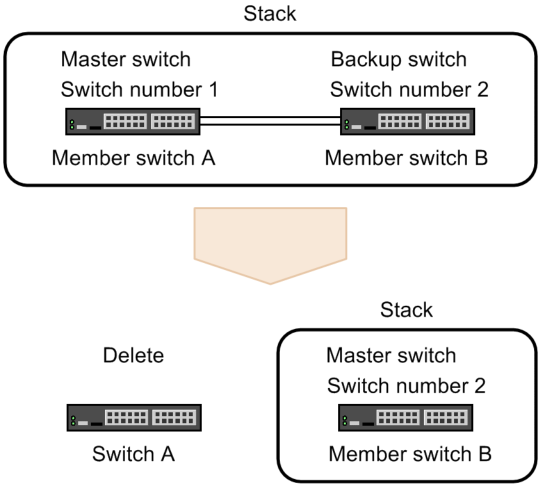
3.
   ```
   (config)# save
   (config)# exit
   ```

   Saves the configuration, and then returns to administrator mode from configuration command mode.

8.1.5 Deleting a member switch (master switch)

As shown in the following figure, member switch A is deleted from the stack that is configured with member switch A operating as the master switch and member switch B operating as the backup switch.

Figure 8-4: Deleting a member switch (master switch)



The following table describes how to delete a member switch (master switch).

Table 8-6: Flow for deleting a member switch (master switch)

Operational flow and description	Target switch
(1) Checking the state of member switch B • Checking that member switch B has been initialized • Checking that the stack ports are activated	Member switch B
(2) Terminating member switch A	Switch A (member switch A)
(3) Deleting the configuration of member switch A • Deleting the model • Deleting the master selection priority	Member switch B

(1) Checking the state of member switch B

Log in to member switch A, and then check the state of member switch B.

Procedure

1. `# show switch`

   Check that member switch B has been initialized.

2. `# remote command 2 show port`

   Check that the stack ports of member switch B are activated.

(2) Terminating member switch A

Terminate member switch A.

Procedure

1. `# reload stop`

   Terminate member switch A. Member switch B switches from the backup switch to the master switch.

2. Turn off the power of member switch A to delete the switch from a stack configuration.

(3) Deleting the configuration of member switch A

From the configurations in member switch B, which is operating as the master switch, delete the configuration of the deleted member switch A.

Points to note

When the model of member switch A is deleted from the configurations in member switch B, the configurations of the Ethernet interfaces associated with the model are also deleted.

Command examples

1. `(config)# no switch 1 provision`

   Deletes the model of the member switch with switch number 1. When the model is deleted, the configurations of the Ethernet interfaces associated with the specified model are also deleted.

2. `(config)# no switch 1 priority`

   Deletes the master selection priority of the member switch with switch number 1.

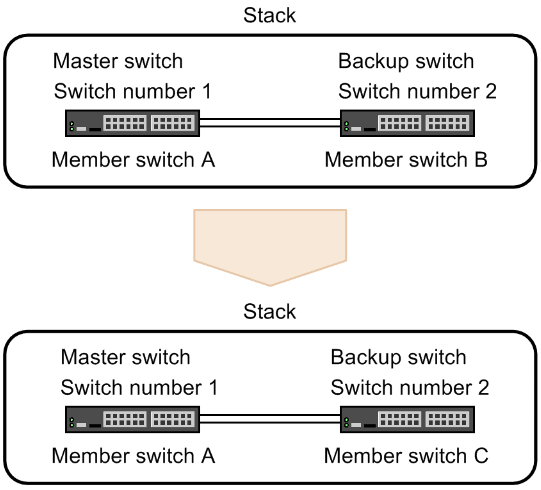
3.
   ```
   (config)# save
   (config)# exit
   ```

   Saves the configuration, and then returns to administrator mode from configuration command mode.

8.1.6 Changing a member switch

As shown in the following figure, member switch C is connected instead of member switch B in a stack configured with member switch A operating as the master switch and member switch B operating as the backup switch.

Figure 8-5: Changing a member switch



The following table describes how to change a member switch.

Table 8-7: Flow for changing a member switch

Operational flow and description	Target switch
(1) Checking the optional licenses and software installed on member switch A and Switch C • Checking the optional licenses • Checking the software	Member switch A Switch C (member switch C)
(2) Terminating member switch B	Member switch B

Operational flow and description	Target switch
(3) Switching Switch C to operate as the member switch with switch number 2 in a stack with one member switch • Setting the switch number • Setting the stack functionality • Restarting the switch	Switch C (member switch C)
(4) Setting the configuration of member switch C to connect with member switch A • Setting stack ports • Setting the master selection priority to 1	Switch C (member switch C)
(5) Switching member switch A and member switch C to operate in a stack with two member switches • Connecting stack ports	--

Legend: --: Not applicable

(1) Checking the optional licenses and software installed on member switch A and Switch C

Check the optional licenses, and the type and version of the software on member switch A, which is operating in a stack, and Switch C, which is to be connected instead of a member switch.

If the optional licenses differ between Switch A and Switch C, add or delete optional licenses so that the optional licenses are the same. If the type and version of the software differ between Switch A and Switch C, update the software so that the type and version are the same.

Procedure

1.
```
# show license
Date 20XX/10/26 12:00:00 UTC
  Available: -----
    ----------------
```
On member switch A, check the optional licenses.

2.
```
# show version software
Date 20XX/10/26 12:01:00 UTC
S/W: OS-L3SA Ver. 11.8
```
On member switch A, check the software type and version.

3.
```
# show license
Date 20XX/10/26 13:00:00 UTC
  Available: -----
    ----------------
```
On Switch C, check the optional licenses. Check that the option licenses are the same as those for member Switch A that were checked in step 1.

4.
```
# show version software
Date 20XX/10/26 13:01:00 UTC
S/W: OS-L3SA Ver. 11.8
```
Check the software type and version on Switch C. Check that the software type and version are the same as those for member switch A that were checked in step 2.

(2) Terminating member switch B

Log in to member switch B, and then terminate the switch.

Procedure

1. `# reload stop`

   Terminate member switch B.

   You can also terminate member switch B on member switch A, which is operating as the master switch. To do so, log in to member switch A and execute the following command:

   ```
   # remote command 2 reload stop
   ```

2. Turn off the power of member switch B to delete the switch from a stack configuration.

(3) Switching Switch C to operate as the member switch with switch number 2 in a stack with one member switch

Set the switch number of Switch C to 2, and then enable the stack functionality.

Points to note

Set the switch number of Switch C to 2. Then, use the `stack enable` command to enable stack operations. You must then restart the Switch, so set the `stack enable` command before starting system operation. You cannot change any configurations from the time when the `stack enable` command is set until the Switch restarts.

Note that the following configurations are automatically set when the `stack enable` command is set:

- spanning-tree disable
- no service ipv6 dhcp

Command examples

1. `# set switch 2`

   Sets the switch number to 2.

2.
   ```
   (config)# stack enable
   After this command execute, please save configuration editing
   now in startup-config, and please reboot a device.
   Do you wish to continue ? (y/n):
   ```

   Switches the operation mode of the Switch to stack mode. When a message confirming the configuration change appears, enter `y`.

3.
   ```
   (config)# save
   (config)# exit
   ```

   Saves the configuration, and then returns to administrator mode from configuration command mode.

4. `# reload`

   Restarts the Switch. After the Switch restarts, it operates as the member switch of a stack with one member switch.

(4) Setting the configuration of member switch C to connect with member switch A

Configure the settings that are essential for member switch C to connect with member switch A in a stack.

Points to note

Set the master selection priority of member switch C to 1. This means that member switch C will not operate as the master switch, even if member switch A restarts because of a failure when member switch C is connected with member switch A.

Note that the configuration set here is overwritten by that in member switch A, which operates as the master switch.

Command examples

1.
```
(config)# interface tengigabitethernet 2/0/25
(config-if)# switchport mode stack
(config-if)# exit
(config)# interface tengigabitethernet 2/0/26
(config-if)# switchport mode stack
(config-if)# exit
```
   Configures stack ports for an Ethernet interface of member switch C (switch number 2).

2.
```
(config)# switch 2 priority 1
```
   Sets the master selection priority of member switch C (switch number 2) to 1.

3.
```
(config)# save
(config)# exit
```
   Saves the configuration, and then returns to administrator mode from configuration command mode.

(5) Switching member switch A and member switch C to operate in a stack with two member switches

Connect member switch A and member switch C, each of which is operating as the member switch in a stack with one member switch, to configure a stack with two member switches.

Because the master selection priority of member switch C is 1 here, member switch A continues to operate as the master switch, and member switch C automatically restarts.

After restarting, member switch C automatically restarts again to synchronize its configurations with those of member switch A. Member switch A then operates as the master switch and member switch C as the backup switch in a stack.

Procedure

1. Connect member switch A and member switch C through their stack ports.
2.
```
# show switch detail
```
   Execute the `show switch detail` operation command to check that member switch A operates as the master switch and that member switch C operates as the backup switch in a stack.

8.1.7 Switching the operating mode to standalone

When member switches with switch number 1 and 2 configure a stack, the operating mode of the member switches is switched to standalone. The procedure differs between the member switch with switch number 1 and the member switch with switch number 2. Before configuring the setting, disconnect the member switches from the network to operate each of the switches in a stack with one member switch.

In this example, the following configuration has been set for a stack with two member switches:

```
stack enable
switch 1 provision 3650-24t6xw
switch 2 provision 3650-24t6xw
switch 1 priority 20
switch 2 priority 10
!
   :
   :
interface gigabitethernet 1/0/1
  switchport mode access
!
   :
   :
interface gigabitethernet 1/0/24
  switchport mode access
!
interface tengigabitethernet 1/0/25
  switchport mode access
!
   :
   :
interface tengigabitethernet 1/0/30
  switchport mode stack
!
interface gigabitethernet 2/0/1
  switchport mode access
!
   :
   :
interface gigabitethernet 2/0/24
  switchport mode access
!
interface tengigabitethernet 2/0/25
  switchport mode access
!
   :
   :
interface tengigabitethernet 2/0/30
  switchport mode stack
!
```

(1) Switching the operating mode of the member switch with switch number 1 to standalone

Delete the configurations of the member switch with switch number 2 and the stack functionality.

Points to note

After deleting the configuration of the stack functionality, restart the Switch.

Command examples

1.
```
(config)# interface tengigabitethernet 1/0/30
(config-if)# no switchport mode stack
(config-if)# exit
```
Deletes the stack port of the local member switch.

2.
```
(config)# no switch 2 provision
```
Deletes the model of the member switch other than the local member switch. Here, the switch number of the local member switch is 1. Therefore, the model of the member switch with switch number 2 is deleted.

3.
```
(config)# no switch 1 priority
(config)# no switch 2 priority
```
Deletes the master selection priority of the member switches with switch number 1 and switch

number 2.

4. `(config)# no stack enable`

   Disables the stack functionality.

5. `(config)# save`

   `(config)# exit`

   Saves the configuration, and then returns to administrator mode from configuration command mode.

6. `# reload`

   Restarts the Switch.

(2) Switching the operating mode of the member switch with switch number 2 to standalone

First, change the switch number to 1. Next, delete the configurations of the member switch with switch number 2 and the stack functionality.

Points to note

Change the switch number to 1, and then restart the member switch.

Next, delete the configurations of the member switch with switch number 2 and the stack functionality, and then restart the switch again.

Command examples

1. `(config)# no switch 1 provision`

   `(config)# save`

   `(config)# exit`

   Deletes the model of the member switch with switch number 1. Saves the configuration, and then returns to administrator mode from configuration command mode.

2. `# set switch 1`

   Sets the switch number to 1.

3. `# reload`

   Restarts the local member switch. After the switch restarts, the switch operates as the master switch with switch number 1.

4. `(config)# no switch 2 provision`

   Deletes the model of the member switch other than the local member switch. Here, the switch number of the local member switch is 1. Therefore, the model of the member switch with switch number 2 is deleted.

5. `(config)# no switch 1 priority`

   `(config)# no switch 2 priority`

   Deletes the master selection priority of the member switches with switch number 1 and switch number 2.

6. `(config)# no stack enable`

   Disables the stack functionality.

7. `(config)# save`

   `(config)# exit`

   Saves the configuration, and then returns to administrator mode from configuration command mode.

8. `# reload`

   Restarts the Switch.

8.1.8 Adding a stack link

Add a stack link to a stack with one stack link. Here, the following settings have been configured before adding a stack link:

```
stack enable
switch 1 provision 3650-24t6xw
switch 2 provision 3650-24t6xw
   :
   :
interface tengigabitethernet 1/0/29
  switchport mode stack
!
interface tengigabitethernet 1/0/30
  switchport mode access
   :
   :
interface tengigabitethernet 2/0/29
  switchport mode stack
!
interface tengigabitethernet 2/0/30
  switchport mode access
!
```

(1) Checking that no cable is connected to the ports to be added

Check that no cable is connected to the ports to be added as stack ports. If cables are connected to the ports, remove the cables before setting the configuration to add the ports as stack ports.

(2) Setting stack port configuration

Set the configuration to add ports as stack ports.

Command examples

1.
   ```
   (config)# interface tengigabitethernet 1/0/30
   (config-if)# switchport mode stack
   (config-if)# exit
   (config)# interface tengigabitethernet 2/0/30
   (config-if)# switchport mode stack
   (config-if)# exit
   ```

   Configures stack ports for an Ethernet interface of the member switches with switch number 1 and switch number 2.

2.
   ```
   (config)# save
   (config)# exit
   ```

   Saves the configuration, and then returns to administrator mode from configuration command mode.

(3) Connecting the stack ports to add a stack link

Connect the stack ports set for the switches with switch number 1 and switch number 2 via a cable to add a stack link to the stack.

8.1.9 Deleting a stack link

Delete stack ports from a stack with two stack links. Here, the following settings have been configured before deleting a stack link:

```
stack enable
switch 1 provision 3650-24t6xw
switch 2 provision 3650-24t6xw
   :
   :
interface tengigabitethernet 1/0/29
  switchport mode stack
!
interface tengigabitethernet 1/0/30
  switchport mode stack
   :
   :
interface tengigabitethernet 2/0/29
  switchport mode stack
!
interface tengigabitethernet 2/0/30
  switchport mode stack
!
```

(1) Disconnecting the stack ports of the stack link to be deleted

Remove the port from the stack ports of the stack link to be deleted. If you are in a situation where it is difficult to remove the cable, use the configuration commands below to shut down the stack ports.

Command examples

1.
```
(config)# interface tengigabitethernet 1/0/30
(config-if)# shutdown
(config-if)# exit
(config)# interface tengigabitethernet 2/0/30
(config-if)# shutdown
(config-if)# exit
```
Shuts down the stack ports of the member switches with switch number 1 and switch number 2.

(2) Deleting the configurations of stack ports

Delete the configurations of the stack ports connected by the stack link to be deleted.

Command examples

1.
```
(config)# interface tengigabitethernet 1/0/30
(config-if)# no switchport mode stack
(config-if)# exit
(config)# interface tengigabitethernet 2/0/30
(config-if)# no switchport mode stack
(config-if)# exit
```
Deletes the configurations of the stack ports from those of the member switches with switch number 1 and switch number 2.

2.
```
(config)# save
```

```
(config)# exit
```

Saves the configuration, and then returns to administrator mode from configuration command mode.

8.2 Operation

8.2.1 List of operation commands

The following table describes the operation commands related to the stack functionality.

Table 8-8: List of operation commands

Command name	Description
show switch	Shows the information about the member switches that configure a stack.
remote command	Sends operation commands from the master switch to the specified member switch.
dump stack	Outputs the detailed event trace information and the control table information which are collected by the stack management program.

8.2.2 Checking information about the member switches that configure a stack

Use the `show switch` operation command to check the information about the member switches that configure a stack. The switch number is displayed in the `No` field. The switch states and the switch-state change process that occurs after a switch state transition are displayed in the `Switch status` field.

Figure 8-6: Results of executing the show switch command

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

By executing the `show switch` operation command with the `detail` parameter, you can check detailed information about member switches. Information about stack ports is displayed in the `Port` and `Neighbor(Port)` fields.

Figure 8-7: Results of executing the show switch detail command

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

Note that you can check the switch state and the switch number on the front panel of each Switch. For details, see *8.2.3 Displaying the switch state and the switch number on the front panel*.

8.2.3 Displaying the switch state and the switch number on the front panel

(1) LED indication [AX3800S]

You can check the switch state and the switch number from the LEDs on the front of the Switch.

ST2 indicates the switch state, which you can determine by checking whether ST2 is on or off. ID1 and ID2 correspond to switch numbers (1 and 2), which you can determine by checking which LED is on.

Table 8-9: Switch states and LED lights

LED name	Switch state	LED light
ST2	Initial state	Off
	Master	Green
	Backup	Off

Table 8-10: Switch numbers and LED lights

Switch number	LED light
Switch number 1	ID1 on
Switch number 2	ID2 on

Note that no lights are on when the Switch is operating in standalone mode.

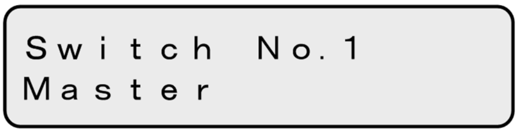
(2) Appearance of the display [AX3650S]

You can check the switch state and the switch number from the information display of the system operation panel mounted on the front of the Switch. The information appears on the display in the following situations, and then automatically disappears after 60 seconds.

- The switch state is changed.
- A key at the bottom of the display is pressed.

You can check the switch number (1 or 2) in the upper line of the display and the switch number in the lower line.

Figure 8-8: Example of displaying stack information



```
Switch No.1
Master
```

Table 8-11: Switch states and displayed information

Switch state	Information
Initial state	`Init`
Master	`Master`
Backup	`Backup`

Note that no information is displayed when the Switch is operating in standalone mode.

8.2.4 Sending operation commands from the master switch to a member switch

You can use the `remote command` operation command to send operation commands from the master switch to the specified member switch.

The example below shows how to use the `remote command` command and the `show clock` operation command to display the times of the member switches when the master switch operates with switch number 1 and the backup switch operates with switch number 2. Note that the switch number and the switch state are displayed at the beginning of the results for each member switch.

Figure 8-9: Displaying the time of the member switch with switch number 2

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

Figure 8-10: Displaying the times of all member switches

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


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

8.2.5 Restarting a stack

When adding or deleting an optional license, or when editing a configuration which requires that you restart the Switch or VLAN program, you must restart the stack to correctly apply the changes.

To restart a stack, you must restart all of the member switches that make up the stack. The procedures below describe how to restart a stack. Note that you must restart all member switches within 30 seconds after the first member switch restarts.

1. Log in to the master switch.
2. Execute the `enable` command to move to administrator mode.
3. Execute the `show switch` command to check the member switches that are being operated.

   Here, the execution results are displayed as shown below. From the results, you can see that the master switch with switch number 1 and the member switch with switch number 2 are being operated.

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

4. Restart the member switches other than the master switch.

   First, restart the member switches other than the master switch.

   Here, a member switch other than the master switch is present and operating with switch number 2. Execute the following command:

```
# remote command 2 reload no-dump-image -f
```

5. Execute the command below to restart the master switch

   Execute the following command to restart the master switch within 30 seconds after the first member switch restarts.

```
# reload no-dump-image -f
```

8.2.6 Configuring optional licenses

This section describes how to add or delete optional licenses to operate switches in a stack.

To configure a stack, the same optional licenses must be installed on the member switches. Because of this, sometimes you need to add or delete optional licenses from member switches. Restart the backup switch, and then restart the master switch within 30 seconds to apply the optional licenses.

1. Log in to the master switch.
2. Execute the `enable` command to move to administrator mode.
3. Use the `remote command` command to add or delete optional licenses from the backup switch.
4. Add or delete optional licenses from the master switch.
5. To apply the optional licenses, restart all member switches that make up the stack.

   For details about how to restart member switches, see *8.2.5 Restarting a stack*.

Chapter

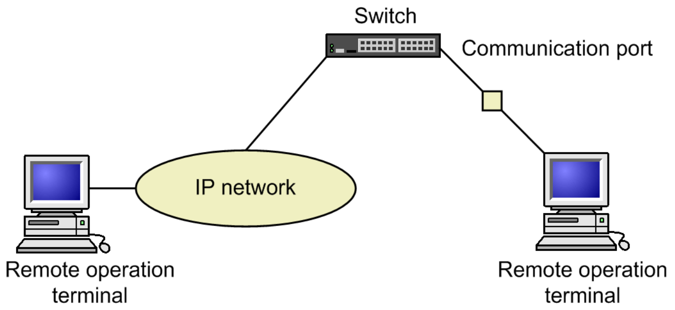
9. Remote Login

This chapter describes remote access to the Switch from a remote operation terminal.

9.1 Description

To log in to the Switch from a remote operation terminal via the communication port, you must first configure the connection in the Switch, including configuring a VLAN and setting its IP address. At initial deployment, no VLANs, IP addresses, or other settings are defined. Log in from the console to set up the connection.

Figure 9-1: Login to the Switch from a remote operation terminal



9.2 Configuration

9.2.1 List of configuration commands

The following table describes the configuration commands related to terminal connections and remote operations.

Table 9-1: List of configuration commands

Command name	Description
ftp-server	Permits access from remote operation terminals using FTP.
line console	Sets parameters for the RS232C port.
line vty	Permits Telnet remote access to a switch.
speed	Sets the communication speed of the RS232C port.
transport input	Regulates access from a remote operation terminal using the various protocols.

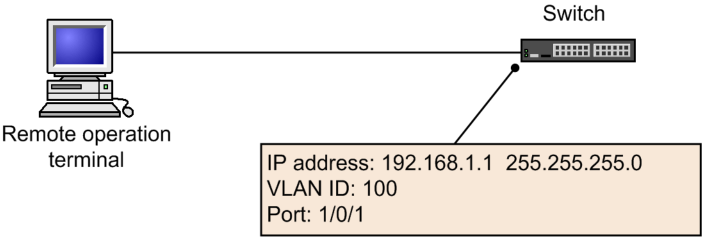
For details on the configuration commands related to setting up VLANs and IPv4/IPv6 interfaces, see *20. VLANs* in this manual, and also *2. Settings and Operation for IP, ARP, and ICMP* in the manual *Configuration Guide Vol. 3 For Version 11.10* or *18. Settings and Operation for IPv6, NDP, and ICMPv6* in the manual *Configuration Guide Vol. 3 For Version 11.10*.

9.2.2 Assigning an IP address to the Switch

Points to note

To access the Switch from a remote operation terminal, you must first set an IP address in the interface that the terminal connects to.

Figure 9-2: Example of connecting with a remote operation terminal


Switch
Remote operation terminal
IP address: 192.168.1.1 255.255.255.0
VLAN ID: 100
Port: 1/0/1

Command examples

1. `(config)# vlan 100`

   `(config-vlan)# exit`

   Creates a port VLAN with VLAN ID 100, and switches to the VLAN configuration mode for VLAN 100.

2. `(config)# interface gigabitethernet 1/0/1`

   `(config-if)# switchport mode access`

   `(config-if)# switchport access vlan 100`

   `(config-if)# exit`

   Switches to the Ethernet interface configuration mode for port 1/0/1. Sets port 1/0/1 for the

VLAN 100 access port.

3.
```
(config)# interface vlan 100
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# exit
(config)#
```

Switches to interface configuration mode for VLAN ID 100. Sets IPv4 address 192.168.1.1 and subnet mask 255.255.255.0 for VLAN ID 100.

9.2.3 Permitting login by using the Telnet protocol

Points to note

The switch's IP address must be assigned before you can use this procedure.

Set the `line vty` configuration command that allows remote login to the Switch via Telnet.

If remote login has not been configured, you can log in only from the console.

Command examples

1.
```
(config)# line vty 0 2
(config-line)#
```

Permits remote access to the Switch from a remote operation terminal by using the Telnet protocol. Also, limits the number of concurrent remote logins to a maximum of three users.

9.2.4 Permitting login by using FTP

Points to note

The switch's IP address must be assigned before you can use this procedure.

Set the `ftp-server` configuration command that allows remote access to the Switch from a remote operation terminal via FTP.

If the Switch is not configured in this manner, users cannot access the Switch by using FTP.

Command examples

1.
```
(config)# ftp-server
```

Permits remote access to the Switch from a remote operation terminal by using FTP.

9.2.5 Permitting login from VRF by using Telnet protocol [OS-L3SA]

(1) To permit users to log in from all VRFs including the global network via Telnet

Points to note

To permit access from all VRFs, set the `vrf all` parameter of the `transport input` configuration command. If the `vrf all` parameter is not set, only access from the global network is allowed.

Command examples

1.
```
(config)# line vty 0 2
(config-line)#
```

Permits remote access to the Switch from a remote operation terminal by using the Telnet protocol. Also, limits the number of concurrent remote logins to a maximum of three users.

2.
```
(config-line)# transport input vrf all telnet
(config-line)#
```

Permits remote access to this Switch from remote operation terminals on all VRFs including the global access via the Telnet protocol.

(2) To permit login via Telnet from a specific VRF

Points to note

To permit access from a specific VRF, set the VRF ID to the `vrf` parameter of the `transport input` configuration command. If this `vrf` parameter is not set, only access from the global network is allowed.

Command examples

1.
```
(config)# line vty 0 2
(config-line)#
```

Permits remote access to the Switch from a remote operation terminal by using the Telnet protocol. Also, limits the number of concurrent remote logins to a maximum of three users.

2.
```
(config-line)# transport input vrf 2 telnet
(config-line)#
```

Permits remote access to the Switch from a remote operation terminal on VRF 2 via the Telnet protocol. The global network is excluded.

9.2.6 Permitting login from VRF by using FTP [OS-L3SA]

(1) To permit users to log in from all VRFs including the global network via FTP

Points to note

To permit access from all VRFs, set the `vrf all` parameter of the `ftp-server` configuration command. If the `vrf all` parameter is not set, only access from the global network is allowed.

Command examples

1.
```
(config)# ftp-server vrf all
```

Permits remote access to this Switch from remote operation terminals on all VRFs including global access via FTP.

(2) To permit login via FTP from a specific VRF

Points to note

To permit access from a specific VRF, set the VRF ID to the `vrf` parameter of the `ftp-server` configuration command. If this `vrf` parameter is not set, only access from the global network is allowed.

Command examples

1.
```
(config)# ftp-server vrf 2
```

VRF 2 permits remote access to the Switch from a remote operation terminal via FTP. The global network is excluded.

9.3 Operation

9.3.1 List of operation commands

The following table describes the operation commands related to terminal connections and remote operations.

Table 9-2: List of operation commands

Command name	Description
set exec-timeout	Specifies the length of time until the user is automatically logged out.
set terminal help	Selects the type of command help messages to be displayed.
set terminal pager	Enables or disables paging.
show history	Shows a log of operation commands executed in the past. (No log is displayed for configuration commands.)
telnet	Connects via Telnet to the remote operation terminal that has the specified IP address.
ftp	Transfers files between the Switch and a remote terminal connected by using TCP/IP.
tftp	Transfers files between the Switch and a remote terminal connected by using UDP.

For details on the configuration commands related to setting up VLANs and IPv4/IPv6 interfaces, see *20. VLANs* in this manual, and also *2. Settings and Operation for IP, ARP, and ICMP* in the manual *Configuration Guide Vol. 3 For Version 11.10* or *18. Settings and Operation for IPv6, NDP, and ICMPv6* in the manual *Configuration Guide Vol. 3 For Version 11.10*.

9.3.2 Checking communication between a remote operation terminal and the Switch

You can check that the Switch and a remote operation terminal are communicating by using the `ping` or `ping ipv6` operation command. For details, see *2. Settings and Operation for IP, ARP, and ICMP* in the manual *Configuration Guide Vol. 3 For Version 11.10* or *18. Settings and Operation for IPv6, NDP, and ICMPv6* in the manual *Configuration Guide Vol. 3 For Version 11.10*.

Chapter

10. Login Security and RADIUS or TACACS+

This chapter describes login control, login security, accounting, and RADIUS and TACACS+ application functionality in the Switch.

10.1 Setting login security

10.1.1 Lists of configuration commands and operation commands

The following table describes the configuration commands for login security.

Table 10-1: List of configuration commands

Command name	Description
aaa authentication enable	Specifies the authentication method to be used when changing to administrator mode (by the `enable` command).
aaa authentication enable attribute-user-per-method	Changes the user name attributes used in authentication when changing to administrator mode (by the `enable` command).
aaa authentication enable end-by-reject	Terminates authentication if an attempt to change to administrator mode (by the `enable` command) is denied.
aaa authentication login	Specifies the authentication method to be used at remote login.
aaa authentication login console	Applies the authentication method specified by the `aaa authentication login` command when the user logs in from the console (RS232C).
aaa authentication login end-by-reject	Terminates authentication if login authentication is denied.
aaa authorization commands	Specifies that command authorization is to be performed by a RADIUS or TACACS+ server.
aaa authorization commands console	Applies the command authorization specified by the `aaa authorization commands` command when the user logs in from the console (RS232C).
banner	Defines the messages to be displayed before and after the user logs in.
commands exec	Adds a command string to a command list used when local command authorization is enabled.
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.
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.
parser view	Generates a command list used when local command authorization is enabled.
username	Sets for a specified user a command list or command class used in local command authorization.

The following table describes the operation commands for login security.

Table 10-2: List of operation commands

Command name	Description
adduser	Adds an account for a new login user.
rmuser	Deletes a user login account registered by the `adduser` command.
password	Changes the password of a login user.
clear password	Deletes the password of a login user.
show sessions	Shows the users currently logged in to the Switch.
show whoami	Shows only the user, logged in to the Switch, who executed this command.

Command name	Description
killuser	Forcibly logs out a login user.

10.1.2 Overview of login control

The Switch supports local login via a serial connection, and remote login using Telnet over an IPv4 or IPv6 network.

The following controls are implemented in the Switch when a user logs in and during a user session:

1. To prevent unauthorized access, a password check is performed at login, and restrictions based on the user ID are placed on the range of commands that the user can execute.
2. Users can log in to a Switch concurrently from multiple terminals.
3. The maximum number of users who can log in concurrently is 16. You can reduce this limit by using the `line vty` configuration command.
4. You can restrict the IPv4 and IPv6 addresses permitted to access the Switch by using the `ip access-list standard`, `ipv6 access-list`, `access-list`, `ip access-group`, and `ipv6 access-class` configuration commands.
5. You can limit the protocols used to access the Switch (Telnet and FTP) by using the `transport input` and `ftp-server` configuration commands.
6. In VRFs, you can restrict the IPv4 and IPv6 addresses permitted to access the Switch by using the `ip access-list standard`, `ipv6 access-list`, `access-list`, `ip access-group`, and `ipv6 access-class` configuration commands. **[OS-L3SA]**
7. In VRFs, you can limit the protocols used to access the Switch (Telnet and FTP) by using the transport input and `ftp-server` configuration commands. **[OS-L3SA]**
8. Command execution results appear only on the terminal where the command was executed. Operation messages appear on all login terminals.
9. Entered commands, response messages, and operation messages are recorded as an operation log. The operation log can be viewed by using the `show logging` operation command.
10. The user is automatically logged out if there is no key input for a specified period (default: 60 minutes).
11. You can forcibly log out a user using the `killuser` operation command.

10.1.3 Creating and deleting user accounts

To create a user account for logging in to the Switch, use the `adduser` command. The following figure shows an example.

Figure 10-1: Creating the account newuser

```
> enable
# adduser newuser
User(empty password) add done. Please setting password.

Changing local password for newuser.
New password:********                                   ...1
Retype new password:********                            ...2
# quit
>
```

1. Type the user's password (the actual characters are not shown).
2. Type the user's password again to confirm it (the actual characters are not shown).

You can delete an account that is no longer needed by executing the `rmuser` command.

If you do not intend to use the pre-defined `operator` account, to prevent any security risk we recommend that you delete the `operator` account by executing the `rmuser` command after you create the new user account. Also, by using the `aaa authentication login` configuration command, you can implement RADIUS or TACACS+ authentication. For configuration examples, see *10.3.2 Configuring RADIUS authentication* and *10.3.3 Configuring TACACS+ authentication*.

Do not forget your login user name. If you forget it, you will not be able to log in even after a default restart.

10.1.4 Setting the password for administrator mode

To execute configuration commands, you must switch to administrator mode by using the `enable` command. Because the Switch has no pre-defined passwords, executing the `enable` command at deployment will place you in administrator mode without authentication. However, there is a security risk if any user can switch to administrator mode during normal operation without any password authentication. You should therefore set an administrator password at deployment, as in the following example.

Figure 10-2: Setting the password for administrator mode immediately after deployment

```
> enable
# password enable-mode
Changing local password for admin.
New password:
Retype new password:
#
```

Using the `aaa authentication enable` configuration command, you can implement authentication using a RADIUS or TACACS+ server. For configuration examples, see *10.3.2 Configuring RADIUS authentication* and *10.3.3 Configuring TACACS+ authentication*.

10.1.5 Permitting login from a remote operation terminal

Using the `line vty` configuration command, you can enable login to the Switch from a remote operation terminal. If remote login has not been configured, you can log in only from the console. The following figure shows an example of configuring permission for remote login.

Figure 10-3: Example of configuring permission for remote login

```
(config)# line vty 0 2
(config-line)#
```

To permit access to the Switch from a remote operation terminal using FTP, you must set the `ftp-server` configuration command. If you omit this setting, users cannot access the Switch by FTP.

Figure 10-4: Example of configuring permission for FTP access

```
(config)# ftp-server
(config)#
```

10.1.6 Setting the maximum number of concurrent users

Using the `line vty` configuration command, you can enable login to the Switch from a remote operation terminal. The value of the <*num*> parameter limits the number of remote users who can log in concurrently. Regardless of this setting, login from the console is always possible. The following setting example allows no more than two users to be logged in concurrently.

Figure 10-5: Example of setting the maximum number of concurrent users

```
(config)# line vty 0 1
```

```
(config-line)#
```

Switch behavior in regard to concurrent users is as follows:

- Multiple users attempting to log in at the same time might not succeed, even if the number of concurrent users is less than the maximum.
- If you change the maximum number of concurrent users, current user sessions will not be terminated.

10.1.7 Setting the IP addresses of remote operation terminals permitted to log in

By setting their IP addresses, you can specify which remote operation terminals are allowed to log in to the Switch. After performing this setup, make sure that other remote operation terminals are denied access.

Points to note

To permit access to the Switch from only specific remote operation terminals, you must register their IP addresses in advance using the `ip access-list standard`, `ipv6 access-list`, `access-list`, `ip access-group`, or `ipv6 access-class` configuration command. You can register a maximum of 128 IPv4 addresses and subnet masks, or IPv6 addresses and prefixes. If you omit this setup, all remote operation terminals will be able to access the Switch. If access is attempted from a terminal that does not have access permission (a terminal not registered in the configuration entry), the message `Unknown host address` <*IP address*> will appear on other login terminals. Changing the IP addresses that are permitted to access the Switch will not terminate current user sessions.

Command examples (IPv4)

1.
```
(config)# ip access-list standard REMOTE
(config-std-nacl)# permit 192.168.0.0 0.0.0.255
(config-std-nacl)# exit
```
Sets the access list `REMOTE`, which permits login only from the network IP address 192.168.0.0/24.

2.
```
(config)# line vty 0 2
(config-line)# ip access-group REMOTE in
(config-line)#
```
Moves to line mode, applies the access list `REMOTE`, and permits login only from the network IP address 192.168.0.0/24.

Command examples (IPv6)

1.
```
(config)# ipv6 access-list REMOTE6
(config-ipv6-nacl)# permit ipv6 3ffe:501:811:ff01::/64 any
(config-ipv6-nacl)# exit
```
Sets the access list `REMOTE6`, which permits login only from the network IP address 3ffe:501:811:ff01::/64.

2.
```
(config)# line vty 0 2
```

```
(config-line)# ipv6 access-class REMOTE6 in
(config-line)#
```

Moves to line mode, applies the access list `REMOTE6`, and permits login only from the network IP address 3ffe:501:811:ff01::/64.

10.1.8 Setting login banners

By setting login banners with the `banner` configuration command, you can display messages before and after a user logs in to the Switch from the console, or from a Telnet or FTP client running on a remote operation terminal.

Points to note

The following pre-login message can be presented when a Telnet or FTP client running on a remote operation terminal connects to the Switch over the network:

```
##########################################
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
##########################################
```

Command examples

1.
```
(config)# banner login plain-text
--- Press CTRL+D or only '.' line to end ---
##########################################
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
##########################################
.
```

Type the pre-login screen message.

After typing the message, enter a line containing a period (.) only, or press **Ctrl** + **D**.

2.
```
(config)# show banner
banner login encode
"IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjCldh
cm5pbmchISEgV2FybmluZyEhISBXYXJuaW5nISEhClRoaXMgaXMgb3VyIHN5c
3RlbS4gWW91IHNob3VsZCBub3QgbG9naW4uClBsZWFzZSBjbG9zZSBjb25uZW
N0aW9uLgojIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMK"
```

The message you entered is encoded automatically.

3.
```
(config)# show banner login plain-text
##########################################
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
```

```
Please close connection.
##########################################
(config)#
```

To check the banner message in text format, specify the `plain-text` parameter in the `show banner login` command.

With these settings, the message you typed will be displayed on the remote operation terminal that connects to the Switch by Telnet or FTP.

Figure 10-6: Example of connection from a remote operation terminal (connected by Telnet)

```
> telnet 10.10.10.10
Trying 10.10.10.10...
Connected to 10.10.10.10.
Escape character is '^]'.

##########################################
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
##########################################
login:
```

Figure 10-7: Example of connection from a remote operation terminal (connected by FTP)

```
> ftp 10.10.10.10
Connected to 10.10.10.10.
220-
##########################################
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
##########################################
220 10.10.10.10 FTP server (NetBSD-ftpd) ready.
Name (10.10.10.10:staff):
```

10.1.9 Permitting login from a remote operation terminal when using VRF [OS-L3SA]

Using the `line vty` configuration command, you can enable login to the Switch from a remote operation terminal. Set the `vrf` parameter of the `transport input` configuration command to permit access from VRFs. If this `vrf` parameter is not set, only access from the global network is allowed.

The figure below shows how to permit remote access to this Switch from remote operation terminals on all VRFs including the global access via the Telnet protocol.

Figure 10-8: Example of configuring permission for remote login in all VRFs including the global network

```
(config)# line vty 0 2
(config-line)# transport input vrf all telnet
(config-line)#
```

The figure below shows how to permit remote access to this Switch from remote operation terminals on a specified VRF via the Telnet protocol. The global network is excluded.

Figure 10-9: Example of configuring permission for remote login in VRF 2

```
(config)# line vty 0 2
(config-line)# transport input vrf 2 telnet
(config-line)#
```

To permit access to the Switch from a remote operation terminal using FTP, you must set the `ftp-server` configuration command. To permit access from VRFs, set the `vrf` parameter. If this `vrf` parameter is not set, only access from the global network is allowed.

The figure below shows how to permit remote access to this Switch from remote operation terminals on all VRFs including the global access via FTP.

Figure 10-10: Example of configuring permission to access from remote operation terminals on all VRFs including the global network via FTP protocol

```
(config)# ftp-server vrf all
(config)#
```

The figure below shows how to permit remote access to this Switch from remote operation terminals on a specified VRF via FTP. The global network is excluded.

Figure 10-11: Example of configuring permission to access from a remote operation terminal when using VRF 2 via FTP protocol

```
(config)# ftp-server vrf 2
(config)#
```

10.1.10 Setting the IP address that permits login from a remote operation terminal when using VRF [OS-L3SA]

By setting their IP addresses in an access list, you can specify which remote operation terminals are allowed to log in to the Switch.

As a rule, access lists are individually set to the global network and each VRF. An access list can also be set to all VRFs including the global network. Although these configurations can be used in combination, the last access list is implicitly discarded when using multiple access lists.

How access lists are applied to the access source VRFs (that is, the application range of access lists) depends on the relationship between the access sources and the locations where access lists are set. As an example, the following table describes how an applied access list will change depending on where access lists are set when the Switch is accessed from the global network, VRF 10 and VRF 20. (Entries in parentheses show which access list is applied.)

Table 10-3: Application range of access lists

Access list location	Access source VRF		
	Global network	VRF 10	VRF 20
• global	(global)	--	--
• global • VRF 10	(global)	(VRF 10)	--
• global • VRF 10 • VRF ALL	(global)# After applied (VRF ALL)	(VRF 10)# After applied (VRF ALL)	(VRF ALL)

Legend:

-: No access list is applied. Therefore, access is not restricted.

global: Global network

VRF 10: VRF 10

VRF ALL: All VRFs including the global network

#

Individually set access lists are applied with a higher priority than access lists set as `VRF ALL`.

When using multiple access lists, individually set access lists will not be implicitly discarded. If no individually set access list satisfies the conditions, the access list set as `VRF ALL` is applied. If the access lists set as `VRF ALL` does not satisfy the conditions either, access is restricted due to the implicit discard.

After configuring settings, check whether other remote operation terminals are denied login to the Switch.

Points to note

Use an access list to permit access to this Switch from specific remote operation terminals. To do so, you must register their IP addresses in advance by using the `ip access-list standard`, `ipv6 access-list`, `access-list`, `ip access-group`, or `ipv6 access-class` configuration commands. You can register a maximum of 128 IPv4 addresses and subnet masks, or IPv6 addresses and prefixes. If you omit this configuration, all remote operation terminals will be able to access the Switch. If access is attempted from a terminal that does not have access permission (a terminal not registered in the configuration entry), the message `Unknown host address` <*IP address*> will appear on other login terminals.

A configuration example is shown below. First, restrict login from remote operation terminals on all VRFs including the global network. Next, permit login from the global network and specific VRFs. After this, login is permitted only from specified networks.

Command examples

1.
```
(config)# ip access-list standard REMOTE_VRFALL
(config-std-nacl)# deny any
(config-std-nacl)# exit
```
Set the access list REMOTE_VRFALL, which restricts login to all VRFs including the global network.

2.
```
(config)# ip access-list standard REMOTE_GLOBAL
(config-std-nacl)# permit 192.168.0.0 0.0.0.255
(config-std-nacl)# exit
```
Sets the access list `REMOTE_GLOBAL`, which permits login only from the network IP address 192.168.0.0/24 in a global network.

3.
```
(config)# ip access-list standard REMOTE_VRF10
(config-std-nacl)# permit 10.10.10.0 0.0.0.255
(config-std-nacl)# exit
```
Sets the access list REMOTE_VRF10, which permits login only from the network IP address 10.10.10.0/24 on VRF 10.

4.
```
(config)# line vty 0 2
(config-line)# ip access-group REMOTE_VRFALL vrf all in
(config-line)# ip access-group REMOTE_GLOBAL in
(config-line)# ip access-group REMOTE_VRF10 vrf 10 in
(config-line)#
```
Moves to line mode, applies the access list `REMOTE_VRFALL` to all VRFs including the global

network, the access list `REMOTE_GLOBAL` to the global network, and the access list `REMOTE_VRF10` to VRF10.

On the global network, permits login only from the network IP address 192.168.0.0/24.

On VRF 10, permits login only from the network IP address 10.10.10.0/24.

Login from other VRFs is restricted.

10.2 Description of RADIUS and TACACS+

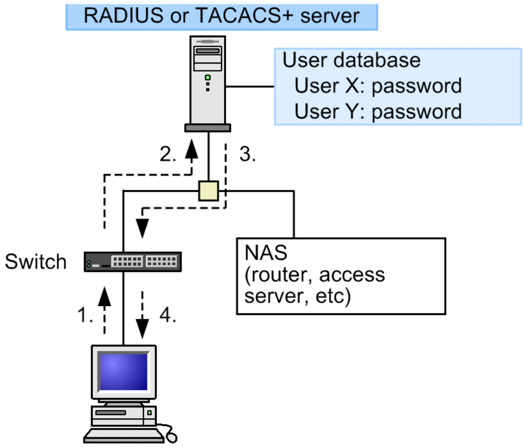
10.2.1 Overview of RADIUS and TACACS+

RADIUS (Remote Authentication Dial In User Service) and TACACS+ (Terminal Access Controller Access Control System Plus) are protocols that provide authentication, authorization, and accounting services to a Network Access Server (NAS). A NAS is a device such as a remote access server or router that acts as a RADIUS or TACACS+ client. A NAS device requests services such as user authentication, command authorization, and accounting from the configured RADIUS or TACACS+ server. The server responds to service requests based on the data in its management information database. The Switch supports NAS functionality.

When RADIUS or TACACS+ is implemented, authentication information such as user passwords used by the NAS devices, command authorization information, and accounting information can be centrally managed by one RADIUS or TACACS+ server. The Switch can request authentication, authorization, and accounting services from a RADIUS or TACACS+ server.

The following figure shows the flow of RADIUS or TACACS+ authentication.

Figure 10-12: Flow of RADIUS or TACACS+ authentication



1. Using the Telnet protocol, user X connects to the Switch from the remote terminal.
2. The Switch requests authentication by the RADIUS or TACACS+ server specified in the configuration.
3. The RADIUS or TACACS+ server authenticates user X from the user database and notifies the Switch that the user has been authenticated.
4. Based on the RADIUS or TACACS+ authentication, the Switch permits Telnet access by user X from the remote terminal.
5. If command authorization is set in the configuration, the Switch permits or denies operating command input according to the command list set in the RADIUS or TACACS+ server.

10.2.2 Scope of RADIUS or TACACS+ implementation

The Switch uses RADIUS or TACACS+ for login authentication from an operation terminal, authentication when changing to administrator mode (by the `enable` command), command authorization, and accounting. RADIUS is also used for IEEE 802.1X authentication and Web authentication of operation terminals. The RADIUS and TACACS+ function support range is listed below.

(1) Supported RADIUS and TACACS+ functions

RADIUS or TACACS+ authentication can be used for the following operations:

- Telnet access from a remote operation terminal (IPv4/IPv6)

- FTP access from a remote operation terminal (IPv4/IPv6)
- Login from the console (RS232C)
- Transition to administrator mode (by the `enable` command)

RADIUS or TACACS+ command authorization can be used for the following operations:

- Telnet access from a remote operation terminal (IPv4/IPv6)
- Login from the console (RS232C)

RADIUS or TACACS+ accounting can be used for the following operations:

- Telnet login-logout from a remote operation terminal (IPv4/IPv6)
- FTP login-logout from a remote operation terminal (IPv4/IPv6)
- Login-logout from the console (RS232C)
- Command input using the CLI (TACACS+ only)

(2) Scope of RADIUS implementation

The Switch supports the following NAS functionality for communication with a RADIUS server:

Table 10-4: Scope of RADIUS support

Category	Description
Documentation	Supported RADIUS functions described herein are limited to NAS-related functions only.
Packet type	Support for the following packet types used in login authentication, authentication when changing to administrator mode (by the `enable` command), and command authorization: • Access-Request (send) • Access-Accept (receive) • Access-Reject (receive) Support for the following accounting packet types: • Accounting-Request (send) • Accounting-Response (receive)

Category	Description
Attribute	Support for the following attributes used in login authentication and authentication when changing to administrator mode (by the `enable` command): • User-Name • User-Password • Service-Type • NAS-IP-Address • NAS-IPv6-Address • NAS-Identifier • Reply-Message Support for the following command authorization attributes: • Class • Vendor-Specific (Vendor-ID: 21839) Support for the following accounting attributes: • User-Name • NAS-IP-Address • NAS-IPv6-Address • NAS-Port • NAS-Port-Type • Service-Type • Calling-Station-Id • Acct-Status-Type • Acct-Delay-Time • Acct-Session-Id • Acct-Authentic • Acct-Session-Time

(a) Description of supported RADIUS attributes

The table below describes the RADIUS attributes used in authentication, command authorization, and accounting.

To perform command authorization using a RADIUS server, you must set up the server in advance so that it returns a `Class` or `Vendor-Specific` attribute when a user is authenticated. Set vendor-specific attributes in a `dictionary` file or other configuration file to register them with the RADIUS server. For details about command authorization, see *10.2.4 RADIUS or TACACS+ and local command authorization*.

Table 10-5: Supported RADIUS attributes

Attribute name	Attribute value	Packet type	Description
User-Name	1	Access-Request Accounting-Request	The name of the user being authenticated. Sends the login user name when login authentication is performed. Following *Table 10-10: User name attributes to be set* sends the user name when authentication is performed to go into administrator mode (by the `enable` command).
User-Password	2	Access-Request	The password of the user being authenticated, sent in encrypted form
Service-Type	6	Access-Request Accounting-Request	`Login` (value = `1`), Administrative (value = 6; used only for Access-Request packet type). Ignored when attached to `Access-Accept` or `Access-Reject`.

Attribute name	Attribute value	Packet type	Description
NAS-IP-Address	4	Access-Request Accounting-Request	The IP address of the Switch. Indicates the local address if the local address is specified. Indicates the IP address of the requesting interface if the local address is not specified.
NAS-IPv6-Address	95	Access-Request Accounting-Request	The IPv6 address of the Switch. Indicates the local address if the local address is specified. Indicates the IPv6 address of the requesting interface if the local address is not specified. If communicating with IPv6 link-local addresses, the IPv6 link-local address of the requesting interface is set, regardless of the local address setting.
NAS-Identifier	32	Access-Request Accounting-Request	The device name of the Switch. This is not attached if a device name was not set.
Reply-Message	18	Access-Accept Access-Reject Accounting-Response	A message from the server. Output as an operation log entry if attached.
Class	25	Access-Accept	The login class; used in command authorization.
Vendor-Specific	26	Access-Accept	A login list; used in command authorization.
NAS-Port	5	Accounting-Request	The port number of the NAS device to which the user is connected. The Switch stores the TTY port number, or 100 for FTP connection.
NAS-Port-Type	61	Accounting-Request	The method of connection to the NAS device. The Switch stores Virtual (5) for Telnet/FTP connection or Async (0) for console connection.
Calling-Station-Id	31	Accounting-Request	The user's ID. The Switch stores the client's IPv4/IPv6 address for Telnet/FTP connection or `console` for console connection.
Acct-Status-Type	40	Accounting-Request	The timing at which the Accounting-Request was sent. The Switch stores Start (1) if sent at login, or Stop (2) if sent at logout.
Acct-Delay-Time	41	Accounting-Request	The length of time (in seconds) taken to send the `Accounting-Request` after an event requiring this attribute to be sent has occurred.
Acct-Session-Id	44	Accounting-Request	A character string for identifying the session. The Switch stores the session's process ID.
Acct-Authentic	45	Accounting-Request	The manner in which the user was authenticated. The Switch stores three authentication types: RADIUS (1), Local (2), or Remote (3).
Acct-Session-Time	46	Accounting-Request (only when Acct-Status-Type is Stop)	The length of time (in seconds) that the user received the service. The Switch stores the time (in seconds) from successful login until logout.

- `Access-Request` packet

  No attributes other than those listed above are attached to `Access-Request` packets sent by the Switch.

- `Access-Accept`, `Access-Reject`, and `Accounting-Response` packets

Attributes other than those listed above are ignored by the Switch if attached to the packet.

(3) Scope of TACACS+ implementation

The Switch supports the following NAS functionality for communication with a TACACS+ server:

Table 10-6: Scope of TACACS+ implementation

Category		Description
Packet type		Support for the following packet types used in login authentication and authentication when changing to administrator mode (by the `enable` command): • Authentication Start (send) • Authentication Reply (receive) • Authentication Continue (send) Support for the following command authorization packet types: • Authorization Request (send) • Authorization Response (receive) Support for the following accounting packet types: • Accounting Request (send) • Accounting Reply (receive)
Login authentication	Attribute	• User • Password • priv-lvl
Authentication when changing to administrator mode (by the `enable` command)		
Command authorization	Service	• taclogin
	Attribute	• class • allow-commands • deny-commands
Accounting	Flag	• TAC_PLUS_ACCT_FLAG_START • TAC_PLUS_ACCT_FLAG_STOP
	Attribute	• task_id • start_time • stop_time • elapsed_time • timezone • service • priv-lvl • cmd

(a) Description of supported TACACS+ attributes

The table below describes the TACACS+ attributes used in authentication, command authorization, and accounting.

To perform command authorization using a TACACS+ server, you must set up the server in advance so that it returns a `class` attribute or an `allow-commands` or `deny-commands` attribute with the requested service when a user is authenticated. For details about command authorization, see *10.2.4 RADIUS or TACACS+ and local command authorization*.

Table 10-7: Supported TACACS+ attributes

Service	Attribute	Description
--	User	The name of the user being authenticated. Sends the login user name when login authentication is performed. Following *Table 10-10: User name attributes to be set* sends the user name when authentication is performed to go into administrator mode (by the `enable` command).
	Password	The password of the user being authenticated, sent in encrypted form
	priv-lvl	The privilege level of the user being authenticated. 1 is used for login authentication. 15 is used for authentication when changing to administrator mode (by the `enable` command).
taclogin	class	Command class
	allow-commands	Authorized command list
	deny-commands	Unauthorized command list

Legend: --: Not applicable

The following table describes the TACACS+ flags for accounting services.

Table 10-8: TACACS+ accounting flags

Flag	Description
TAC_PLUS_ACCT_FLAG_START	Indicates `Accounting START` packets. However, if the `stop-only` transmission mode is specified in the `aaa` configuration entry, no `Accounting START` packets will be sent.
TAC_PLUS_ACCT_FLAG_STOP	Indicates `Accounting STOP` packets. However, if the `stop-only` transmission mode is specified in the `aaa` configuration entry, only `Accounting STOP` packets will be sent.

The following table describes the values of the TACACS+ attribute-value pairs used for accounting.

Table 10-9: TACACS+ accounting attribute-value pairs

Attribute	Value
task_id	The ID assigned to the event. The Switch stores process IDs for accounting events.
start_time	The time at which the event started. The Switch stores the times at which each accounting event was started. This attribute is stored when the following events occur: • In `start-stop` transmission mode: At login and before command execution • In `stop-only` transmission mode: Before command execution
stop_time	The time at which the event ended. The Switch stores the times at which each accounting event ended. This attribute is stored when the following events occur: • In `start-stop` transmission mode: At logout and after command execution • In `stop-only` transmission mode: At logout
elapsed_time	The elapsed time (in seconds) after the event started. The Switch stores the length of time (in seconds) from the start to the end of accounting events. This attribute is stored when the following events occur: • In `start-stop` transmission mode: At logout and after command execution • In `stop-only` transmission mode: At logout

Attribute	Value
timezone	A string representing the time zone
service	The character string `shell`
priv-lvl	Privilege level 1 if using an operation command when setting up command accounting, or level 15 if using a configuration command
cmd	The command string (maximum 250 characters) entered when setting up command accounting

10.2.3 Authentication using RADIUS or TACACS+

This section describes authentication methods when using RADIUS or TACACS+.

(1) Selecting the authentication service

You can specify multiple services for login authentication and for authentication when changing to administrator mode (by the `enable` command). Specifiable services cover RADIUS and TACACS+ authentication, and login security functions implemented in the Switch by the `adduser` and `password` commands.

These authentication methods can be specified singly or in combination. When multiple authentication methods are specified, the configuration command with end-by-reject set (see below) can change the behavior of the authentication service performed when the first-specified authentication method fails.

For login authentication

```
aaa authentication login end-by-reject
```

For authentication when changing to administrator mode (by the `enable` command)

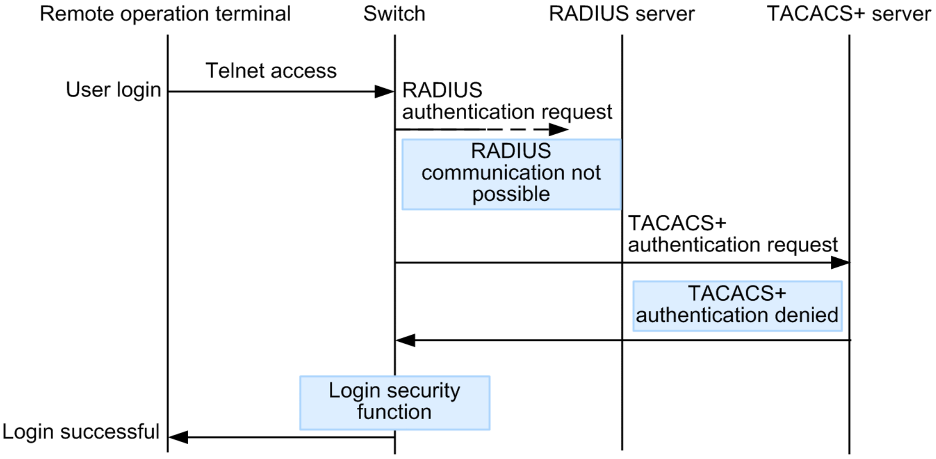
```
aaa authentication enable end-by-reject
```

(a) When end-by-reject is not set

The following explains how an authentication service is selected when end-by-reject is not set. If authentication fails when using the first specified method when end-by-reject is not set, authentication can be performed using the next specified method regardless of the reason of failure.

As an example, the figure below shows the sequence in which authentication is performed when RADIUS, TACACS+, and individual login security methods are specified and performed in that order. The authentication results are as follows: The RADIUS server cannot communicate, the TACACS+ server denies authentication, and authentication succeeds through the login security function.

Figure 10-13: Sequence of authentication (without end-by-reject specified)


Remote operation terminal
Switch
RADIUS server
TACACS+ server
User login
Telnet access
RADIUS authentication request
RADIUS communication not possible
TACACS+ authentication request
TACACS+ authentication denied
Login security function
Login successful

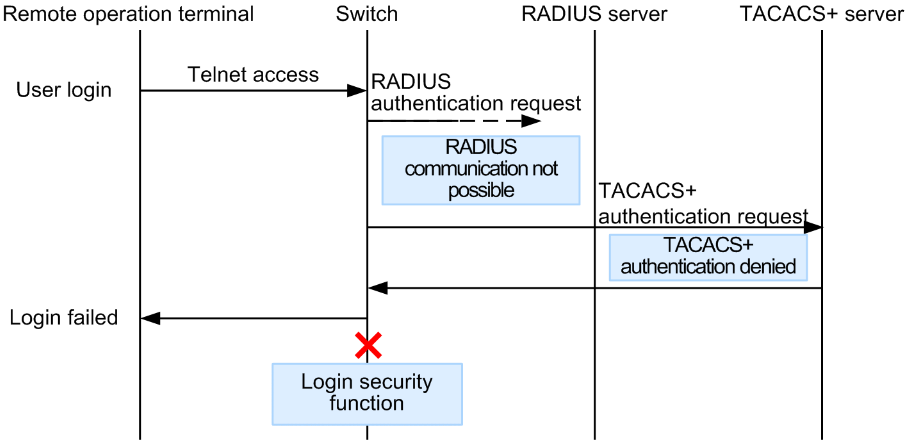
In this figure, the user accesses the Switch via Telnet from a remote operation terminal, and the Switch requests the RADIUS server to perform authentication. If the RADIUS authentication fails due to a communication failure, the Switch requests the TACACS+ server to perform authentication. If TACACS+ authentication fails because the TACACS+ server denied the request, the Switch performs authentication using the local login security functions. At this point, authentication is successful and the user is able to log in to the Switch.

(b) When end-by-reject is set

The following explains how an authentication service is selected when end-by-reject is set. If authentication fails when using the first specified method when end-by-reject is set, authentication is not performed using the next specified method. The entire authentication process is terminated at the first denial and is treated as a failure. The next authentication is performed only when authentication failed due to an abnormality such as communication failure.

As an example, the figure below shows the sequence in which authentication is performed when RADIUS, TACACS+, and individual login security methods are specified and performed in that order. The authentication results are as follows: The RADIUS server cannot communicate, and the TACACS+ server denies authentication.

Figure 10-14: Sequence of authentication (with end-by-reject specified)


Remote operation terminal
Switch
RADIUS server
TACACS+ server
User login
Telnet access
RADIUS authentication request
RADIUS communication not possible
TACACS+ authentication request
TACACS+ authentication denied
Login failed
Login security function

In this figure, the user accesses the Switch via Telnet from a remote operation terminal, and the Switch requests the RADIUS server to perform authentication. If the RADIUS authentication fails due to a communication failure, the Switch requests the TACACS+ server to perform authentication. The entire authentication process fails when authentication is denied by the TACACS+ server. The login security functionality of this Switch that is specified as the next method is not performed. As a result, the user fails to log in to the Switch.

(2) Selecting the RADIUS or TACACS+ server

You can specify a maximum of four RADIUS servers and four TACACS+ servers. If one server is unreachable and its authentication service is unavailable, each of the other servers are attempted in turn.

When the RADIUS or TACACS+ servers are specified by host name and multiple addresses can be resolved, a single address is determined in order of priority and that server is communicated with.

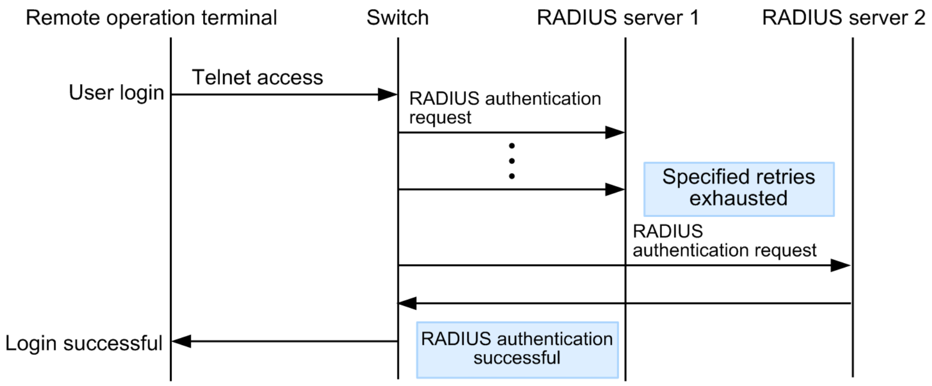
For details about order of priority, see *12.1 Description* in *12. Host Names and DNS*.

Notes

If you are using a DNS server to resolve host names, communication with the server can take a long time. For this reason, we recommend that you specify the RADIUS or TACACS+ servers by IP address.

You can set a timeout period after which a RADIUS or TACACS+ server is judged unreachable. The default is 5 seconds. If a RADIUS server times out, another attempt is made to connect to it. You can set the maximum number of connection retries that the server makes with each server (3 by default). Thus, the maximum length of time until RADIUS login authentication is deemed unavailable is given by the equation: (*timeout-period*) x (*number-of-retries*) x (*number-of-configured-RADIUS-servers*). Reconnecting to a TACACS+ server is not attempted. Thus, the maximum length of time until TACACS+ login authentication is deemed unavailable is given by the equation:(*timeout-period*) x (*number-of-configured-TACACS+-servers*). The following figure shows the RADIUS server selection sequence.

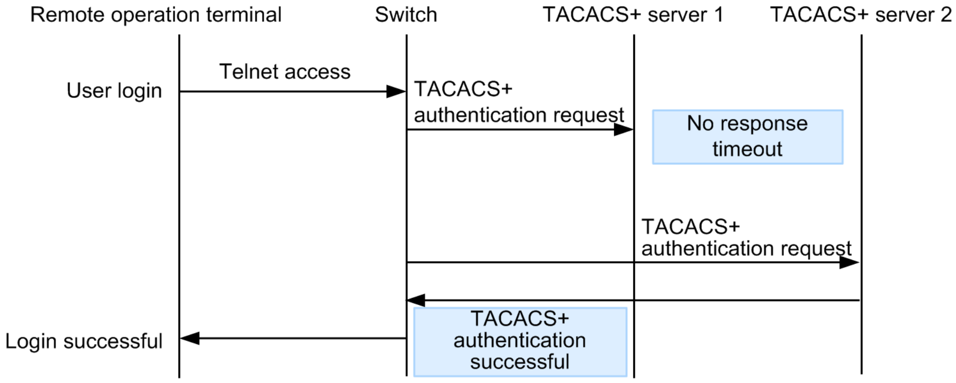
Figure 10-15: RADIUS server selection sequence


Remote operation terminal
Switch
RADIUS server 1
RADIUS server 2
User login
Telnet access
RADIUS authentication request
Specified retries exhausted
RADIUS authentication request
Login successful
RADIUS authentication successful

In this figure, the user accesses the Switch via Telnet from a remote operation terminal, and the Switch requests RADIUS server 1 to perform authentication. If RADIUS server 1 is unreachable, the RADIUS authentication request is sent to RADIUS server 2. At this point, authentication is successful and the user is able to log in to the Switch.

The following figure shows the TACACS+ server selection sequence.

Figure 10-16: TACACS+ server selection sequence


Remote operation terminal
Switch
TACACS+ server 1
TACACS+ server 2
User login
Telnet access
TACACS+ authentication request
No response timeout
TACACS+ authentication request
TACACS+ authentication successful
Login successful

In this figure, the user accesses the Switch via Telnet from a remote operation terminal, and the Switch requests TACACS+ server 1 to perform authentication. If TACACS+ server 1 is unreachable, the TACACS+ authentication request is sent to TACACS+ server 2. At this point, authentication is successful and the user is able to log in to the Switch.

(3) Registering information with a RADIUS or TACACS+ server

(a) For login authentication

Register the user name and password with the RADIUS or TACACS+ server. A user name can be registered in either of two ways:

- User name already registered in the Switch by the `adduser` command

  Login processing is based on the user information registered in the Switch.

- Unregistered user name

  Login processing is based on the following common user information:

  - User ID: remote_user
  - Home directory: /usr/home/remote_user

Note the following when an unregistered user logs in:

- File management

  All created files are managed under the `remote_user` ID, which means that other users will be able to read and write to them. Manage files carefully, for example by storing important files outside the network by FTP or other means.

(b) For authentication when changing to administrator mode (enable command)

Register the following user information for changing to administrator mode (by the `enable` command):

- User name

  This Switch sends the user names shown in the table below to the server as user name attributes. The user names to be sent can be changed using configuration commands. Register the corresponding user names with the server.

Table 10-10: User name attributes to be set

Command name	User name	
	RADIUS authenticatio n	TACACS+ authentication
Not set	admin	admin
aaa authentication enable attribute-user-per-method	$enab15$	Login user name

- Privilege level

  The privilege level is fixed at 15.

However, some servers use specific names (e.g. `$enab15$`) regardless of the sent user name attributes, and in some cases, privilege level registration is not necessary. For details, see your server documentation.

10.2.4 RADIUS or TACACS+ and local command authorization

This section describes command authorization using RADIUS or TACACS+ and local command authorization.

(1) Overview of command authorization

You can restrict the types of operation commands available to a login user who has been authenticated by a RADIUS server, TACACS+ server, or local password. This is known as command authorization. The operation commands that the user is allowed to use are controlled according to a command class or command lists obtained from the RADIUS or TACACS+ server or set in the local configuration. Operation commands that the user is not allowed to use do not appear among the character strings presented by command line completion. When a partially entered operation command contains a parameter with a value or character string, such as <*option*> or <*Host Name*>, the parameter part does not appear among the displayed entry completion strings.

Figure 10-17: RADIUS or TACACS+ login authentication and command authorization

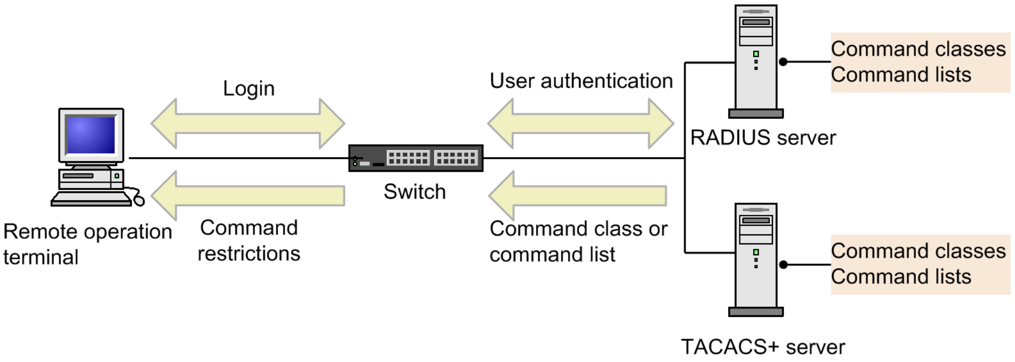
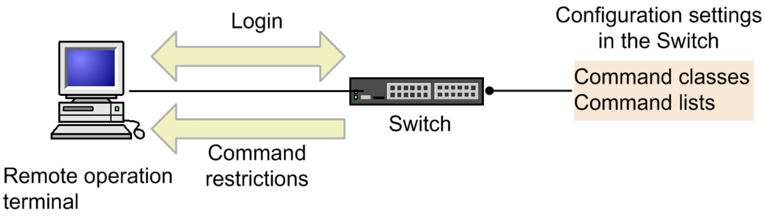


Figure 10-18: Local login authentication and command authorization


Login
Configuration settings in the Switch
Command classes
Command lists
Switch
Remote operation terminal
Command restrictions

When command authorization is configured in the `aaa` configuration entries and RADIUS or

TACACS+ authorization is specified, the command lists for the user are retrieved from the server concurrently with login authentication. If local command authorization is specified, the command lists set in the configuration entries are obtained concurrently with the login authentication. The Switch permits or denies operation commands entered by the login user according to these command lists.

Figure 10-19: Sequence of RADIUS or TACACS+ command authorization

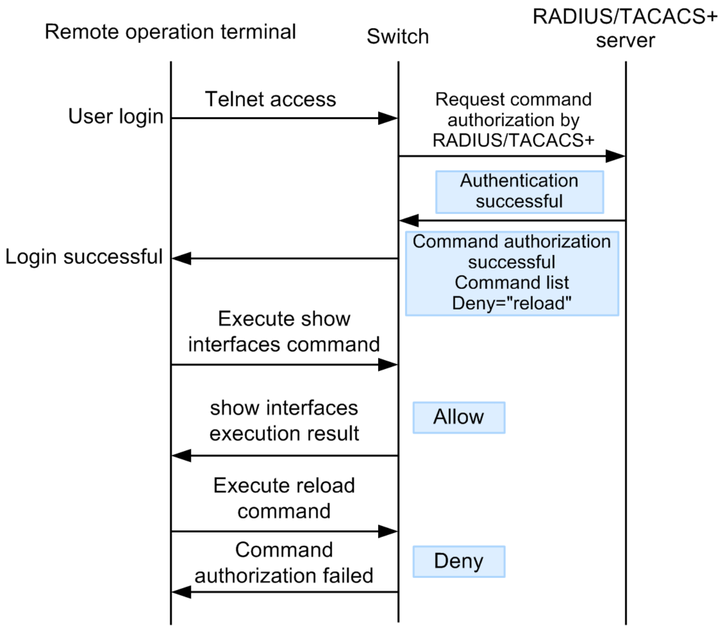
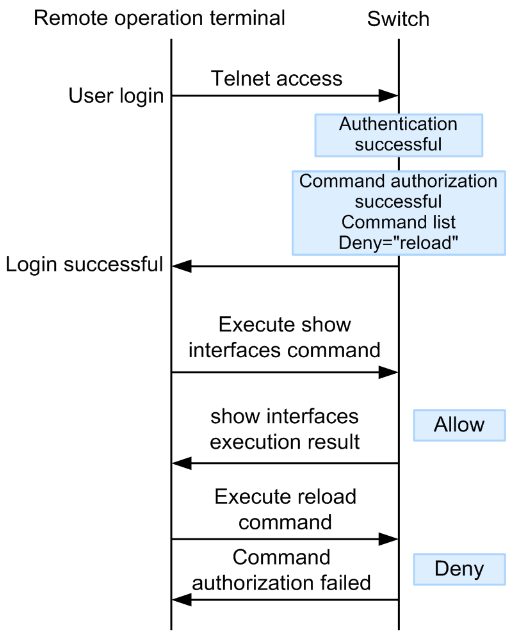

Remote operation terminal
Switch
RADIUS/TACACS+ server
User login
Telnet access
Request command authorization by RADIUS/TACACS+
Authentication successful
Login successful
Command authorization successful Command list Deny="reload"
Execute show interfaces command
show interfaces execution result
Allow
Execute reload command
Command authorization failed
Deny

Figure 10-20: Sequence of local command authorization


Remote operation terminal
Switch
User login
Telnet access
Authentication successful
Command authorization successful Command list Deny="reload"
Login successful
Execute show interfaces command
show interfaces execution result
Allow
Execute reload command
Command authorization failed
Deny

In *Figure 10-19: Sequence of RADIUS or TACACS+ command authorization*, the user accesses the Switch via Telnet from a remote operation terminal, and the Switch requests the RADIUS or TACACS+ server to perform authentication and command authorization. Authentication succeeds, the associated command lists are retrieved from the server, and the user logs in to the Switch.

In *Figure 10-20: Sequence of local command authorization*, the user accesses the Switch via Telnet from a remote operation terminal and the Switch performs local authentication.

Authentication succeeds, the associated command lists are obtained from the local configuration, and the user logs in to the Switch.

After login, the user can execute operation commands such as `show interfaces` on the Switch. The `reload` operation command cannot be executed, however, because it is included in the unauthorized command list.

Note:

> Any changes you make to a command list on the RADIUS or TACACS+ server, or to a locally configured command list, apply after the next login authentication.

(2) Setup procedures for RADIUS or TACACS+ and local command authorization

To use RADIUS or TACACS+ command authorization, set up a RADIUS or TACACS+ server and the Switch as follows:

1. Decide your policies for restricting command execution.

   Decide for each user which operation commands to permit and which to restrict.

2. Create command lists.

   In addition to specifying a command class, you can set up separate lists of authorized commands and unauthorized commands.

3. Set up a RADIUS or TACACS+ server.

   On the RADIUS or TACACS+ remote authentication server, perform the settings for authorizing commands based on your command restriction policies.

4. Set up remote authentication on the Switch.

   Configure RADIUS or TACACS+ authentication and complete the `aaa` configuration tasks.

5. Test the command authorization to make sure it works.

   Log in to the Switch from a remote operation terminal that is set up for RADIUS or TACACS+ authentication, and make sure that entered commands are permitted or denied correctly.

To use local command authorization, set up the Switch as follows:

1. Decide your policies for restricting command execution.

   Decide for each user which operation commands to permit and which to restrict.

2. Create command lists.

   You can specify a command class, or you can enter authorized and unauthorized commands in separate command lists. Configure each command list based on your command restriction policies.

   There is no need to create any command lists if you are using command classes only.

3. Assign a command class or command lists to each user.

   Enter the `username` configuration command for each user, specifying the appropriate command class or command lists.

   When you have finished, complete the `aaa` configuration tasks.

4. Test the command authorization to make sure it works.

   Log in to the Switch by local authentication, and check that commands are permitted or denied correctly.

(3) Deciding your command restriction policies

Decide for each user which operation commands to permit and which to restrict. This means that each user, once logged in, will be allowed to use some commands but not others. For details about setting command restriction policies, see *(5) Settings required for RADIUS or TACACS+ and local command authorization*.

A command restriction policy applies only to operation commands. It does not apply to undocumented debugging commands (such as the `ps` command) which are always unauthorized. (If you ever need to set permission for debugging commands, specify the `root` unrestricted command class described below.) The `logout`, `exit`, `quit`, `disable`, `end`, `set terminal`, `show whoami`, and `who am i` commands are always permitted.

The following policies are pre-defined in the Switch. By selecting one of these standard command classes, you can set the command restrictions associated with that class.

Table 10-11: Command classes

Command class	Authorized command	Unauthorized command
root Unrestricted access to all commands	All commands (including undocumented debugging commands) with no authorization required	None
allcommand Unrestricted access to all operation commands	All operation commands "all"	None (except undocumented debugging commands)
noconfig No configuration changes permitted (no authority to execute configuration commands)	Operation commands except those in the next column	"config, copy, erase configuration"
nomanage No user management commands permitted	Operation commands except those in the next column	"adduser, rmuser, clear password, password, killuser"
noenable No commands requiring administrator privilege permitted	Operation commands except those in the next column	"enable"

In addition to specifying a command class, you can specify an authorized command list and unauthorized command list.

(4) Setting command lists

In addition to specifying a command class, you can set up separate lists of authorized commands and unauthorized commands. When entering commands in each list, be aware of any spaces required in the command strings and separate each command with a comma (`,`). To create a command list for local command authorization, specify each command in a separate `commands exec` configuration command. The entered commands, linked with commas, are used on the Switch as a command list.

It is determined whether any of the command strings in the command lists match the initial character string of the command entered by the user (match beginning). As a special character, you can specify `all` in a command list, which means all operation commands.

When an entered command matches commands in both the authorized command list and unauthorized command list, the resultant action is determined by the matched command that has the greater number of characters (where `all` counts as one character). If both command lists contain the same command string, the input command is taken to be authorized.

If you specify command classes as well as authorized/unauthorized command lists, the command lists associated with each command class (the entries enclosed with double quotation marks (`"`) in *Table 10-11: Command classes*) and the specified authorized/unauthorized command lists are all subject to judgment. Also, if you specify the `root` command class, this will invalidate the authorized/unauthorized command class settings, allowing the user to execute all commands including undocumented debugging commands (such as the `ps` command).

The following seven examples show which commands will be permitted or restricted on the Switch according to the command lists set in each case.

Example 1

If you set only an authorized command list, the user is authorized to execute only the commands in that list.

Table 10-12: Command list example 1

Command list	Input by user	Judgment
Authorized command list = "show ,ping" Unauthorized command list: None set	show ip arp	Allow
	ping ipv6 ::1	Allow
	reload	Deny

Example 2

If an entered command matches commands in both the authorized command list and unauthorized command list, the judgment is determined by the matched command that has the greater number of characters (where `all` counts as one character).

Table 10-13: Command list example 2

Command list	Input by user	Judgment
Authorized command list = "show ,ping ipv6" Unauthorized command list = "show ip,ping"	show system	Allow
	show ipv6 neighbors	Deny
	ping ipv6 ::1	Allow
	ping 10.10.10.10	Deny

Example 3

If you set both authorized and unauthorized command lists, entered commands that match neither list are taken to be authorized.

Table 10-14: Command list example 3

Command list	Input by user	Judgment
Authorized command list = "show" Unauthorized command list = "reload"	ping 10.10.10.10	Allow
	reload	Deny

Example 4

If the same command string appears in both the authorized and unauthorized command lists, the command is taken to be authorized.

Table 10-15: Command list example 4

Command list	Input by user	Judgment
Authorized command list = "show" Unauthorized command list = "show ,ping"	show system	Allow
	ping ipv6 ::1	Deny

Example 5

If you do not set any command lists, all entered commands except `logout` and some others are denied.

Table 10-16: Command list example 5

Command list	Input by user	Judgment
Authorized command list: None set Unauthorized command list: None set	All commands	Deny
	logout, exit, quit, disable, end, set terminal, show whoami, who am i	Allow

Example 6

The `root` command class allows all commands to be executed with no authorization required. If you specify `root`, the authorized/unauthorized command class settings are invalidated, and the user can execute all commands including undocumented debugging commands (such as the `ps` command).

Table 10-17: Command list example 6

Command list	Input by user	Judgment
Command class = "root"	All commands (including undocumented debugging commands)	Allow

Example 7

If you set only an unauthorized command list, the user is authorized to execute all operation commands that do not match those in the list.

Table 10-18: Command list example 7

Command list	Input by user	Judgment
Authorized command list: None set Unauthorized command list = "reload"	All operation commands except reload	Allow
	reload	Deny

To illustrate how command authorization is implemented, assume that the following command restriction policies have been decided:

Table 10-19: Examples of command restriction policies

User name	Command class	Authorized commands	Unauthorized commands
staff	allcommand	All operation commands	None

User name	Command class	Authorized commands	Unauthorized commands
guest	None	All operation commands except those in the next column	Reload ...# Inactivate ...# Enable ...#
test	None	show ip ...# (show ipv6 ... is unauthorized)	All operation commands except those in the previous column

#: The ellipsis (...) represents a parameter (for example, `show ip...` might represent `show ip arp`).

(5) Settings required for RADIUS or TACACS+ and local command authorization

Based on the example command restriction policies in *Table 10-19: Examples of command restriction policies*, enter settings on the RADIUS or TACACS+ remote authentication server, additional to the usual login authentication settings, to implement command restrictions based on the attribute values described in the table below.

Note that if command authorization has not been configured on the server side, after authentication and successful login from a remote operation terminal you will not be authorized to execute any commands except `logout`, `exit`, `quit`, `disable`, `end`, `set terminal`, `show whoami`, and `who am i`. In this case, log in from the console.

If command authorization has also been implemented on the console by the `aaa authorization commands console` configuration command, perform a default restart and then log in.

- When using RADIUS servers

To implement command authorization with a RADIUS server, set up the server so that the following attributes will be returned at authentication.

Table 10-20: RADIUS setup attributes

Attribute	Vendor-specific attribute	Value
25 Class	--	Class Specify one of the following strings: `root`, `allcommand`, `noconfig`, `nomanage`, or `noenable`
26 Vendor-Specific Vendor-ID: 21839	ALAXALA-Allow-Commands Vendor type: 101	Authorized command list Specify the initial string of each of the authorized commands to be matched, separated by commas (`,`). Spaces are also matched. Use `"all"` to specify every operation command. When an authorized command list alone is set, all commands other than those in the list are prohibited. Example: `ALAXALA-Allow-Commands="show ,ping ,telnet "`
	ALAXALA-Deny-Commands Vendor type: 102	Unauthorized command list Specify the initial string of each of the unauthorized commands to be matched, separated by commas (`,`). Spaces are also matched. Use `"all"` to specify every operation command. When an unauthorized command list alone is set, all commands other than those in the list are permitted. Example: `ALAXALA-Deny-Commands="enable,reload, inactivate"`

Legend: --: Not applicable

Set these vendor-specific attributes in a `dictionary` file or other configuration file to register them with the RADIUS server.

Figure 10-21: Example of registering vendor-specific attributes in a dictionary file for a RADIUS server

```
VENDOR          ALAXALA                     21839
ATTRIBUTE       ALAXALA-Allow-Commands      101      string  ALAXALA
ATTRIBUTE       ALAXALA-Deny-Commands       102      string  ALAXALA
```

The following figure shows an example of implementing the policies determined in *Table 10-19: Examples of command restriction policies* in a typical RADIUS server.

Figure 10-22: Example of RADIUS server setup

```
staff  Password = "******"
       Class = "allcommand"                                ...1


guest  Password = "******"
       Alaxala-Deny-Commands = "enable,reload,inactivate"   ...2


test  Password = "******"
      Alaxala-Allow-Commands = "show ip "                  ...3
```

Note: The asterisks (`******`) represent the user password.

1. The `allcommand` class permits all operation commands.
2. Prohibits commands beginning with `enable`, `reload`, or `inactivate`.

   Because `allow-commands` is not specified, all other commands are permitted.
3. Spaces are meaningful.

   Because `show ip` is followed by a space, commands such as `show ip arp` are permitted, but commands such as `show ipv6 neighbors` are not.

   All other commands are prohibited.

Notes

- When multiple `Class` entries are received on the Switch, the first entry is recognized and subsequent entries are ignored.

Figure 10-23: Example of setting multiple Class entries

```
Class = "noenable"                                           ...1

Class = "allcommand"
```

1. Only the first `noenable` is valid.

- When multiple class names are registered in the `Class` entry on the Switch, the first class name is recognized and subsequent class names are ignored. For example, if you enter `class="nomanage,noenable"`, only `nomanage` will be valid.
- When multiple entries are received with the `ALAXALA-Deny-Commands` attribute or `ALAXALA-Allow-Commands` attribute, a maximum of 1024 characters are recognized, including commas (`,`) and spaces. Subsequent characters are ignored. Also, if you specify multiple entries for the same attribute as in the example below, a comma (`,`) will be automatically placed in front of each entry on receipt of the second and subsequent entries.

Figure 10-24: Example of setting multiple Deny-Commands entries

```
ALAXALA-Deny-Commands = "inactivate,reload"                  ...1

ALAXALA-Deny-Commands = "activate,test,..........."          ...1
```

1. The Switch can recognize the underlined parts up to a total of 1024 characters.

As shown in the figure below, when the above `Deny-Commands` entries are received, a comma (`,`) is automatically placed in front of the `activate` command which is the first command in the second entry.

```
Deny-Commands =
"inactivate,reload,activate,test,........."
```

- When using TACACS+ servers

To implement command authorization with a TACACS+ server, set attribute-value pairs as shown below.

Table 10-21: TACACS+ setup attributes

Service	Attribute	Value
taclogin	class	Command class Specify one of the following strings: `root`, `allcommand`, `noconfig`, `nomanage`, or `noenable`
	allow-commands	Authorized command list Specify the initial string of each of the authorized commands to be matched, separated by commas (`,`). Spaces are also matched. Use `"all"` to specify every operation command. When an authorized command list alone is set, all commands other than those in the list are prohibited. Example: `allow-commands="show ,ping ,telnet "`
	deny-commands	Unauthorized command list Specify the initial string of each of the unauthorized commands to be matched, separated by commas (`,`). Spaces are also matched. Use `"all"` to specify every operation command. When an unauthorized command list alone is set, all commands other than those in the list are permitted. Example: `deny-commands="enable,reload,inactivate"`

The following figure shows an example of implementing the policies determined in *Table 10-19: Examples of command restriction policies* in a typical TACACS+ server.

Figure 10-25: Example of TACACS+ server setup

```
user=staff {
    login = cleartext "******"
    service = taclogin {                                  ...1
        class = "allcommand"
    }
}


user=guest {
    login = cleartext "******"
    service = taclogin {
        deny-commands = "enable,reload,inactivate"        ...2
}


user=test {
    login = cleartext "******"
    service = taclogin {
        allow-commands = "show ip "                        ...3
}
```

Note: The asterisks (`******`) represent the user password.

1. Sets `taclogin` as the `service` name.

   The `allcommand` class permits all operation commands.

2. Prohibits commands beginning with `enable`, `reload`, or `inactivate`.

   Because `allow-commands` is not specified, all other commands are permitted.

3. Spaces are meaningful.

   Because `show ip` is followed by a space, commands such as `show ip arp` are permitted, but commands such as `show ipv6 neighbors` are not.

   All other commands are prohibited.

Notes

- When multiple class names are registered in the `Class` entry of the Switch, the first class name is recognized and subsequent class names are ignored. For example, if you enter `class="nomanage,noenable"`, only `nomanage` will be valid.
- For each of the `deny-commands` and `allow-commands` attributes, a maximum of 1024 characters are recognized, including commas (`,`) and spaces. Subsequent characters are ignored.

■ When using local command authorization

The following figure shows an example of implementing the policies determined in *Table 10-19: Examples of command restriction policies* in a local authorization scenario.

Figure 10-26: Example of configuring local command authorization

```
username guest view guest_view
username staff view-class allcommand                       ...1
username test view test_view
!
parser view guest_view
  commands exec exclude all "enable"                       ...2
  commands exec exclude all "inactivate"                   ...2
  commands exec exclude all "reload"                       ...2
!
parser view test_view
  commands exec include all "show ip "                     ...3
!
aaa authentication login default local
aaa authorization commands default local
```

1. Assigns the `allcommand` class to the user `staff`, permitting all operation commands.

2. Prohibits commands beginning with `enable`, `inactivate`, or `reload`.

   Because `commands exec include` is not specified, all other commands are permitted.

3. Spaces are meaningful.

   Because `show ip` is followed by a space, commands such as `show ip arp` are permitted, but commands such as `show ipv6 neighbors` are not.

   All other commands are prohibited.

(a) Testing the setup

Having completed the above setup, log in to the Switch from a remote operation terminal that uses

RADIUS or TACACS+ or local command authorization. After you log in, execute the `show whoami` command to make sure that the command lists are set, and then execute one or two commands to make sure they are permitted or denied correctly.

Figure 10-27: Example of login and testing by the user "staff"

```
> show whoami
Date 20XX/01/07 12:00:00 UTC
staff ttyp0    -----  2   Jan  6 14:17 (10.10.10.10)

Home-directory: /usr/home/staff
Authentication: TACACS+ (Server 192.168.10.1)
Class: allcommand
      Allow: "all"
      Deny : -----
Command-list: -----
>
> show clock
Wed Jan 7 12:00:10 UTC 20XX
> /bin/date
% Command not authorized.
>
```

Figure 10-28: Example of login and testing by the user "guest"

```
>show whoami
Date 20XX/01/07 12:00:00 UTC
guest ttyp0    -----  2   Jan  6 14:17 (10.10.10.20)

Home-directory: /usr/home/guest
Authentication: RADIUS (Server 192.168.10.1)
Class: -----
Command-list:
      Allow: -----
      Deny : "enable,reload,inactivate"
>
> show clock
Wed Jan 7 12:00:10 UTC 20XX
> reload
% Command not authorized.
>
```

Figure 10-29: Example of login and testing by the user "test"

```
>show whoami
Date 20XX/01/07 12:00:00 UTC
test ttyp0    -----  2   Jan  6 14:17 (10.10.10.30)

Home-directory: /usr/home/test
Authentication: LOCAL
Class: -----
Command-list:
      Allow: "show ip "
      Deny : -----
>
> show ip arp
***The command is executed.***
> show ipv6 neighbors
% Command not authorized.
>
```

10.2.5 RADIUS and TACACS+ accounting

This section describes RADIUS and TACACS+ accounting methods.

(1) Setting up accounting

By configuring RADIUS or TACACS+ and `aaa accounting`, you can set up the Switch to send accounting information to the RADIUS or TACACS+ server whenever a user logs in or logs out from a remote operation terminal. Accounting information will also be sent to the TACACS+ server at every command input to the Switch.

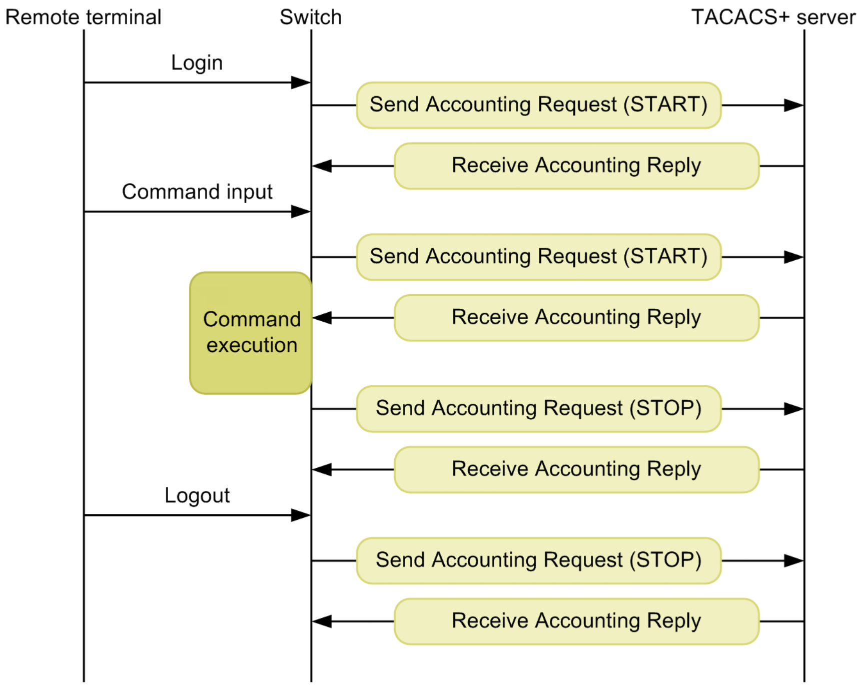
Two types of accounting can be configured: login accounting for sending login and logout events to the server, and command accounting for sending command input events. Command accounting is supported only by TACACS+.

For each type of accounting, you can select either start-stop mode which sends both START and STOP accounting notices, or stop-only mode which sends STOP notices only. For command accounting, you can choose to report all entered commands or only configuration commands. Normally, records are sent to each RADIUS or TACACS+ server in turn, as long as each server is available and until accounting is successful, but you can also choose to broadcast accounting records to all the servers regardless of success or failure.

(2) Accounting flow

The following figure shows the processing sequence when the system is configured to send accounting notices to a TACACS+ server in START-STOP transmission mode for both login accounting and command accounting.

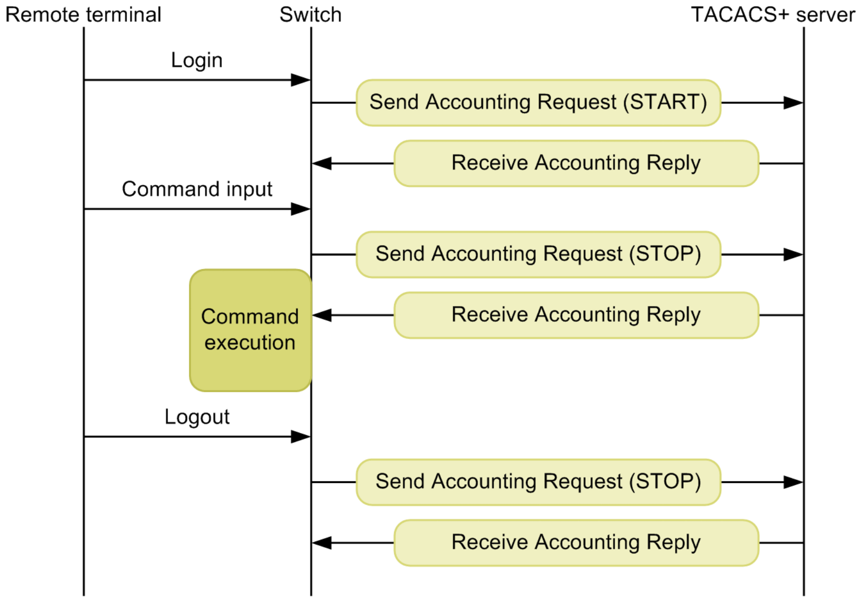
Figure 10-30: TACACS+ accounting sequence (login and command accounting in START-STOP transmission mode)



In this figure, when a user successfully logs in from a remote operation terminal, accounting information such as user data and timestamps is sent from the Switch to the TACACS+ server. In addition, command accounting information is forwarded before and after every command executed by the user. Finally, when the user logs out, information such as the duration of the session is sent.

The following figure shows the processing sequence when the system is configured to send accounting notices to a TACACS+ server in START-STOP transmission mode for login accounting, and in STOP-ONLY transmission mode for command accounting.

Figure 10-31: TACACS+ accounting sequence (login accounting in START-STOP mode; command accounting in STOP-ONLY)



The login-logout accounting behavior here is the same as the example in *Figure 10-30: TACACS+ accounting sequence (login and command accounting in START-STOP transmission mode)*, but because STOP-ONLY transmission mode is specified for command accounting, command-related accounting information is sent from the Switch to the TACACS+ server before command execution only.

(3) Notes

When you configure RADIUS or TACACS+ accounting and `aaa accounting`, or change the IPv4 device address using the `interface loopback` command, accounting events being sent or received, unsent events, and statistical records are cleared and the accounting sequence follows the new settings.

If numerous users are entering commands and logging in and out in succession, some accounting events might not be logged due to the large volume of generated events.

To avoid overloading the Switch, servers, and network with a large volume of accounting events, we recommend that you set STOP-ONLY mode for command accounting. Take care not to specify a RADIUS or TACACS+ server that is likely to be unreachable.

If you clear the accounting statistics using the `clear accounting` operation command, the service will recommence recording statistics about accounting events sent to the servers only when the accounting events that were being sent to a server when the `clear accounting` command was executed have been successfully transmitted.

If you are using a DNS server to resolve host names, communication with the server can take a long time. For this reason, we recommend that you specify the RADIUS and TACACS+ servers by IP address.

10.2.6 Connecting with RADIUS or TACACS+

(1) Connecting to RADIUS servers

(a) Switch identification on the RADIUS server side

RADIUS protocol states that the source IP address of the request packet must be used as the key for identifying the NAS. The Switch uses the following types of address as the source IP address of a request packet:

- If a local address is set by the `interface loopback 0` configuration command, the local address is used as the source IP address.
- If a local address is not set, the IP address of the sending interface is used.

Therefore, if the local address is set, that IP address must be used to register the Switch with the RADIUS server. By setting the local address, the RADIUS server will be able to reliably identify the Switch from the registered information, if the interface for communicating with the RADIUS server were unidentifiable.

(b) RADIUS server messages

In some cases, the RADIUS server attaches a `Reply-Message` attribute to a response and sends a message to the requestor. The Switch outputs the contents of the `Reply-Message` attribute to an operation log. If authentication by the RADIUS server fails, check this operation log.

(c) Port number of the RADIUS server

Port 1812 is assigned to the RADIUS authentication service in RFC 2865. Unless otherwise specified, the Switch uses port 1812 in requests sent to a RADIUS server. However, some RADIUS servers still use port 1645, which was used in early implementations. For a RADIUS server of this type, specify 1645 in the `auth-port` parameter of the `radius-server host` configuration command. Because you can specify any value from 1 to 65535 in the `auth-port` parameter, the RADIUS server is supported regardless of the specified port.

(2) Connecting with a TACACS+ server

(a) TACACS+ server setup

- Take care with the service and attribute name settings when connecting the Switch with a TACACS+ server. For TACACS+ server attributes, see *10.2.4 RADIUS or TACACS+ and local command authorization*.
- If a local address is set by the `interface loopback 0` configuration command, the local address is used as the source IP address.

10.3 RADIUS and TACACS+ configurations

10.3.1 List of configuration commands

The following tables describe the configuration commands for RADIUS or TACACS+ and accounting services.

Table 10-22: Configuration commands (RADIUS)

Command name	Description
radius-server host	Sets a RADIUS server for authentication, authorization, and accounting purposes.
radius-server key	Sets a RADIUS server key for authentication, authorization, and accounting purposes.
radius-server retransmit	Sets the maximum number of retransmissions to a RADIUS server used for authentication, authorization, and accounting purposes.
radius-server timeout	Sets a response timeout value for a RADIUS server used for authentication, authorization, and accounting purposes.

Table 10-23: Configuration commands (TACACS+)

Command name	Description
tacacs-server host	Sets a TACACS+ server for authentication, authorization, and accounting purposes.
tacacs-server key	Sets a shared private key for communication with a TACACS+ server used for authentication, authorization, and accounting purposes.
tacacs-server timeout	Sets a response timeout value for a TACACS+ server used for authentication, authorization, and accounting purposes.

Table 10-24: Configuration commands (accounting)

Command name	Description
aaa accounting commands	Enables command accounting.
aaa accounting exec	Enables login-logout accounting.

10.3.2 Configuring RADIUS authentication

(1) Example of configuring login authentication

Points to note

The example below shows how to configure RADIUS authentication and local authentication. Configure the settings so that local authentication is performed only when authentication failed due to an abnormality, for example, when communication with the RADIUS server fails. If authentication failed due to denial, the whole authentication process ends at that point, and no local authentication is performed.

The usual setup for remote access must be completed in advance.

Command examples

1.
```
(config)# aaa authentication login default group radius local
```

Sets RADIUS authentication and local authentication, in that order, as the authentication methods to be used when a user logs in.

2. `(config)# aaa authentication login end-by-reject`

   Configures the settings so that the whole authentication process ends when denied by RADIUS authentication and no local authentication is performed.

3. `(config)# radius-server host 192.168.10.1 key "039fkllf84kxm3"`

   Sets IP address 192.168.10.1 as the server to be used for RADIUS authentication and a shared key for communication with the server.

(2) Example of configuring authentication for changing to administrator mode (enable command)

Points to note

The example below shows how to configure RADIUS authentication and local authentication. Configure the settings so that local authentication is performed only when authentication failed due to an abnormality, for example, when communication with the RADIUS server fails. If authentication failed due to denial, the whole authentication process ends at that point, and no local authentication is performed.

Also set `$enab15$` to be sent as the user name attribute for RADIUS authentication.

Command examples

1. `(config)# aaa authentication enable default group radius enable`

   Sets RADIUS authentication and local authentication, in that order, as the authentication methods to be used when the user changes to administrator mode (by the `enable` command).

2. `(config)# aaa authentication enable end-by-reject`

   Configures the settings so that the whole authentication process ends when denied by RADIUS authentication and no local authentication is performed.

3. `(config)# aaa authentication enable attribute-user-per-method`

   Sets `$enab15$` to be sent as the user name attribute for RADIUS authentication.

4. `(config)# radius-server host 192.168.10.1 key "039fkllf84kxm3"`

   Sets IP address 192.168.10.1 as the server to be used for RADIUS authentication and a shared key for communication with the server.

10.3.3 Configuring TACACS+ authentication

(1) Example of configuring login authentication

Points to note

The example below shows how to configure TACACS+ authentication and local authentication. Configure the settings so that local authentication is performed only when authentication failed due to an abnormality, for example, when communication with the TACACS+ server fails. If authentication failed due to denial, the whole authentication process ends at that point, and no local authentication is performed.

The usual setup for remote access must be completed in advance.

Command examples

1. `(config)# aaa authentication login default group tacacs+ local`

   Sets TACACS+ authentication and local authentication, in that order, as the authentication methods to be used when a user logs in.

2. `(config)# aaa authentication login end-by-reject`

   Configures the settings so that the whole authentication process ends when denied by TACACS+ authentication and no local authentication is performed.

3. `(config)# tacacs-server host 192.168.10.1 key "4h8dlir9r-w2"`

   Sets IP address 192.168.10.1 as the server to be used for TACACS+ authentication and a shared key for communication with the server.

(2) Example of configuring the Switch for authentication when changing to administrator mode (enable command)

Points to note

The example below shows how to configure TACACS+ authentication and local authentication. Configure the settings so that local authentication is performed only when authentication failed due to an abnormality, for example, when communication with the TACACS+ server fails. If authentication failed due to denial, the whole authentication process ends at that point, and no local authentication is performed.

Also set the login user name to be sent as the user name attribute when performing TACACS+ authentication.

Command examples

1. `(config)# aaa authentication enable default group tacacs+ enable`

   Sets TACACS+ authentication and local authentication, in that order, as the authentication methods to be used when the user changes to administrator mode (by the `enable` command).

2. `(config)# aaa authentication enable end-by-reject`

   Configures the settings so that the whole authentication process ends when denied by TACACS+ authentication and no local authentication is performed.

3. `(config)# aaa authentication enable attribute-user-per-method`

   Sets the login user name to be sent as the user name attribute when performing TACACS+ authentication.

4. `(config)# tacacs-server host 192.168.10.1 key "4h8dlir9r-w2"`

   Sets IP address 192.168.10.1 as the server to be used for TACACS+ authentication and a shared key for communication with the server.

10.3.4 Configuring RADIUS or TACACS+ and local command authorization

(1) Example of configuring RADIUS command authorization

Points to note

The example below shows how to configure command authorization using a RADIUS server.

Before performing this procedure, complete the setup for using RADIUS authentication.

Command examples

1.
```
(config)# aaa authentication login default group radius local
(config)# radius-server host 192.168.10.1 key "RaD#001"
```
Configures RADIUS authentication as a prerequisite step.

2.
```
(config)# aaa authorization commands default group radius
```
Performs command authorization using a RADIUS server.

Notes

If command authorization has been configured as described above, but has not been set up on the RADIUS server side, all commands will be prohibited when the RADIUS-authenticated user logs in. If you are unable to execute any commands, because a setup task has been omitted, for example, log in from the console and complete the required setup. If command authorization has also been implemented on the console by the `aaa authorization commands console` configuration command, perform a default restart and then log in.

(2) Example of configuring TACACS+ command authorization

Points to note

The example below shows how to configure command authorization using a TACACS+ server.

Before performing this procedure, complete the setup for using TACACS+ authentication.

Command examples

1.
```
(config)# aaa authentication login default group tacacs+ local
(config)# tacacs-server host 192.168.10.1 key "TaC#001"
```
Configures authentication by a TACACS+ server as a prerequisite step.

2.
```
(config)# aaa authorization commands default group tacacs+
```
Performs command authorization using a TACACS+ server.

Notes

If command authorization has been configured as described above, but has not been set up on the TACACS+ server side, all commands will be prohibited when the TACACS+-authenticated user logs in. If you are unable to execute any commands, because a setup task has been omitted, for example, log in from the console and complete the required setup. If command authorization has also been implemented on the console by the `aaa authorization commands console` configuration command, perform a default restart and then log in.

(3) Example of configuring local command authorization

Points to note

The example below shows how to configure local command authorization.

Before performing this procedure, set the user name and the associated command class (`username view-class`) or command lists (`username view`, `parser view`, or `commands exec` command).

Also, change the settings so that local password authentication can be used.

Command examples

1.

```
(config)# parser view Local_001
(config-view)# commands exec include all "show"
(config-view)# commands exec exclude all "reload"
```

Creates the command lists to be used for local authorization.

There is no need to create any command lists if you are using command classes only.

2.

```
(config)# username user001 view Local_001
(config)# username user001 view-class noenable
```

Assigns a command class or command lists to the specified user.

Both a command class and command lists can be used together.

3.

```
(config)# aaa authentication login default local
```

Configures local password authentication.

4.

```
(config)# aaa authorization commands default local
```

Performs command authorization using local authentication.

Notes

Be aware that local command authorization applies to all users who log in with local authentication. Configure local authorization carefully so that security is not compromised.

If no command class or command list has been set for a user, no commands will be permitted or executable by that user.

If you are unable to execute any commands, because a setup task has been omitted, for example, log in from the console and complete the required setup. If command authorization has also been implemented on the console by the `aaa authorization commands console` configuration command, perform a default restart and then log in.

10.3.5 Configuring RADIUS or TACACS+ login-logout accounting

(1) Example of configuring RADIUS login-logout accounting

Points to note

The example below shows how to configure RADIUS login-logout accounting. Before you begin, complete the setup on the RADIUS server host to which the accounting records will be sent.

Command examples

1. `(config)# radius-server host 192.168.10.1 key "RaD#001"`

   Configures the RADIUS server as a prerequisite step.

2. `(config)# aaa accounting exec default start-stop group radius`

   Configures login-logout accounting.

Notes

If you set `aaa accounting exec` without first executing the `radius-server` configuration command, the operation log entry `System accounting failed` will appear whenever a user logs in or logs out. Make sure that you configure the destination RADIUS server first.

(2) Example of configuring TACACS+ login-logout accounting

Points to note

The example below shows how to configure TACACS+ login-logout accounting. Before you begin, complete the setup on the TACACS+ server host to which the accounting records will be sent.

Command examples

1. `(config)# tacacs-server host 192.168.10.1 key "TaC#001"`

   Configures the TACACS+ server as a prerequisite step.

2. `(config)# aaa accounting exec default start-stop group tacacs+`

   Configures login-logout accounting.

Notes

If you set `aaa accounting exec` without first executing the `tacacs-server` configuration command, the operation log entry `System accounting failed` will appear whenever a user logs in or logs out. Make sure that you configure the destination TACACS+ server first.

10.3.6 Configuring TACACS+ command accounting

(1) Example of configuring TACACS+ command accounting

Points to note

The example below shows how to configure TACACS+ command accounting.

Before you begin, complete the setup on the TACACS+ server host to which the accounting records will be sent.

Command examples

1. `(config)# tacacs-server host 192.168.10.1 key "TaC#001"`

   Configures the TACACS+ server as a prerequisite step.

2.
   ```
   (config)# aaa accounting commands 0-15 default start-stop group
   tacacs+
   ```

   Configures command accounting.

Notes

If you set `aaa accounting commands` without first executing the `tacacs-server` configuration command, the operation log entry `System accounting failed` will appear whenever the user enters a command. Make sure that you configure the destination TACACS+ server first.

Chapter

11. Time Settings and NTP

This chapter describes the time settings and NTP.

11.1 Setting the time and checking the NTP configuration

Set the clock time at first deployment of the Switch. Time information is used in the Switch's log entries and in timestamps when files are created. Set the correct time when you begin using the Switch. You can set the time using the `set clock` operation command.

You can also use Network Time Protocol (NTP) to synchronize the time to an NTP server on the network. The Switch is compliant with NTP version 3 as stipulated in RFC 1305.

11.1.1 Lists of configuration commands and operation commands

The following table describes the configuration commands related to time settings and NTP.

Table 11-1: List of configuration commands

Command name	Description
clock timezone	Sets the time zone.
ntp access-group	Creates an access group that can be permitted or denied access to NTP services by means of an IPv4 address filter.
ntp authenticate	Enables the NTP authentication functionality.
ntp authentication-key	Sets an authentication key.
ntp broadcast	Broadcasts NTP packets to each interface and synchronizes other devices with the Switch.
ntp broadcast client	Specifies the setting for accepting NTP broadcast messages from devices on the connected subnet.
ntp broadcastdelay	Specifies the estimated latency (time delay) between the NTP broadcast server sending time information and the Switch.
ntp master	Designates the switch as a local time server.
ntp peer	Sets NTP server symmetric active/passive mode.
ntp server	Sets client/server mode and specifies client mode for an NTP server.
ntp trusted-key	Sets a key number to perform authentication for security purposes when synchronizing with other devices.

The following table describes the operation commands related to time settings and NTP.

Table 11-2: List of operation commands

Command name	Description
set clock	Shows and sets the date and time.
show clock	Shows the current date and time.
show ntp associations	Shows the activity status of the connected NTP server.
restart ntp	Restarts the local NTP server.

11.1.2 Setting the system clock

Points to note

To set the switch's system clock, you must first set the time zone. Using the `clock timezone` configuration command, enter the appropriate country abbreviation for standard local time and specify the offset of +9 from UTC.

Command examples

1. `(config)# clock timezone JST +9`

   Sets the JST time zone and an offset of +9 from UTC.

2.
```
(config)# save
(config)# exit
```

   Saves the settings and moves from configuration mode to administrator mode.

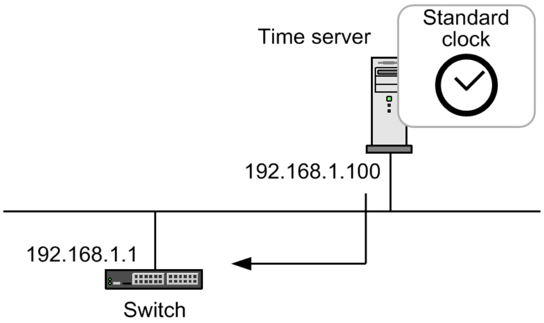
3.
```
# set clock 0506221530
Wed Jun 22 15:30:00 2005 JST
```

   Sets the date and time as `15:30 on June 22, 2005`.

11.1.3 Synchronizing a switch with the time server by NTP

Using NTP functionality, synchronize the system clock of the Switch with a time server.

Figure 11-1: NTP configuration example (synchronization with a time server)



Points to note

When multiple time servers are configured in the network, the `prefer` parameter of the `ntp server` command selects the time server for synchronizing the system clock of the Switch. If you omit the `prefer` parameter, the selected time server will be the one with the least `stratum` value, or a randomly selected time server if they all have the same `stratum` value.

Command examples

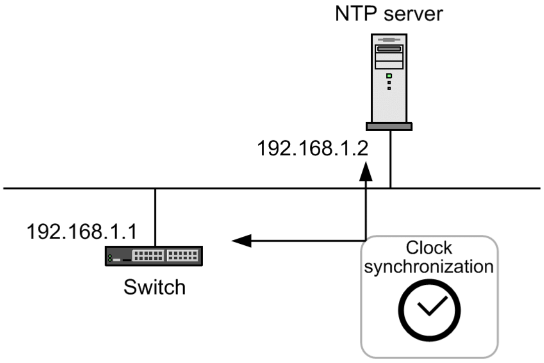
1. `(config)# ntp server 192.168.1.100`

   Synchronizes the Switch with the time server whose IP address is 192.168.1.100.

11.1.4 Synchronizing a switch with an NTP server

Using NTP functionality, synchronize the system clock of the Switch with the NTP server, adjusting both time settings.

Figure 11-2: NTP configuration example (synchronization with an NTP server)



Points to note

To synchronize the Switch with multiple NTP servers, you must configure multiple settings using the `ntp peer` command.

When multiple NTP servers are configured in the network, the `prefer` parameter of the `ntp peer` command selects the NTP server to be used for synchronizing the Switch's system clock. If you omit the `prefer` parameter, the selected NTP server will be the one with the least `stratum` value, or a randomly selected NTP server if they all have the same `stratum` value.

Command examples

1.
```
(config)# ntp peer 192.168.1.2
```
Establishes a peer relationship with the NTP server whose IP address is 192.168.1.2.

11.1.5 Configuring NTP authentication

Points to note

To synchronize the switch's clock with other devices using NTP functionality, configure authentication for security purposes.

Command examples

1.
```
(config)# ntp authenticate
```
Enables the NTP authentication functionality.

2.
```
(config)# ntp authentication-key 1 md5 NtP#001
```
Sets `NtP#001` in key number 1 as the NTP authentication key.

3.
```
(config)# ntp trusted-key 1
```
Specifies key number 1 for NTP authentication.

11.1.6 Synchronizing time on VRF by using NTP [OS-L3SA]

Use the NTP functionality to synchronize time with NTP servers and NTP clients on VRFs.

Points to note

Using the NTP functionality, synchronize the Switch's system clock with a given NTP server on a VRF. Once the Switch's system clock is synchronized to an NTP server, the Switch's system clock time can be distributed to multiple NTP clients on all VRFs including the global network.

If the clock-source NTP server and NTP clients are on different VRFs, notify the NTP clients of the referred-to host of the Switch as the local time server.

Command examples

1. `(config)# ntp server vrf 10 192.168.1.100`

   Synchronizes the Switch's system clock to the NTP server with the IP address 192.168.1.100 on VRF 10. The configuration is client/server mode.

2. `(config)# ntp peer vrf 10 192.168.1.100`

   Synchronizes the Switch's system clock to the NTP server with the IP address 192.168.1.100 on VRF 10. The configuration is symmetric active/passive mode

3. `(config)# ntp broadcast client`

   Synchronizes the Switch's system clock using NTP broadcast messages. Receives NTP broadcast messages from the NTP server to all subnets within all VRFs including the global network.

4.
   ```
   (config)# interface vlan 100
   (config-if)# vrf forwarding 20
   (config-if)# ip address 192.168.10.1 255.255.255.0
   (config-if)# ntp broadcast
   ```

   Sets NTP broadcasting to the interface with the specified VRF. Once the Switch's clock is synchronized to the NTP server, sends NTP broadcast packets to the network of VRF20, IPv4 address 192.168.10.0, subnet 255.255.255.0.

11.1.7 Note on changing the time

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

11.1.8 Checking the time

Using the `show clock` operation command, you can check the time information set in the Switch. An example is shown below:

Figure 11-3: Checking the time settings

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

When you use the NTP protocol to synchronize the switch's clock with an NTP server on the network, you can use the `show ntp associations` operation command to check the activity status of the NTP server. An example is shown below:

Figure 11-4: Checking the activity status of the NTP server

```
> show ntp associations
Date 20XX/01/23 12:00:00 UTC
  remote         refid       st t when poll reach   delay   offset    disp
==============================================================================
```

```
*timesvr    192.168.1.100    3 u    1   64  377     0.89   -2.827    0.27
>
```

Chapter

12. Host Names and DNS

This chapter explains host names and describes the Domain Name Service and its operation.

12.1 Description

Host name information for identifying other devices on the network can be set in the Switch. This information can be used to specify another networked device when configuring the Switch to perform logging, for example. You can set host name information in the Switch by using either of the following methods:

- Specify host names individually using the `ip host` or `ipv6 host` configuration command.
- Query the DNS server on the network using the DNS resolver functionality.

When setting host names by using the `ip host` or `ipv6 host` configuration command, you must explicitly associate an IP address with each host name to be used. When using the DNS resolver, there is no need to map IP addresses with referenced host names because the Switch looks them up by querying the DNS server.

If you set a host name by using the `ip host` or `ipv6 host` configuration command and also use the DNS resolver, the host name set in the configuration command takes priority. Whichever method you use, if the same host name is associated with both an IPv4 address and an IPv6 address, the IPv4 address takes priority.

The DNS resolver functionality provided by the Switch complies with RFC 1034 and RFC 1035.

12.2 Configuration

12.2.1 List of configuration commands

The following table describes the configuration commands for host names and the DNS.

Table 12-1: List of configuration commands

Command name	Description
ip domain lookup	Enables or disables the DNS resolver functionality.
ip domain name	Sets the domain name to be used by the DNS resolver.
ip host	Sets host name information mapped to an IPv4 address.
ip name-server	Sets the name server referenced by the DNS resolver.
ipv6 host	Sets host name information mapped to an IPv6 address.

12.2.2 Configuring host names

(1) Mapping a host name to an IPv4 address

Points to note

The example below shows how to map a host name to an IPv4 address.

Command examples

1. `(config)# ip host WORKPC1 192.168.0.1`

   Maps the host name `WORKPC1` to the device whose IPv4 address is 192.168.0.1.

(2) Mapping a host name to an IPv6 address

Points to note

The example below shows how to map a host name to an IPv6 address.

Command examples

1. `(config)# ipv6 host WORKPC2 3ffe:501:811:ff45::87ff:fec0:3890`

   Maps the host name `WORKPC2` to the device whose IPv6 address is 3ffe:501:811:ff45::87ff:fec0:3890.

12.2.3 Configuring DNS settings

(1) DNS resolver setting

Points to note

The example below shows how to set the domain name to be used by the DNS resolver, and the name server that the DNS resolver looks up. Because the DNS resolver functionality is enabled by default, it works as soon as the name server has been set.

Command examples

1. `(config)# ip domain name router.example.com`

   Sets the domain name as `router.example.com`.

2.
```
(config)# ip nameserver 192.168.0.1
```
Sets the name server as 192.168.0.1.

(2) Disabling the DNS resolver

Points to note

The example below shows how to disable the DNS resolver functionality.

Command examples

1.
```
(config)# no ip domain lookup
```
Disables the DNS resolver functionality.

Chapter

13. Device Management

This chapter describes the tasks involved in deploying and managing the Switch.

13.1 Settings related to status display and system operation

13.1.1 Lists of configuration commands and operation commands

The following tables describe the configuration commands and operation commands needed to manage the switch.

Table 13-1: List of configuration commands

Command name	Description
swrt_multicast_table	This command setting is required if both IPv4 and IPv6 multicasting and IGMP or MLD snooping are used.
swrt_table_resource	Sets a resource allocation pattern for routing tables.
system fan mode	Sets the operating mode of the fan.
system l2-table mode	Sets the search method for the Layer 2 hardware table.
system recovery	The `no system recovery` command specifies that no recovery processing is to be performed if a problem occurs, and the failed part will remain shut down.
system temperature-warning-level	Outputs a warning message when the intake temperature of the Switch reaches or exceeds the specified temperature.
switch provision#	Sets the model of a Switch.

#

See *4. Stack* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.

Table 13-2: Operation commands (software version and switch status check)

Command name	Description
show version	Shows information about the Switch software and the board installed.
show system	Shows the Switch's operating status.
clear control-counter	Resets to zero the number of the full and partial restarts due to a failure.
show environment	Shows the status of the chassis fan and power supply unit, the temperature, and the total operating hours.
reload	Restarts the switch.
show tech-support	Shows information about the status of the hardware and software required for technical support.
show tcpdump	Monitors incoming and outgoing packets.

Table 13-3: Operation commands (internal memory and memory card check)

Command name	Description
show flash	Shows internal memory usage.
show mc	Shows the memory card format and card usage.
format mc	Formats the memory card for use by the Switch.

Table 13-4: Operation commands (logging control)

Command name	Description
show logging	Shows the log entries recorded by the Switch.
clear logging	Erases the log entries recorded by the Switch.
show logging console	Shows the contents set by the `set logging console` command.
set logging console	Controls the logging of operation messages by event level.

Table 13-5: Operation commands (resource and dump information check)

Command name	Description
show cpu	Shows CPU usage.
show processes	Shows information about processes being executed by the switch.
show memory	Shows information about the amount of memory being used by the switch.
df	Shows the available disk space.
du	Shows the amount of space being used by the files in a directory.
erase dumpfile	Erases the dump file.
show dumpfile	Lists the dump files stored in the dump file storage directory.

13.1.2 Checking the software version

Using the `show version` operation command, you can view information about the software installed in the Switch. An example is shown below:

Figure 13-1: Checking the software version

```
> show version software
Date 20XX/12/25 15:11:20 UTC
S/W: OS-L3SA Ver. 11.6
>
```

13.1.3 Checking the switch status

Using the `show system` operation command, you can view the switch's activity status, installed memory, and other information. An example is shown below:

Figure 13-2: Checking the switch status

```
> show system
Date 20XX/12/10 15:26:54 UTC
System: AX3650S-20S6XW, OS-L3SA Ver. 11.5
Node : Name=System Name
    Contact=Contact Address
    Locate=Location
    Elapsed time : 04:32:13
    LED Brightness mode : normal
    Machine ID : 0012.e222.1dd3
    Power redundancy-mode : check is not executed
    Power slot 1 : active PS-M(AC)
        Fan  : active No = Fan1(1) Speed = normal
        PS   : active
        Lamp : Power LED=green , ALM1 LED=light off , ALM2 LED=light off
    Power slot 2 : active PS-M(AC)
        Fan  : active No = Fan2(1) Speed = normal
        PS   : active
        Lamp : Power LED=green , ALM1 LED=light off , ALM2 LED=light off
    Fan slot : active FAN-M
        Fan  : active No = Fan3(1) , Fan3(2) , Fan3(3) , Fan3(4) Speed = normal
        Lamp : ALM LED=light off
    Main board : active
        Boot : 20XX/12/10 10:54:49 , operation reboot
        Fatal restart : CPU 0 times ,  SW 0 times
        Lamp : Power LED=green , Status LED1=green
        Board : CPU=PowerPC 800MHz , Memory=1,048,576kB(1024MB)
        Temperature : normal(28degree)
        Flash :
                  user area   config area     dump area    area total
            used  114,175kB          74kB       3,306kB     117,555kB
            free   91,381kB     120,597kB      62,084kB     274,062kB
            total 205,556kB     120,671kB      65,390kB     391,617kB
        MC   : notconnect
    Device resources
        Current selected swrt_table_resource: l3switch-2
        Current selected swrt_multicast_table: On
        Current selected unicast multipath number: 8
        IP routing entry :
            Unicast : current number=6 , max number=8192
            Multicast : current number=0 , max number=1024
            ARP : current number=1 , max number=2048
        IPv6 routing entry :
            Unicast : current number=1 , max number=4096
            Multicast : current number=0 , max number=256
            NDP : current number=0 , max number=2048
        MAC-Address table entry : current number=7 , max number=32768
        System Layer2 Table Mode : auto (mode=1)
        Flow detection mode : layer3-1
          Used resources for filter inbound(Used/Max)
                                     MAC     IPv4     IPv6
            Port 0/ 1-24       :   0/512   30/512      n/a
            Port 0/25-48       :   0/512   24/512      n/a
            Port 0/49-52       :   0/512   24/512      n/a
            VLAN               :   0/512    2/512      n/a
          Used resources for QoS inbound(Used/Max)
                                     MAC     IPv4     IPv6
            Port 0/ 1-52       :   0/256   26/256      n/a
            VLAN               :   0/256    2/256      n/a
          Used resources for UPC inbound(Used/Max)
                                     MAC     IPv4     IPv6
            Port 0/ 1-52       :   0/256   26/256      n/a
            VLAN               :   0/256    2/256      n/a
          Used resources for TCP/UDP port detection pattern
            Resources(Used/Max):  3/32
        Flow detection out mode : layer3-3-out
          Used resources for filter outbound(Used/Max)
                                     MAC     IPv4     IPv6
            Port 0/ 1-52       :     n/a      n/a      n/a
            VLAN               : 256/256  256/256  256/256
>
```

You can check the status of the fan and power supply unit, the temperature, and the total operating hours using the `show environment` operation command. The operation mode of the fan can be set using the `system fan mode` configuration command. An example is shown below:

Figure 13-3: Checking the switch environment

```
> show environment
Date 20XX/12/10 10:00:00 UTC
Power slot 1 : PS-M(AC)
Power slot 2 : PS-M(AC)
Fan slot     : FAN-M

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

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

Temperature environment
    Main  :  30 degrees C
    Warning level : normal

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

The `temperature-logging` parameter of the `show environment` command allows you to check the temperature log. An example is shown below:

Figure 13-4: Checking temperature log data

```
> show environment temperature-logging
Date 20XX/12/10 20:00:00 UTC
Date         0:00  6:00 12:00 18:00
20XX/12/10      -     -  26.0  24.0
20XX/12/09   22.2  24.9  26.0  24.0
20XX/12/08   24.0  23.5  26.0  24.0
20XX/12/07   21.0     -  26.0  24.0
20XX/12/06   25.6     -  26.0  24.0
20XX/12/05   21.8  25.1  26.0  24.0
20XX/12/04   24.3  24.2  26.0
>
```

13.1.4 Checking the switch's internal memory

Using the `show flash` operation command, you can check file system usage in the switch's internal memory. If more than 95% of internal memory is in use, see the *Troubleshooting Guide* and take appropriate action. An example is shown below:

Figure 13-5: Checking flash memory capacity

```
> show flash
Date 20XX/06/21 17:53:11 UTC
Flash :
          user area   config area     dump area    area total
    used  114,175kB          74kB       3,306kB     117,555kB
    free   91,381kB     120,597kB      62,084kB     274,062kB
    total 205,556kB     120,671kB      65,390kB     391,617kB
>
```

13.1.5 Viewing and controlling operation message output

When its status changes, the Switch displays an operation message containing operating data or fault data on the console or remote operation terminal. For example, a message might report that a line error has been restored, or that a line has failed and operation has stopped. For details about operation messages, see *2. Routing Event Information* in the manual *Message and Log Reference*

For Version 11.10.

Using the `set logging console` operation command, you can set an event level to limit the types of operation messages displayed. You can view the set event level by executing the `show logging console` operation command. The following setting example prevents operation messages up to event level E5 from being logged to the terminal.

Figure 13-6: Example of controlling operation message output

```
> set logging console disable E5
> show logging console
  System message mode : E5
>
```

Notes

When a large number of operation messages are generated in succession, only a portion of them will be shown on the console or remote operation terminal. To view all messages, use the `show logging` operation command.

13.1.6 Viewing logged data

Operation messages are also stored internally as operation log data. You can use this information to manage the operating status of switches and failures.

An operation log records information about events that occur during switch operation in chronological order. This information is the same as the operation messages. The following information is saved as an operation log:

- Operations performed by an operator and the response messages
- Operation message

In a reference log, log information about the failures and warnings occurring on a switch is grouped by message ID. In addition, the reference log also contains information such as the date and time the event occurred the first time, the date and time the event last occurred, and the cumulative number of times that the event occurred.

This data is logged in text format inside the switch. To view the entries, use the `show logging` operation command. By specifying a pattern string using the `grep` command, you can view a particular type of log data. For example, if you execute `show logging | grep EVT` or `show logging | grep ERR`, the entire set of error-related log entries will be displayed. An example is shown below.

Figure 13-7: Display of error-related log entries

```
> show logging | grep EVT
:
(data omitted)
:
EVT 08/10 20:39:38 01S E3 SOFTWARE 00005002 1001:000000000000 Login operator
from LOGHOST1 (ttyp1).
EVT 08/10 20:41:43 01S E3 SOFTWARE 00005003 1001:000000000000 Logout operator
from LOGHOST1 (ttyp1).
:
(data omitted)
:
>
```

13.1.7 Setting a resource allocation pattern for routing tables

You can change the resource allocation pattern for routing tables according to the Switch environment. Specify the allocation pattern in the `l3switch-1`, `l3switch-2`, or `l3switch-3` parameter of the `swrt_table_resource` configuration command.

The following table describes the number of table entries for each allocation pattern:

Table 13-6: Number of table entries for each allocation pattern **[AX3800S]**

Item		Number of table entries for each allocation pattern		
		l3switch-1	l3switch-2	l3switch-3
IPv4	Unicast route	13312	8192	1024
	Multicast route	1024	256	16
	ARP	8190#	5120	128
IPv6	Unicast route	--	2048	7560
	Multicast route	--	128	16
	NDP	--	1024	1024

Legend: --: Not applicable

#

When ARP and multicast routing are used together, the maximum number of total entries is 8190.

Table 13-7: Number of table entries for each allocation pattern **[AX3650S]**

Item		Number of table entries for each allocation pattern		
		l3switch-1	l3switch-2	l3switch-3
IPv4	Unicast route	16384	8192	1024
	Multicast route	1024	1024	16
	ARP	11264#	2048	128
IPv6	Unicast route	--	4096	7680
	Multicast route	--	256	768
	NDP	--	2048	2048

Legend: --: Not applicable

#

When ARP and multicast routing are used together, the maximum number of total entries is 11264.

The default pattern is `l3switch-1`, which allocates resources to IPv4 routing. Change this setting if you are also using IPv6 routing.

You can check information about the resource allocation pattern and number of table entries by using the `show system` operation command.

Points to note

Because you must restart the Switch for any changes to take effect, we recommend that you perform this setting at initial deployment.

Command examples

1. `(config)# swrt_table_resource l3switch-2`

   In configuration mode, sets `l3switch-2` as the table entries allocation pattern.

2. `(config)# save`

   `(config)# exit`

   Saves the settings and switches from configuration mode to administrator mode.

3. `# reload`

   Restarts the Switch.

13.1.8 Enabling both IPv4 or IPv6 multicasting and IGMP or MLD snooping

Setting the `swrt_multicast_table` configuration command allows you to use both IPv4 and IPv6 multicasting and IGMP or MLD snooping with the Switch.

You can check whether `swrt_multicast_table` is set by using the `show system` operation command.

Points to note

By default, `swrt_multicast_table` is not set. After you set it, you must restart the Switch to apply the setting. For this reason, we recommend that you perform the setting at initial deployment.

Command examples

1. `(config)# swrt_multicast_table`

   In configuration mode, sets `swrt_multicast_table`.

2. `(config)# save`

   `(config)# exit`

   Saves the settings and switches from configuration mode to administrator mode.

3. `# reload`

   Restarts the Switch.

13.1.9 Configuration that corresponds to each model

The Switch provides the `switch provision` configuration command to set a switch model.

The model of the local switch is automatically set. The model cannot be changed or deleted.

For operation in stack mode, you must set a model for member switches other than the local switch before configuring stack.

You can use the `show running-config` operation command to check the `switch provision` settings.

Figure 13-8: Checking the switch provision settings

```
# show running-config
#default configuration file for AX3650S-24T6XW
!
switch 1 provision 3650-24t6xw
!
  :
  :
#
```

13.2 Backing up and restoring operating information

This section describes how to restore operating information after a failure or module replacement.

Carry out the tasks described in *13.2.2 Backup and restore command procedures*. You can also restore the information manually, but we do not recommend this because the switch handles a wide variety of operating information which is complicated to manage and cannot be fully restored.

13.2.1 List of operation commands

The following table describes the operation commands used for backing up and restoring information.

Table 13-8: List of operation commands

Command name	Description
backup	Saves switch information and information about active applications to a memory card or remote FTP server.
restore	Restores the switch information saved to a memory card or remote FTP server to the Switch.

13.2.2 Backup and restore command procedures

(1) Backing up information

Create a backup by using the `backup` command at a time when the switch is running normally. The `backup` command places the information below, which is required for switch operation, in one file, and then saves the file to a memory card or external FTP server.

If you make any subsequent changes to the information, we recommend that you back it up again using the `backup` command.

- Files for updating software to the version in current use
- Software upgrades
- startup-config
- Power mode
- User accounts and passwords
- Optional licenses
- Web authentication database
- Registered HTML files for Web authentication pages
- MAC-based authentication database
- IPv6 DHCP server DUID files
- Stack information file

Note that the `backup` command does not save the following information:

- Operation log entries and other log entries displayed by the `show logging` command
- Dump files and other error information saved internally
- Files created or saved by a user in a home directory set for that user account

(2) Restoring information

To restore information from a backup file created by the `backup` command, use the `restore` command.

When you execute the `restore` command, the switch software is updated automatically from the software update files stored in the backup file. At completion, the Switch restarts automatically, and the restoration is continued.

Note the following points when you execute the `restore` command:

- Restore the information from a backup file created on a switch that has the same model name as the Switch you are restoring the information to.

  Check the `Model` name given in the result displayed by the `show version` command.
- Make sure that the software version of the switch on which you take the backup is supported by the switch to which you are restoring the information.
- Make sure that the user account set for the switch is the same as that included in the backup file (the user name and also the order of the user addition/deletion are the same). If the user accounts differ from each other, you will be unable to perform file operations after restoration.

13.3 Failure recovery

Recovery processing is performed automatically when a problem occurs during Switch operation. The processing is localized according to where the problem occurred, minimizing its impact and allowing unaffected sections to continue operating.

13.3.1 Error locations and recovery processing

Recovery processing differs according to the nature of the problem. The following table describes error locations and the recovery processing.

Table 13-9: Error locations and recovery processing

Error location	Switch response	Recovery processing	Scope of effect
Error detected at a port	Makes an unlimited number of auto-recovery attempts.	Re-initializes the affected port.	Communication via the affected port is suspended.
Main board (CPU) failure	Makes auto-recovery attempts up to six times. If a failure occurs at the sixth auto-recovery attempt, the switch stops. The number of auto-recovery attempts are reset after one hour of post recovery operation.	Re-initializes the main board.	Communication via all ports on the switch is suspended.
Main board (SW) failure	Makes six auto-recovery attempts in one hour. If a failure occurs at the sixth auto-recovery attempt, the switch stops.# The number of auto-recovery attempts are reset after one hour of operation since the first failure.	Re-initializes the switching processor.	Communication via all ports on the switch is suspended.
Power supply (PS) failure	Stops when the power required to run the switch ceases to be supplied. Keeps running if power redundancy has been configured.	Stops the switch. Keeps running if power redundancy has been configured.	Communication via all ports on the switch is suspended. If the redundant power supply unit is used, communication is not suspended.
Fan failure	Increases the speed of the other fan.	There is no means of auto-recovery. Replace the power supply unit or failed fan unit.	The other fan runs faster, but this does not affect communications.

#: Auto-recovery will not be performed if you have disabled recovery processing by using the `no system recovery` configuration command.

Chapter

14. Power Saving Functionality

This chapter describes the power saving functionality of the Switch.

14.1 Description of the power saving functionality

14.1.1 Overview of the power saving functionality

In cases where bandwidth is increased by having a greater number of ports to handle an expected increase in traffic on the network, the switch will consume proportionally more power. In the Switch, unnecessary power consumption is reduced by the switch's power saving functionality.

(1) Supported functionality

The Switch supports the power saving functionality below. You can use the functionality at all times, or you can limit their use to a scheduled time range.

- Sleep functionality
- Port power OFF
- Power saving for ports in the link-down status
- LED brightness control functionality

14.1.2 Power saving functionality

(1) Sleep functionality

This functionality puts the Switch into sleep mode during a scheduled time period and cancels the sleep mode and starts the Switch when a normal time range begins. The Switch can be scheduled to be in operation or in sleep mode (for example, on Sundays, Saturdays, long weekends, national holidays, or nights). The PWR LED blinks green in long intervals during sleep mode. The Switch stops all functionality including switching (frame forwarding) and remote access. To forcibly wake up the Switch from sleep mode, perform the following operations:

- Forcible cancellation of sleep mode

  Press and hold down the RESET button on the front panel of the Switch when the Switch is in sleep mode until the PWR LED on the front panel lights up green (at least five seconds). Release the RESET button as soon as the PWR LED lights up green. The sleep mode will be canceled. The Switch then starts up in schedule-disabled mode. If this operation is performed at the beginning of the normal time period, the Switch runs in normal mode without going into schedule-disabled mode.

(2) Port power OFF

By turning off the power supplied to unused ports, you can reduce power consumption. To turn off the power supply to unused ports:

- Use a configuration command to place the port in the shutdown status
- Use an operation command to place the port in the inactive status

(3) Power saving for ports in the link-down status

This functionality limits the power supplied to ports until an electrical signal is detected, allowing you to reduce power consumed by ports in link-down status due to LAN cable disconnection or remote devices being powered off. Although use of this functionality reduces power consumed by ports in link-down status, more time is required to place these ports in link-up status.

To use this functionality, execute configuration commands to enable the power saving setting for link-down ports. This setting is applied globally to the entire Switch and cannot be set to individual ports. Also, note that the link-down port power saving functionality can only be used for 10BASE-T/100BASE-TX/1000BASE-T ports. Using this functionality for optical signal ports will not change power consumption of the port during link-down status.

(4) LED brightness control functionality

You can control the brightness of the LEDs on the Switch to reduce power consumption.

The Switch allows you to permanently set the LED brightness to power saving mode or turn off the LEDs. The Switch also has a functionality to automatically adjust the brightness of the LEDs on the Switch. This function is called the automatic brightness control functionality.

Once the LED automatic brightness control functionality is enabled, it turns down the brightness of the LED on the Switch after a certain period of time has elapsed without the following events occurring, and then the LEDs are turned off when a certain period of time elapses again without any of the following events occurring:

- Login from the console
- Inserting or removing a memory card
- Ethernet interface link-up or link-down

Note that this functionality does not change the LEDs' brightness while a user is logged in from the console, and the LEDs remain at normal brightness until the user logs out.

The following table describes the LED brightness settings used when the LED brightness control is enabled.

Table 14-1: LED brightness in the LED brightness control settings

LED	LED brightness control setting		
	Normal brightness	Power saving brightness	Off
PWR LED	Normal brightness	Normal brightness	Normal brightness
Port LED (ON)	Normal brightness	Power saving brightness	Off
STATUS1 (ON)	Normal brightness	Power saving brightness	Flashing
Access LED (ON)	Normal brightness	Power saving brightness	Power saving brightness

Note that, in some circumstances, Port LED, STATUS1, and Access LEDs are off regardless of the LED brightness settings.

14.1.3 Scheduling power saving functionality

You can schedule the power saving functionality to run for a specific period of time. To set power control, specify a power saving function and the period of time when the function is enabled. When the specified start time arrives, the power saving functionality is initiated automatically. Once you have scheduled the power saving functionality, you can also disable it for a particular period. A set time when power control is enabled is referred to as a scheduled time range and a time when power control is not enabled is referred to as a normal time range.

(1) Specifiable power saving functionality

You can set a schedule for the following power saving functionality: sleep, port power off, link-down port power saving, and LED brightness control. Power saving functionality other than the sleep functionality can be used in combination. However, the sleep functionality takes priority.

(2) Scheduling power control

Set the time range when the switch is to operate in power control mode. Specify the start time and end time in any of the following ways:

- Enabling power control by date and time
- Enabling power control by day of the week and time
- Enabling power control by daily time range
- Disabling power control by time range

You can use these methods in combination to enable or disable power control at various times.

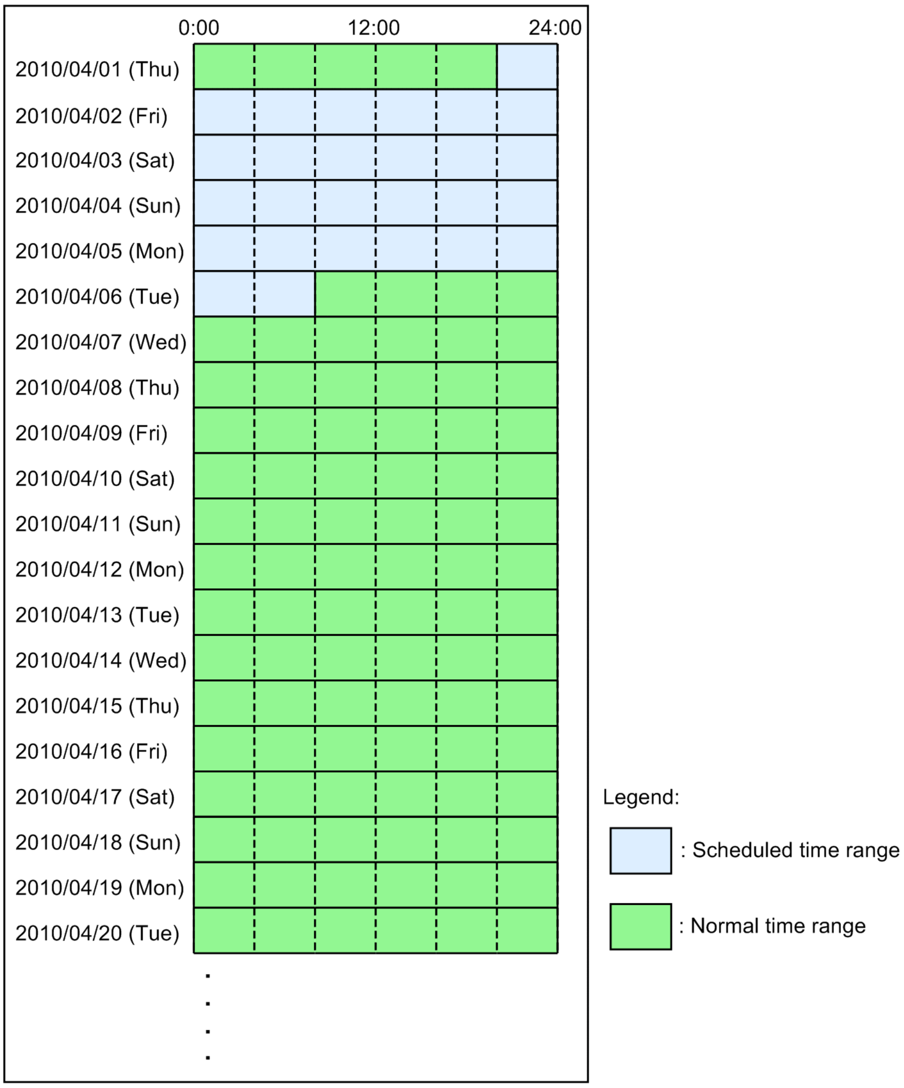
(a) Enabling power control by date and time

Specify the start and end dates and times for implementing power control.

Example:

From April 2 to April 5, 2010, the business system will have a reduced workload. In line with this expectation, schedule power control from 20:00 on April 1 to 8:00 on April 6, 2010. The following figure shows the operation schedule.

Figure 14-1: Power control schedule (by date)

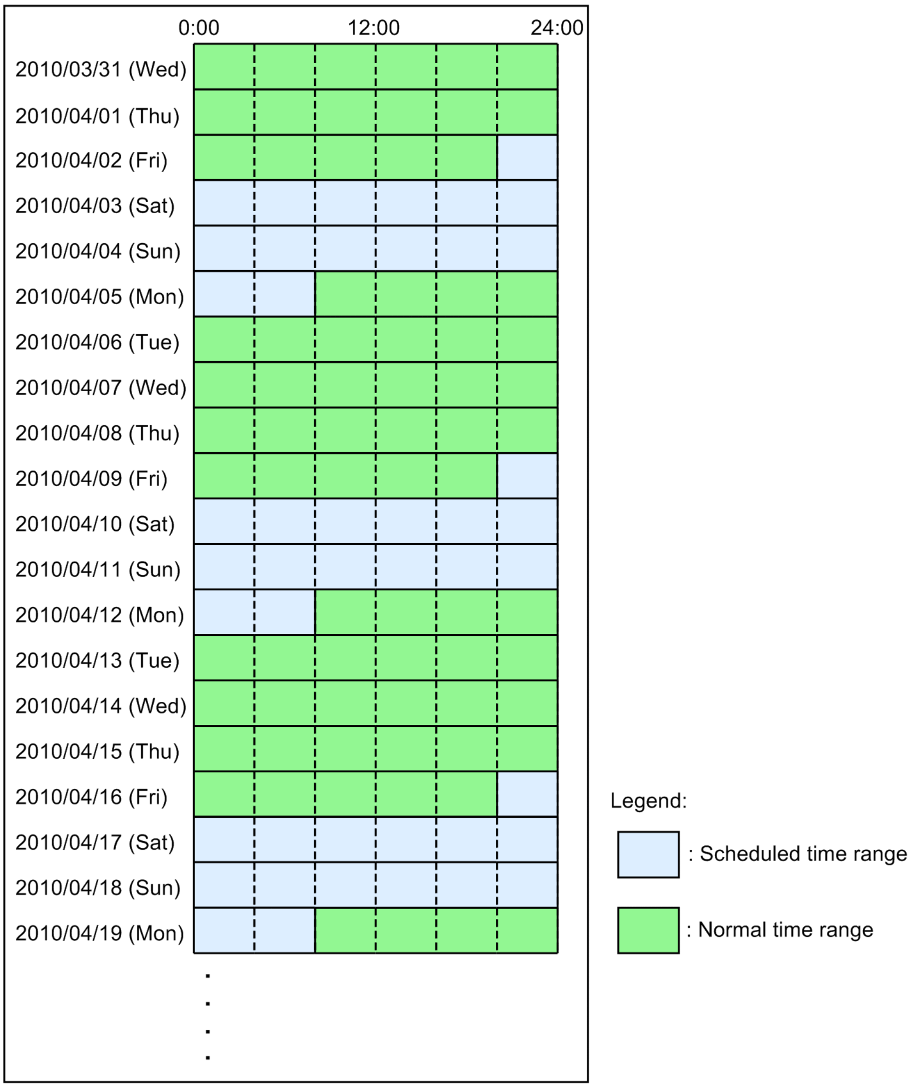


(b) Enabling power control by day of the week and time

Specify the start and end days of the week and times for implementing power control.

Example:

> The office is closed every Saturday and Sunday, and the business system has a reduced workload on these two days. Therefore, schedule power control from 20:00 every Friday to 8:00 every Monday. The following figure shows the operation schedule.
>
> *Figure 14-2:* Power control schedule (by day of the week)



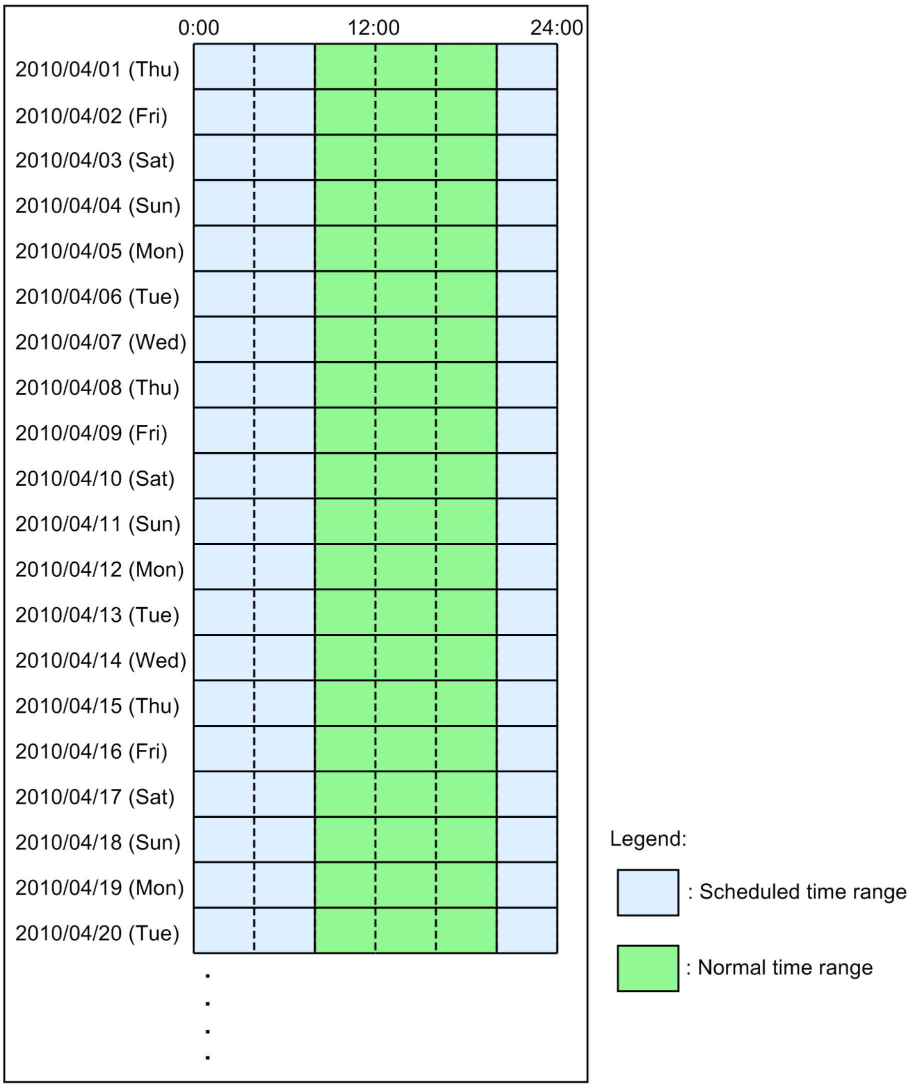
(c) Enabling power control by daily time range

Specify the start time and end time for implementing power control.

Example:

Normal office hours are from 8:30 to 17:00 every day, so the business system needs to operate at normal power from 8:00 to 20:00. Schedule power control from 20:00 every day to 8:00 the following day. The following figure shows the operation schedule.

Figure 14-3: Power control schedule (daily)



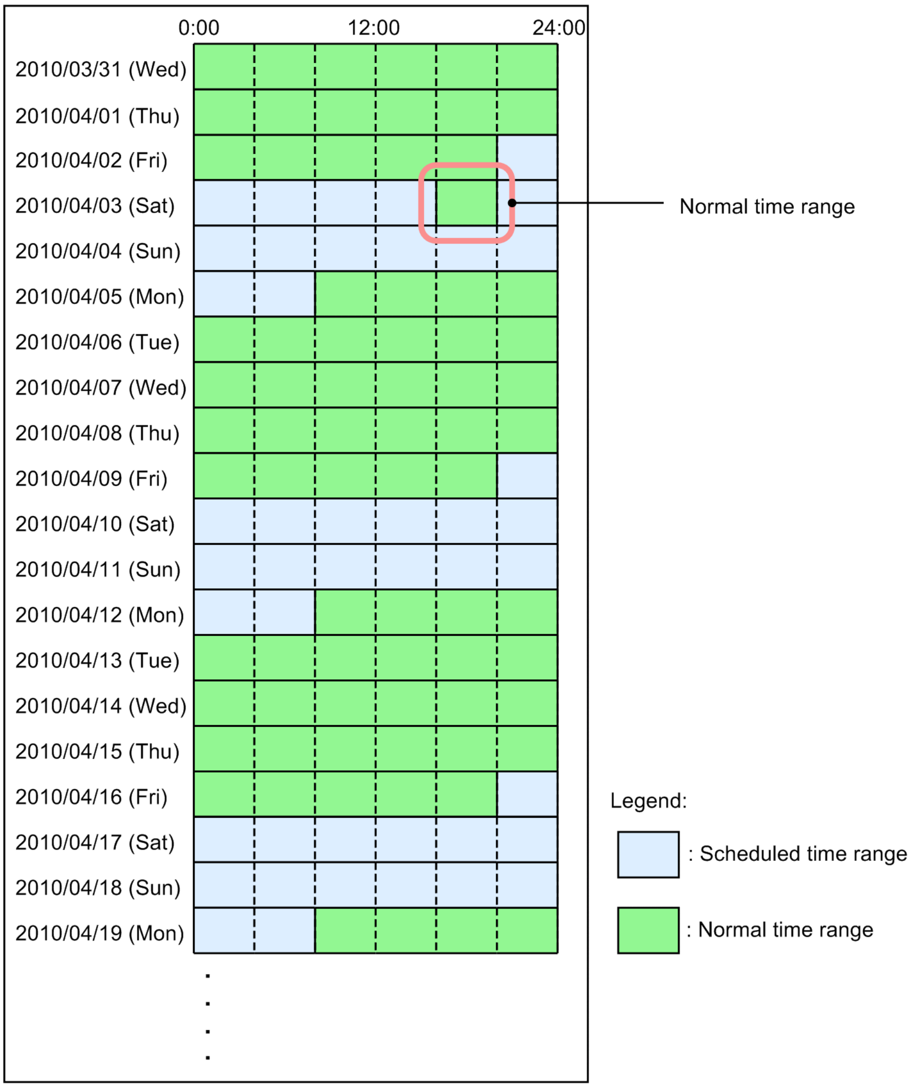
(d) Disabling power control by time range

You can disable power control for a specified time during a scheduled time range. Specify the start and end times for disabling the functionality. You can specify particular dates or days of the week, or certain times every day.

Example:

The office is closed every Saturday and Sunday, and power control is scheduled from 20:00 every Friday to 8:00 every Monday. However, the business system needs to run at normal power to perform batch processing from 16:00 to 20:00 on April 3, 2010. The following figure shows the operation schedule.

Figure 14-4: Power control schedule (disable)



14.1.4 Notes on the power saving functionality

(1) Scheduling power control

- To use the same power saving functionality during a normal time range and a scheduled time range, perform the setting for both time ranges.

  Example

  Suppose you use the `shutdown` configuration command to turn off a particular port during a normal time range. If you want to turn off that port during a scheduled time range, you must include it in the parameter of the `schedule-power-control shutdown` configuration command.

(2) Time lag in starting and ending power control

Because scheduling uses a software timer, a situation such as a high CPU load might cause a time lag before the set start or end of a scheduled time range takes effect. The delay should be less than one minute. Also, depending on the network configuration, there could be a time lag before communication with the port resumes at the end of a scheduled time range in which the port's power supply has been turned off. Allow a certain margin when you schedule power control.

(3) Notes on the sleep functionality

Note the following points if you schedule the sleep functionality:

- If entering the scheduled time period in configuration command mode, the Switch does not go into sleep mode. The Switch goes into sleep mode after exiting configuration command mode (after moving to administrator mode).
- If entering the scheduled time period while the software is being updated or restored, the Switch does not go into sleep mode. The Switch enters the sleep mode after the software is updated or restoration is completed.
- An unsaved configuration will be discarded when going into sleep mode. The following confirmation message appears when exiting configuration command mode.

  ```
  Unsaved changes found! Do you exit "configure" without save ? (y/n):
  ```

  Press `n` to execute the `save` command.
- If there is no key input for a set duration (30 minutes by default), you are automatically logged out. If automatic logout occurs while editing a configuration, an unsaved configuration is discarded.
- The Switch automatically wakes up from sleep mode and restarts once in 20 days. Then, it goes into sleep mode again after startup.
- Because the normal startup process is performed after waking from sleep mode, communication will not be available immediately. Make sure to take the startup time into account when scheduling normal and sleep time periods.
- If the switch is started via MC, do not set the `schedule-power-control system-sleep` configuration command used to make the switch enter the sleep state in the scheduled time range.
- Operations executed immediately before or after the following log message indicating the start of switch sleep (hereinafter called sleep notification) may be interrupted: `E3 SOFTWARE 01910405 1001:000000000000 System is going to sleep soon..`
- Even if the `disable` parameter of the `set power-control schedule` operation command is executed after sleep notification is output, the switch enters the sleep state without the schedule being disabled.
- Even if the `set clock` operation command is executed or the time zone is changed by the `clock timezone` configuration command between one minute before sleep notification is output and when it is actually output, the sleep mode functionality may be executed according to the schedule before the change.
- When the Switch uses the sleep mode functionality, if you perform either of the following operations immediately before or after sleep notification, the history functionality may not operate correctly (a command entered in the past cannot be called, or the character string of a called command is wrongly displayed). In this case, the details of the command entered in the past cannot be restored.
  - logout

- Move from configuration command mode to administrator mode

To restore the details, perform the following operation for each of the command input modes.

User mode or administrator mode

After changing the mode to the configuration command mode, execute `"$rm .clihistory"` and then delete the file.

Configuration command mode

After changing the mode to the administrator mode, execute `"rm .clihihistory"` and then delete the file.

Note that if `.clihistory` or `.clihihistory` does not exist under the home directory of the user, no operations are required to be performed.

- When the Switch uses the sleep mode functionality, if you execute a command that configures the CLI environment information (`set exec-timeout`, `set terminal help`, `set terminal pager`) immediately before or after sleep notification, the already set CLI environment information (any or all of Auto-logout, Paging, and Help functionality) may return to the default settings.

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

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

(4) Combined use of sleep mode functionality and DHCP snooping

For combined use of the sleep mode functionality and DHCP snooping, configure the settings so that the time period of the sleep status is longer than the lease time of an IP address distributed by the DHCP server. If the time period of the sleep status is shorter than the lease time, the binding database cannot be restored when the sleep mode is cancelled, possibly disconnecting communication from DHCP clients.

If this occurs, release and update the IP addresses on the DHCP clients. In Windows, for example, in the command prompt, execute `ipconfig /release` and then execute `ipconfig /renew`. This re-registers terminal information in the binding database and enables communication by DHCP clients.

14.2 Configuration of the power saving functionality

14.2.1 List of configuration commands

The following table describes the configuration commands for the power saving functionality.

Table 14-2: List of configuration commands

Command name		Description
For setting a normal time range	For setting a scheduled time range	
--	schedule-power-control system-sleep	Sets sleep mode.
shutdown#	schedule-power-control shutdown	Turns off the power supplied to a port.
power-control port cool-standby	schedule-power-control port cool-standby	Reduces power consumed by link-down ports.
system port-led	schedule-power-control port-led	Controls the brightness of the LEDs.
system port-led trigger console		Configures the setting for logging in from the console when automatic brightness adjustment takes place.
system port-led trigger interface		Configures the port link-up and down settings used when the automatic brightness adjustment takes place.
system port-led trigger mc		Configures the memory card insertion and removal settings used when the automatic brightness adjustment takes place.
--	schedule-power-control time-range	Specifies the time range of the power control schedule.

Legend: --: Not applicable

#

See *10. Ethernet* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.

14.2.2 Configuration command setting example

(1) Sleep functionality

The configuration commands below are an example of how to put the Switch into sleep mode in the scheduled time period.

Points to note

Put the Switch into sleep mode during the scheduled time period to reduce power consumption.

Command examples

1. `(config)# schedule-power-control system-sleep`

   Sets the Switch to go into sleep mode in the scheduled time period.

2.
```
(config)# schedule-power-control time-range 1 weekly
start-time fri 2000 end-time mon 0800 action enable
```

Specifies a power control schedule that runs from 20:00 every Friday to 8:00 every Monday.

(2) Scheduled power-off of unused ports

The example below shows how to use configuration commands to schedule the powering off of unused ports.

Points to note

Reduce power consumption by turning off the power supplied to unused ports.

Command examples

1.
```
(config)# schedule-power-control shutdown interface
gigabitethernet 1/0/1-10
```

Specifies the ports to turn off during the scheduled time range.

2.
```
(config)# schedule-power-control time-range 1 weekly
start-time fri 2000 end-time mon 0800 action enable
```

Specifies a power control schedule that runs from 20:00 every Friday to 8:00 every Monday.

3.
```
(config)# schedule-power-control time-range 2 date start-time
100403 1600 end-time 100403 2000 action disable
```

Disables the power control schedule for the time range from 16:00 to 20:00 on April 3, 2010.

(3) Scheduled power reduction of link-down ports

The configuration command below is an example of how to reduce power consumed by link-down ports during the scheduled time period.

Points to note

Reduces power consumed by link-down ports during the scheduled time period.

Command examples

1.
```
(config)# schedule-power-control port cool-standby
```

Reduces power consumed by link-down ports during the scheduled time period.

(4) LED brightness control functionality

The configuration commands below are an example of how to automatically control the brightness of LEDs during both scheduled and normal time periods.

Points to note

If scheduling settings are configured, set the LED brightness control functionality for both normal and scheduled time periods. Set login from ports 1/0/1-10 and the console as events that trigger automatic brightness adjustment.

Command examples

1.
```
(config)# system port-led enable
```

Sets LED automatic brightness adjustment for the normal time period.

2. `(config)# schedule-power-control port-led enable`

   Sets LED automatic brightness adjustment for the scheduled time period.

3. `(config)# system port-led trigger interface gigabitethernet 1/0/1-10`

   Sets ports 1/0/1-10 as events that trigger LED automatic brightness adjustment.

4. `(config)# system port-led trigger console`

   Sets logging in from the console as an event that triggers LED automatic brightness adjustment.

14.3 Operation of the power saving functionality

14.3.1 List of operation commands

The following table describes the operation commands for the power saving functionality.

Table 14-3: List of operation commands

Command name	Description
show power-control schedule	Lists power control schedules.
show power	Shows information about power consumption and the total amount of power consumed by the Switch.
clear power	Clears the information about the power consumption of the Switch.
set power-control schedule	Sets whether to apply a power control schedule.
show power-control port	Shows the power saving status of the ports.
inactivate#	Turns off the power to a port.

#

See *16. Ethernet* in the manual *Operation Command Reference Vol.1 For Version 11.10*.

14.3.2 Displaying the LED behavior

You can check the LED behavior settings by using the `show system` operation command and viewing `LED Brightness mode`. For details, see *13.1.3 Checking the switch status*.

Figure 14-5: Checking the LED behavior

```
> show system
Date 20XX/09/06 15:26:54 UTC
System: AX3650S-20S6XW, OS-L3SA Ver. 11.5
Node : Name=System Name
    Contact=Contact Address
    Locate=Location
    Elapsed time : 04:32:13
    LED Brightness mode : normal
                :
                :
>
```

14.3.3 Checking the power control status

(1) Checking power control schedules

Using the `show power-control schedule` operation command, you can check the current power control status and the power control schedules you have set up. The following example shows five schedules set for April 1, 20*XX* or thereafter.

Figure 14-6: Checking power control schedules

```
> show power-control schedule XX0401 count 5
Date 20XX/04/01(Thu) 18:36:57 UTC
Current Schedule Status : Disable
Schedule Power Control Date:
  20XX/04/01(Thu) 20:00 UTC  -  20XX/04/02(Fri) 06:00 UTC
  20XX/04/02(Fri) 20:00 UTC  -  20XX/04/05(Mon) 06:00 UTC
  20XX/04/05(Mon) 20:00 UTC  -  20XX/04/06(Tue) 06:00 UTC
  20XX/04/06(Tue) 20:00 UTC  -  20XX/04/07(Wed) 06:00 UTC
  20XX/04/07(Wed) 20:00 UTC  -  20XX/04/08(Thu) 06:00 UTC
>
```

14.3.4 Whether to apply power control schedules

You can use the `set power-control schedule` operation command to determine whether to apply power saving schedules during the scheduled time periods. If power saving schedules are disabled because the Switch was restarted in sleep mode by pressing the reset button, you can enable the schedules again using this command.

Figure 14-7: Applying power control schedules

```
> show power-control schedule XX1001 count 1
Date 20XX/10/01(Fri) 18:36:57 UTC
Current Schedule Status : Enable(force disabled)
Schedule Power Control Date:
  20XX/10/01(Fri) 18:36 UTC  -  20XX/10/02(Sat) 06:00 UTC
```

Check power control schedules. `Enable(force disabled)` indicates that the schedules are disabled.

```
> set power-control schedule enable
```

Enable the power control schedules.

```
> show power-control schedule XX1001 count 1
Date 20XX/10/01(Fri) 18:37:20 UTC
Current Schedule Status : Enable
Schedule Power Control Date:
  20XX/10/01(Fri) 18:37 UTC  -  20XX/10/02(Sat) 06:00 UTC
```

Check power control schedules. `Enable` indicates that the schedules are enabled.

14.3.5 Checking power saving status of ports

You can use the `show power-control port` operation command to check the power control status of ports. In this example, the link-down port power saving functionality is not applied to ports 0/50 and 0/51 because they use optical signals.

Figure 14-8: Checking power control status of ports

```
> show power-control port
Date 20XX/09/21 20:03:12 UTC
Port  Status  Cool-standby
0/1  up      -
0/2  down    applied
0/3  down    applied
0/4  up      -
0/5  up      -
:
:
0/48 down    applied
0/49 up      -
0/50 down    -
0/51 down    -
0/52 up      -
>
```

14.3.6 Checking power consumption information

You can periodically collect and analyze power consumption information to check the effects of the power saving functionality and to make effective power control schedules.

(1) Checking power consumption information

You can use the `show power` operation command to check the power consumption and the total power consumption amount of the Switch. An example is shown below:

Figure 14-9: Checking power consumption information

```
>show power
Date 20XX/09/21 12:00:00 UTC
```

```
Elapsed time 2Days 01:30
H/W       Wattage  Accumulated Wattage
Chassis   60.59 W             3.50 kWh
>
```

Chapter

15. Software Management

This chapter describes how to update the software. For further details, see the *Software Update Guide*.

15.1 List of operation commands

The following table describes the operation commands related to software management.

Table 15-1: List of operation commands

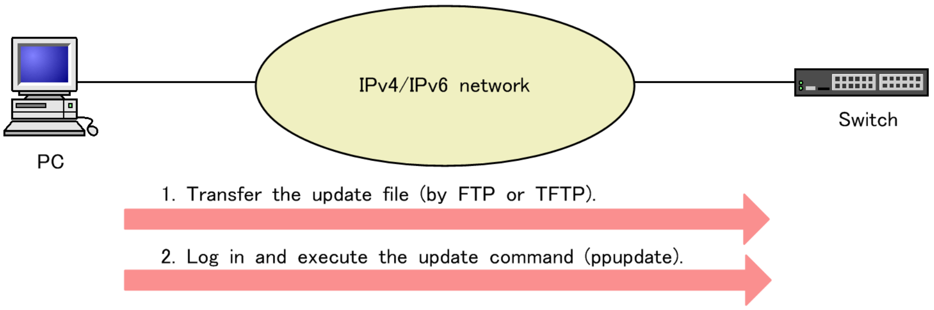
Command name	Description
ppupdate	Updates the software to a later version, which was downloaded via FTP or TFTP.
set license	Registers a purchased optional license to the switch.
show license	Shows authorized optional licenses.
erase license	Erases the specified optional license.

15.2 Software update

Software update means updating an older version of your software to a later version. To perform a software update, transfer an update file from a remote operation terminal (PC), and then execute the `ppupdate` operation command. During the update process, the switch management configuration and user information (such as login accounts and passwords) remain in effect. For details, see the *Software Update Guide*.

The following figure provides an overview of software update.

Figure 15-1: Overview of software update


IPv4/IPv6 network
PC
Switch
1. Transfer the update file (by FTP or TFTP).
2. Log in and execute the update command (ppupdate).

15.2.1 Notes on updating software

To update software when the Switch is in the sleep state, cancel the forced sleep and start the Switch, and then update the software.

15.3 Registering an optional license

Optional licenses are required to use additional functionality incorporated in the Switches. An optional license is provided with each additional functionality. If a license is not registered, you cannot use that functionality. For details about registering and erasing licensed software, see the *Optional License Configuration Guide*.

Chapter

16. Ethernet

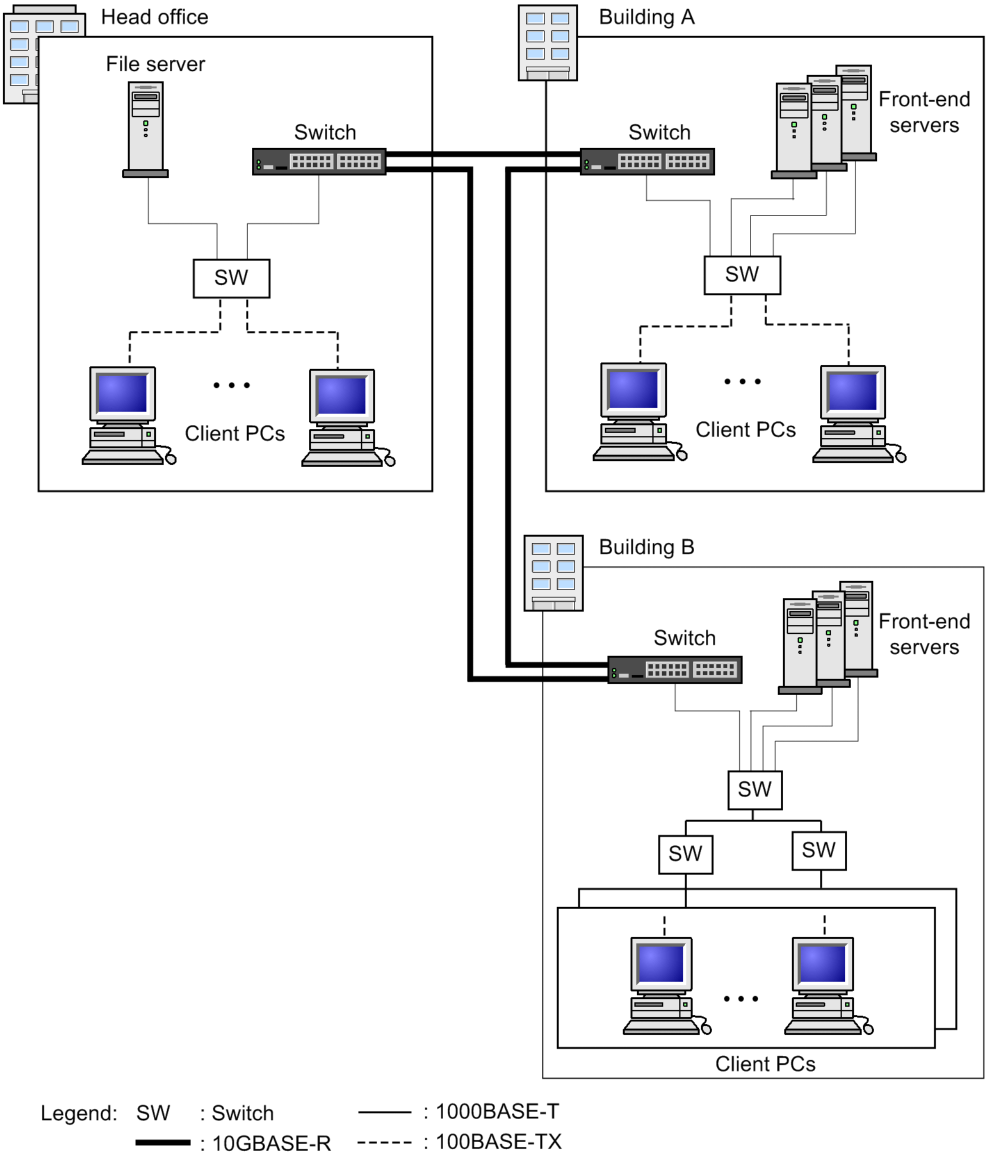
This chapter describes Ethernet as used with the Switch.

16.1 Description of information common to all Ethernet interfaces

16.1.1 Network configuration example

The figure below shows an example of a typical Ethernet configuration that uses the Switch. In this example, the use of 10GBASE-R for connections between buildings and between servers improves communication performance between servers, as compared to the use of 10BASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X.

Figure 16-1: Ethernet configuration example



16.1.2 Physical interfaces

There are four types of Ethernet interfaces:

- Interface using a 10BASE-T, 100BASE-TX, or 1000BASE-T twisted pair cable (UTP) compliant with IEEE 802.3
- Interface using a 100BASE-FX or 1000BASE-X optical fiber cable compliant with IEEE 802.3#

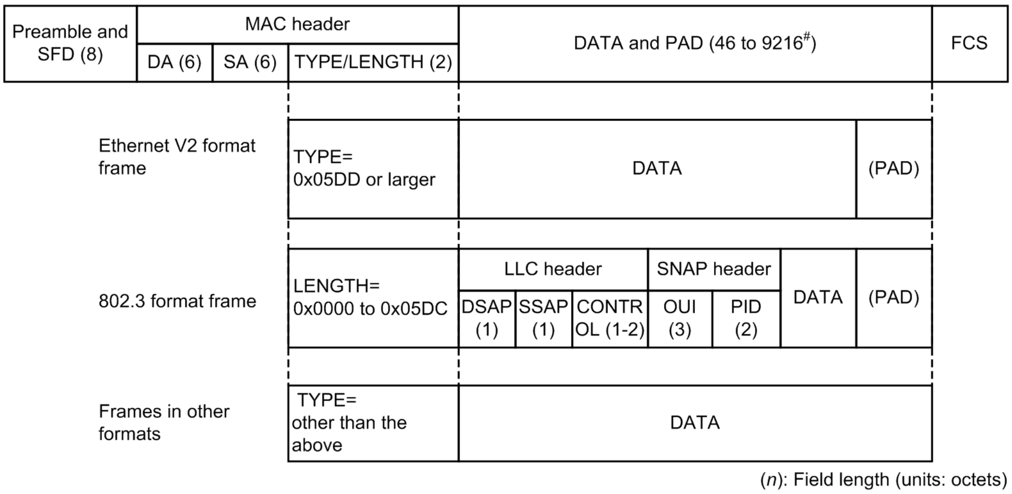
- Interface using a 10GBASE-R optical fiber cable compliant with IEEE 802.3ae
- Interface using a 40GBASE-R optical fiber cable compliant with IEEE 802.3ba **[AX3800S]**

  #: Includes IEEE 802.3ah.

16.1.3 Control on the MAC and LLC sublayers

The following figure shows frame formats.

Figure 16-2: Frame formats



#: The maximum length of the DATA and PAD field is 9216 only when the frame format is Ethernet V2. For 802.3 and other formats, the maximum length is 1500.

(1) MAC sublayer frame format

(a) Preamble and SFD field

The Preamble and SFD field contains a 64-bit binary number. The first 62 bits are repetitions of 10, and the last two bits are 11 (1010...1011). Frames without this 64-bit pattern cannot be received.

(b) DA and SA fields

The DA and SA fields support a 48-bit format. They do not support 16-bit or local address formats.

(c) TYPE/LENGTH field

The following table describes how the TYPE/LENGTH field is handled.

Table 16-1: Handling of the TYPE/LENGTH field

TYPE/LENGTH value	How the Switch handles the value
0x0000 to 0x05DC	IEEE 802.3 CSMA/CD frame length
0x05DD or larger	Ethernet V2.0 frame type

(d) FCS field

The FCS field uses a 32-bit CRC.

(2) LLC sublayer frame format

The switch supports IEEE 802.2 LLC type 1. In Ethernet V2, there is no LLC sublayer.

(a) DSAP field

The DSAP field indicates the destination service access point to which the LLC information section will be sent.

(b) SSAP field

The SSAP field indicates the source service access point from which the LLC information section was sent.

(c) CONTROL field

The CONTROL field indicates one of the following three formats: information transfer format, monitoring format, or non-numeric control format.

(d) OUI field

The OUI field indicates an organizationally unique identifier of the organization that sent the SNAP information section.

(e) PID field

The PID field indicates the Ethernet type with which the SNAP information section was sent.

(3) Handling of LLC frames

The switch supports IEEE 802.2 LLC type 1. The switch forwards only the LLC frames that satisfy the conditions described below, and discards all the other LLC frames.

(a) CONTROL field

Table 16-2: Support status for sending and receiving the value of the CONTROL field describes the support status for sending and receiving the value of the CONTROL field. For the TEST and XID frames in *Table 16-2: Support status for sending and receiving the value of the CONTROL field*, a response is made as shown in *Table 16-3: XID and TEST responses*.

Table 16-2: Support status for sending and receiving the value of the CONTROL field

Type	Code (hexadecimal)	Command	Response	Remarks
TEST	F3 or E3	Receiving is supported	Sending is supported	A TEST response is sent according to the IEEE 802.2 specifications.
XID	BF or AF	Receiving is supported	Sending is supported	An XID response is sent according to the IEEE 802.2 specifications. Note that the information section of the XID response is 129.1.0 (the value defined by IEEE 802.2 to indicate Class 1).

Table 16-3: XID and TEST responses

DA field in the MAC header	Frame type	DSAP	Response
Broadcast or multicast	XID and TEST	AA (SNAP) 42 (BPDU) 00 (null) FF (global)	Sent
		All other cases	Not sent
Individual and local address	XID and TEST	AA (SNAP) 42 (BPDU) 00 (null) FF (global)	Sent
		All other cases	Not sent
Individual and remote address	XID and TEST	All addresses	Not sent

(4) Conditions for discarding received frames

Frames satisfying any of the following conditions are discarded:

- The frame length is not a multiple of an octet.
- The length of the received frame (from DA to FCS) is either less than 64 octets or more than 1522 octets.

  If the use of jumbo frames is selected, the length of the received frame exceeds the specified size.
- An FCS error has occurred.
- A collision occurred during reception of the frame on a half-duplex connection interface.

(5) Handling of padding

If the length of a sent frame is less than 64 octets, padding is added immediately before the FCS field. The values to be padded are undefined.

16.1.4 MAC address of the Switch

(1) Device MAC addresses

The Switch has one MAC address as a device identifier. This MAC address is called the device MAC address. A device MAC address is used as a MAC address in a Layer 3 interface or as a device identifier used in a protocol such as the Spanning Tree Protocol.

(2) Functionality that uses a device MAC address

The following table describes the types of functionality that use the device MAC address.

Table 16-4: Functionality that uses a device MAC address

Functionality	Purpose
VLAN	MAC address in a Layer 3 interface
LACP for link aggregation	Device identifier
Spanning Tree Protocols	Device identifier
Ring Protocol	Device identifier
GSRP	Device identifier
IEEE 802.3ah/UDLD	Device identifier
L2 Loop Detection	Device identifier
CFM	Device identifier
LLDP	Device identifier
OADP	Device identifier

16.2 Configuration common to all Ethernet interfaces

16.2.1 List of configuration commands

The following table describes the configuration commands common to all Ethernet interfaces.

Table 16-5: List of configuration commands

Command name	Description
bandwidth	Sets the bandwidth.
description	Sets supplementary information.
duplex	Sets duplex mode.
flowcontrol	Sets flow control.
frame-error-notice	Sets the condition for sending a notification when a frame reception error or a frame sending error occurs.
interface fortygigabitethernet	Specifies an Ethernet internet configuration with a maximum line speed of 40 Gbit/s.
interface gigabitethernet	Specifies an Ethernet internet configuration with a maximum line speed of 1000 Mbit/s.
interface tengigabitethernet	Specifies an Ethernet internet configuration with a maximum line speed of 10 Gbit/s.
link debounce	Sets the time required before a link-down is detected.
link up-debounce	Sets the time required before a link-up is detected.
mdix auto	Sets the automatic MDIX functionality.
mtu	Sets the Ethernet MTU.
shutdown	Shuts down Ethernet.
speed	Sets the speed.
system flowcontrol off	Disables flow control for all ports on the switch.
system mtu	Sets a value for an Ethernet MTU device.

16.2.2 Configuring an Ethernet interface

Points to note

To configure Ethernet, specify the Switch number of the interface, the NIF number, and the port number, and then move to `config-if` mode to set up the information.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
```
Specifies that Ethernet interface 1/0/1 is to be configured.

16.2.3 Configuring multiple interfaces at one time

Points to note

When Ethernet is configured, the same information sometimes needs to be set for multiple interfaces. In such cases, the same information can be set for the interfaces at the same time by using a range specification.

Command examples

1. `(config)# interface range gigabitethernet 1/0/1-10, gigabitethernet 1/0/15-20, tengigabitethernet 1/0/25`

   Specifies Gigabit Ethernet interfaces from 1/0/1 to 1/0/10 and from 1/0/15 to 1/0/20, and 10 Gigabit Ethernet interface 1/0/25.

2. `(config-if-range)# *****`

   Performs the same configuration for all the interfaces.

16.2.4 Shutting down an Ethernet interface

Points to note

Configuring an Ethernet interface might require the execution of multiple commands. If an Ethernet interface is placed in the link-up status before all required commands are executed, communication will not be as expected. For this reason, we recommend that you first shut down the Ethernet interface, and then release the interface from the shutdown status after configuration has been completed. Always make sure that Ethernet interfaces that will not be used are shut down.

Command examples

1. `(config)# interface gigabitethernet 1/0/10`

   Specifies that Ethernet interface 1/0/10 is to be configured.

2. `(config-if)# shutdown`

   Shuts down the Ethernet interface.

3. `(config-if)# *****`

   Configures the Ethernet interfaces.

4. `(config-if)# no shutdown`

   Releases the Ethernet interface from the shutdown status.

Related information:

You can also use the `inactivate` operation command to stop the operation of an Ethernet interface. Note that if a switch is deactivated by using this command is restarted, the status of the Ethernet interface reverts to active. However, if a switch that has been shut down is restarted, its status remains disabled. To change the status from disabled to active, you must release the Ethernet interface from the shutdown status by using `no shutdown` to configure the interface.

16.2.5 Configuring jumbo frames

The maximum transmission unit (MTU) in the Ethernet interface standard is 1500 octets. On the Switch, the MTU can be extended by using jumbo frames to increase the amount of data that is transmitted at one time, which improves throughput.

For a port to send or receive jumbo frames, an MTU must be set. When an MTU is set, the Switch can send or receive frames whose maximum size is the specified MTU plus the size of one VLAN tag.

Determine the port MTU value appropriate for the network and remote device. Because two VLAN tags are sometimes added (for example, when VLAN tunneling is used), add 4 to the MTU value so that frames with two VLAN tags can be sent or received.

(1) Setting the MTU for a specific port

Points to note

The example below shows how to set 8192 octets as the MTU for port 1/0/10. This setting enables the sending and receiving of jumbo frames (8206 octets for untagged frames and 8210 octets for tagged frames).

Command examples

1.
```
(config)# interface gigabitethernet 1/0/10
(config-if)# shutdown
(config-if)# mtu 8192
```
Sets the MTU of the port to 8192 octets.

2.
```
(config-if)# no shutdown
```

Notes

- Even if the MTU for all ports is set by using a configuration command, the MTU is fixed at 1500 octets when a 10BASE-T, 100BASE-TX, or 100BASE-FX half-duplex connection is used. This note also applies when auto-negotiation results in a 10BASE-T or 100BASE-TX half-duplex connection.
- If the MTU is changed using this configuration in an AX3650S series switch, communication is temporarily disabled on the port.

(2) Setting the MTU for all ports

Points to note

The example below shows how to set 4096 octets as the MTU for the ports of all Ethernet interfaces on the Switch. This setting enables the sending and receiving of jumbo frames (4110 octets for untagged frames and 4114 octets for tagged frames).

Command examples

1.
```
(config)# system mtu 4096
```
Sets the MTU of all ports on a switch to 4096 octets.

Notes

- Even if the MTU for all ports is set by using a configuration command, the MTU is fixed at 1500 octets when a 10BASE-T, 100BASE-TX, or 100BASE-FX half-duplex connection is used. This note also applies when auto-negotiation results in a 10BASE-T or 100BASE-TX half-duplex connection.
- If the MTU is changed using this configuration in an AX3650S series switch, communication is temporarily disabled on the port.

16.2.6 Configuring the link-down detection timer

If the wait time before a link-down is detected after the detection of a link fault is too short, depending on the remote device, the link might be unstable. You can avoid this problem by setting a link-down detection timer.

Points to note

Make sure that you set as small a link-down detection timer value as possible without risking the link becoming unstable. If the link is stable even when a link-down detection timer is not set, you do not need to set one.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/10
```
   Specifies that Ethernet interface 1/0/10 is to be configured.

2.
```
(config-if)# link debounce time 5000
```
   Sets the link-down detection timer value to 5000 milliseconds.

Notes

Using a link-down detection timer can prevent a link from becoming unstable. However, if a fault occurs, the time required for the interface to settle in the link-down status is longer. If you want this time to be short, do not set a link-down detection timer.

16.2.7 Configuring the link-up detection timer

If the wait time before a link-up is detected after the detection of a link fault is short, depending on the remote device, the network might be unstable. You can avoid this problem by setting a link-up detection timer.

Points to note

Make sure that you set as small a link-up detection timer value as possible without risking the network becoming unstable. If the network is stable even when a link-up detection timer is not set, you do not need to set one.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/10
```
   Specifies that Ethernet interface 1/0/10 is to be configured.

2.
```
(config-if)# link up-debounce time 5000
```
   Sets the link-up detection timer value to 5000 milliseconds.

Notes

The larger the value you set for the link-up detection timer, the more time it takes until communication is restored after a link fault has been corrected. If you want this time to be short, do not set a link-up detection timer.

16.2.8 Configuring the notification of a frame sending or reception error

If sending or receiving frames fails because of a minor error, the Switch collects statistics about why the frames were discarded. If the number of error occurrences or the error occurrence rate over 30 seconds exceeds the threshold, the error occurrences are logged and reported by private traps.

The Switch can be configured for these thresholds and for notification. If no settings are specified, the log is displayed for only the first error when 15 errors have occurred in 30 seconds.

(1) Using the number of error frames as the threshold for notification

Points to note

To set the threshold for error occurrences (the number of error frames) as the condition for error notification on the Switch, execute the `frame-error-notice` command with `error-frames` specified.

Command examples

```
1. (config)# frame-error-notice error-frames 50
```

Sets the threshold for error occurrences (the number of error frames) to 50.

(2) Using the error occurrence rate as the threshold for notification

Points to note

To set the threshold for the error occurrence rate (the error rate) as an error notification condition on the Switch, execute the `frame-error-notice` command with `error-rate` specified.

Command examples

```
1. (config)# frame-error-notice error-rate 20
```

Sets the threshold for the error occurrence rate to 20%.

(3) Displaying the log when an error is reported

Points to note

To have the log displayed in the event of an error as the condition for error notification, execute the `frame-error-notice` command with either `onetime-display` or `everytime-display` specified. If you do not want the log to be displayed, specify `off` in the command. Settings configured by using this command do not affect private traps.

Command examples

```
1. (config)# frame-error-notice everytime-display
```

Displays the log every time an error occurs.

(4) Combining multiple conditions

Points to note

To set a combination of error notification conditions, specify the corresponding arguments in the `frame-error-notice` command. Note that executing a `frame-error-notice` command overrides the notification condition settings configured by a previous `frame-error-notice` command. If you want to use the previous settings, specify them again in the `frame-error-notice` command.

Command examples

The following shows an example of setting the threshold for the error occurrence rate in addition to setting that the log is displayed every time an error occurs.

```
1. (config)# frame-error-notice error-frames 50 everytime-display
```

Sets the threshold for error occurrences (the number of error frames) to 50, and sets the log to be displayed every time an error occurs.

Notes

If you want to use private traps, use the `snmp-server host` command to configure that a trap is sent whenever a frame reception error or a frame sending error occurs.

16.2.9 Configuring flow control [AX3650S]

To prevent the Switch from discarding received frames when the reception buffer has become full, the Switch needs to send a pause packet to the remote device to request regulated sending. The remote device must be able to receive pause packets and regulate sending in response to a received pause packet.

Whether the Switch regulates sending when it receives a pause packet from the remote device depends on the settings. During auto-negotiation, the Switch can determine whether pause packets will be passed between the Switch and the remote device.

For the Switch, you can enable flow control for a specific port, and can disable flow control for all ports on the Switch. If flow control for all ports is disabled, port-specific flow control settings remain in a configuration file, but have no effect.

(1) Specifying the flow control settings for a specific port

Points to note

Determine flow control settings that do not conflict with the settings on the remote device.

Command examples

1.
```
(config)# interface tengigabitethernet 1/0/25
(config-if)# shutdown
```
Shuts down the Ethernet interface.

2.
```
(config-if)# flowcontrol send off
(config-if)# flowcontrol receive off
```
Stops the passing of pause packets between the switch and the remote device.

3.
```
(config-if)# no shutdown
```
Releases the Ethernet interface from the shutdown status.

(2) Specifying the same flow control settings for all ports

Points to note

The example below shows how to disable flow control for all ports on the switch.

Command examples

1.
```
(config)# system flowcontrol off
```
Disables the passing of pause packets between the switch and the remote device through any port.

2.
```
(config)# save
(config)# exit
```

Saves the settings and switches from configuration mode to administrator mode.

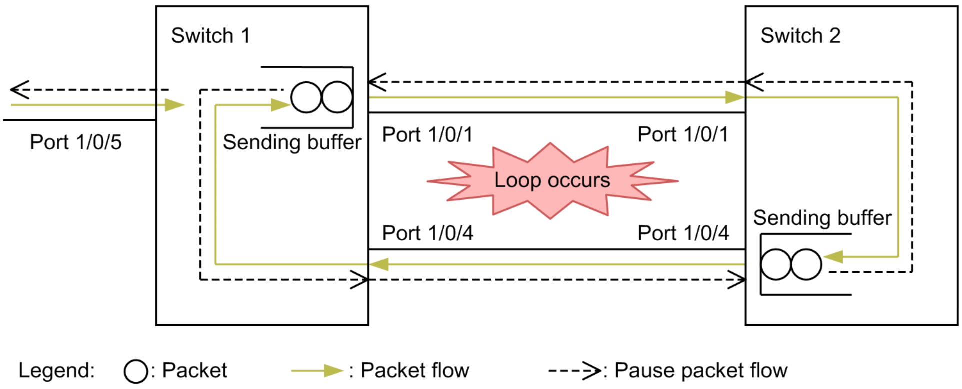
3. `# restart vlan`

Restarts the VLAN program. After the VLAN program has restarted, pause packets can neither be sent to nor received from the remote device through any port. All Ethernet interfaces are initialized again, and the ports that make up the VLAN temporarily cannot be used to send or receive data.

(3) Specifying loose flow control mode

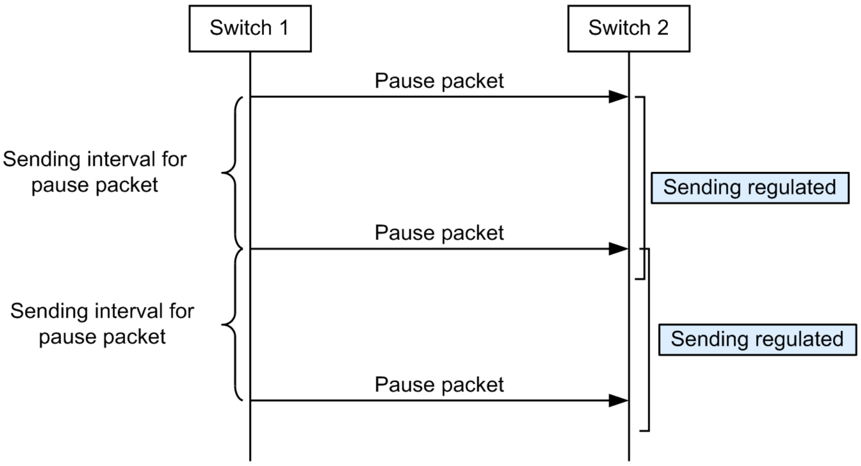
Precise flow control is necessary to minimize packet loss when connecting to the server. However, precise flow control may create a momentary loop configuration that triggers status in which both parties regulate each other (shown in the figure below). Loose flow control mode is suited for this type of network.

Figure 16-3: Example of parties regulating each other



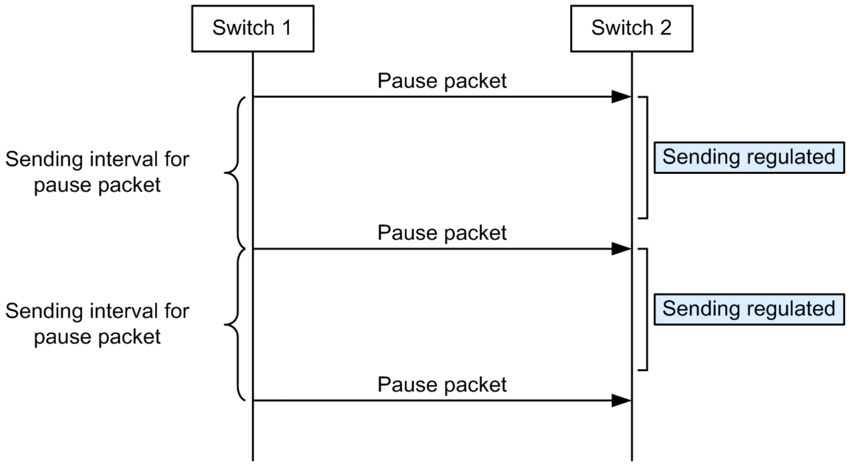
Because the pause packet sending interval is equal to or shorter than the transmission restriction time in default mode, transmission from the receiving side of pause packets will be completely stopped. The following figure describes the default behavior sequence:

Figure 16-4: Default behavior sequence



Because the pause packet sending interval is longer than the transmission restriction time in loose mode, transmission will not be completely stopped when Switches communicate with each other. The following figure describes the sequence of operations in loose mode:

Figure 16-5: Operating sequence in loose mode



Points to note

The example below shows how to set loose flow control mode.

Command examples

1. `(config)# interface tengigabitethernet 1/0/25`
   `(config-if)# shutdown`

   Shuts down the Ethernet interface.

2. `(config-if)# flowcontrol send on loose`

   Sets the mode for sending pause packets to the remote device to loose mode.

3. `(config-if)# no shutdown`

   Releases the Ethernet interface from the shutdown status.

16.3 Operations common to all Ethernet interfaces

16.3.1 List of operation commands

The following table describes the operation commands for Ethernet interfaces.

Table 16-6: List of operation commands

Command name	Description
show interfaces	Shows Ethernet information.
clear counters	Clears the Ethernet statistics counters.
show port	Shows Ethernet information in list format.
activate	Changes the status of an Ethernet port from inactive to active.
inactivate	Changes the status of an Ethernet port from active to inactive.
test interfaces	Conducts a line test.
no test interfaces	Stops a line test, and displays the test results.

16.3.2 Checking the Ethernet operating status

(1) Checking the operating status of all Ethernet ports

You can use the `show port` command to check the status of all Ethernet ports on the Switch. If you want to use an Ethernet port, confirm that `up` is displayed for `Status` of the port in the execution results.

The following figure shows an example of the results of executing the `show port` command.

Figure 16-6: Example of displaying the status of all Ethernet ports on the Switch

```
> show port
Date 20XX/11/21 15:16:19 UTC
Port Counts: 24
Port  Name            Status   Speed       Duplex     FCtl FrLen ChGr/Status
 0/ 1 geth1/0/1       up       1000BASE-SX full(auto) off   1518   -/-
 0/ 2 geth1/0/2       down     -           -          -     -      -/-
 0/ 3 geth1/0/3       up       100BASE-TX  full(auto) off   1518   -/-
 0/ 4 geth1/0/4       up       1000BASE-SX full(auto) off   1518   -/-
      :
      :
```

16.4 Description of the 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces

This section describes an Ethernet interface that uses a 10BASE-T, 100BASE-TX, or 1000BASE-T twisted pair cable (UTP).

16.4.1 Functionality

(1) Connection interface

(a) Automatic recognition (auto-negotiation) of 10BASE-T, 100BASE-TX, and 1000BASE-T

10BASE-T, 100BASE-TX, and 1000BASE-T support connection methods that use automatic recognition (auto-negotiation) and fixed settings.

- Connection by automatic recognition:10BASE-T, 100BASE-TX, and 1000BASE-T (full duplex)
- Connection using fixed settings:10BASE-T and 100BASE-TX

You can configure either of the modes shown below. Select the appropriate mode for the network to be connected. The default for the Switch is auto-negotiation mode.

- Auto-negotiation
- 100BASE-TX full duplex (fixed)
- 100BASE-TX half duplex (fixed)
- 10BASE-T full duplex (fixed)
- 10BASE-T half duplex (fixed)

(b) 10BASE-T, 100BASE-TX, and 1000BASE-T connection specifications

The following describes the connection specifications for transmission speed and duplex mode (full or half) for a connection between the Switch and a remote device.

Note that, depending on the remote device, auto-negotiation is sometimes unavailable for a 10BASE-T or 100BASE-TX connection. For this reason, if at all possible, use the fixed settings appropriate for the interface on the remote device.

Also note that a 1000BASE-T connection supports only full-duplex in auto-negotiation mode.

■ AX3830S

10BASE-T (half duplex) and 100BASE-TX (half duplex) connections are not supported.

Table 16-7: Connection specifications for transmission speed and duplex mode (full or half) **[AX3800S]**

Settings on the remote device		Settings on the Switch				
Method	**Interface**	**Fixed settings**				**Auto-negotiation**
		10BASE-T half duplex	**10BASE-T full duplex**	**100BASE-TX half duplex**	**100BASE-TX full duplex**	
Fixed settings	10BASE-T half duplex	--	N	--	N	N
	10BASE-T full duplex	--	10BASE-T full duplex	--	N	N
	100BASE-TX half duplex	--	N	--	N	N
	100BASE-TX full duplex	--	N	--	100BASE-TX full duplex	N
	1000BASE-T half duplex	--	N	--	N	N
	1000BASE-T full duplex	--	N	--	N	N

Settings on the remote device		Settings on the Switch				
Method	Interface	Fixed settings				Auto-negotiation
		10BASE-T half duplex	10BASE-T full duplex	100BASE-TX half duplex	100BASE-TX full duplex	
Auto-negotiation settings	10BASE-T half duplex	--	N	--	N	N
	10BASE-T full duplex	--	N	--	N	10BASE-T full duplex
	10BASE-T full duplex and half duplex	--	N	--	N	10BASE-T full duplex
	100BASE-TX half duplex	--	N	--	N	N
	100BASE-TX full duplex	--	N	--	N	100BASE-TX full duplex
	100BASE-TX full duplex and half duplex	--	N	--	N	100BASE-TX full duplex
	10BASE-T/ 100BASE-TX full duplex and half duplex	--	N	--	N	100BASE-TX full duplex
	1000BASE-T half duplex	--	N	--	N	N
	1000BASE-T full duplex	--	N	--	N	1000BASE-T full duplex
	1000BASE-T full duplex and half duplex	--	N	--	N	1000BASE-T full duplex
	10BASE-T/ 100BASE-TX/ 1000BASE-T full duplex and half duplex	--	N	--	N	1000BASE-T full duplex

Legend: N: A connection is not possible, --: Operation mode not supported

Table 16-8: Connection specifications for transmission speed and duplex mode (full or half) (when using SFP for 10BASE-T, 100BASE-TX, and 1000BASE-T on SFP and SFP+ ports) **[AX3800S]**

Settings on the remote device		**Settings on the Switch**				
Method	**Interface**	**Fixed settings**				**Auto negotiation**
		10BASE-T half duplex	**10BASE-T full duplex**	**100BASE-TX half duplex**	**100BASE-TX full duplex**	
Fixed settings	10BASE-T half duplex	--	--	--	--	N
	10BASE-T full duplex	--	--	--	--	N
	100BASE-TX half duplex	--	--	--	--	N
	100BASE-TX full duplex	--	--	--	--	N
	1000BASE-T half duplex	--	--	--	--	N
	1000BASE-T full duplex	--	--	--	--	N

Settings on the remote device		Settings on the Switch				
Method	Interface	Fixed settings				Auto negotiation
		10BASE-T half duplex	10BASE-T full duplex	100BASE-TX half duplex	100BASE-TX full duplex	
Auto-negotiation settings	10BASE-T half duplex	--	--	--	--	N
	10BASE-T full duplex	--	--	--	--	N
	10BASE-T full duplex and half duplex	--	--	--	--	N
	100BASE-TX half duplex	--	--	--	--	N
	100BASE-TX full duplex	--	--	--	--	N
	100BASE-TX full duplex and half duplex	--	--	--	--	N
	10BASE-T/ 100BASE-TX full duplex and half duplex	--	--	--	--	N
	1000BASE-T half duplex	--	--	--	--	N
	1000BASE-T full duplex	--	--	--	--	1000BASE-T full duplex
	1000BASE-T full duplex and half duplex	--	--	--	--	1000BASE-T full duplex
	10BASE-T/ 100BASE-TX/ 1000BASE-T full duplex and half duplex	--	--	--	--	1000BASE-T full duplex

Legend: N: A connection is not possible, --: Operation mode not supported

■ AX3650S

Table 16-9: Connection specifications for transmission speed and duplex mode (full or half) **[AX3650S]**

Settings on the remote device		Settings on the Switch				
Method	Interface	Fixed settings				Auto negotiation
		10BASE-T half duplex	10BASE-T full duplex	100BASE-TX half duplex	100BASE-TX full duplex	
Fixed settings	10BASE-T half duplex	10BASE-T half duplex	N	N	N	10BASE-T half duplex
	10BASE-T full duplex	N	10BASE-T full duplex	N	N	N
	100BASE-TX half duplex	N	N	100BASE-TX half duplex	N	100BASE-TX half duplex
	100BASE-TX full duplex	N	N	N	100BASE-TX full duplex	N
	1000BASE-T half duplex	N	N	N	N	N
	1000BASE-T full duplex	N	N	N	N	N

Settings on the remote device		Settings on the Switch				
Method	Interface	Fixed settings				Auto negotiation
		10BASE-T half duplex	10BASE-T full duplex	100BASE-TX half duplex	100BASE-TX full duplex	
Auto-negotiation settings	10BASE-T half duplex	10BASE-T half duplex	N	N	N	10BASE-T half duplex
	10BASE-T full duplex	N	N	N	N	10BASE-T full duplex
	10BASE-T full duplex and half duplex	10BASE-T half duplex	N	N	N	10BASE-T full duplex
	100BASE-TX half duplex	N	N	100BASE-TX half duplex	N	100BASE-TX half duplex
	100BASE-TX full duplex	N	N	N	N	100BASE-TX full duplex
	100BASE-TX full duplex and half duplex	N	N	100BASE-TX half duplex	N	100BASE-TX full duplex
	10BASE-T/ 100BASE-TX full duplex and half duplex	10BASE-T half duplex	N	100BASE-TX half duplex	N	100BASE-TX full duplex
	1000BASE-T half duplex	N	N	N	N	N
	1000BASE-T full duplex	N	N	N	N	1000BASE-T full duplex
	1000BASE-T full duplex and half duplex	N	N	N	N	1000BASE-T full duplex
	10BASE-T/ 100BASE-TX/ 1000BASE-T full duplex and half duplex	10BASE-T half duplex	N	100BASE-TX half duplex	N	1000BASE-T full duplex

Legend: N: A connection is not possible

(2) Auto-negotiation

Auto-negotiation is functionality by which two devices negotiate to determine the connection conditions (transmission speed, duplex mode (full or half), and whether to use flow control).

For details on the connection specifications for the Switch, see *Table 16-7: Connection specifications for transmission speed and duplex mode (full or half) [AX3800S]* to *Table 16-9: Connection specifications for transmission speed and duplex mode (full or half) [AX3650S]*. Note that if the connection conditions are not determined by auto-negotiation, the Switch attempts to establish a connection until a link is established.

(3) Flow control [AX3650S]

The flow control functionality sends a pause packet to the remote device to instruct it to temporarily stop sending frames so that received frames are not discarded when the reception buffer on the switch is full. Conversely, when the switch receives a pause packet, it regulates sending to the remote device. Note that flow control is available only in full-duplex mode.

The Switch monitors the usage of the reception buffer, and sends a pause packet to the remote device when sending on the remote device must be regulated. When the Switch receives a pause packet, it regulates sending to the remote device. Whether to enable or disable flow control is set separately for sending and reception. The flow control settings for sending and reception are configured separately. Whether to enable or disable flow control depends on these settings and the auto-negotiation result. When specifying the flow control settings, make sure that the sending and receiving settings on the Switch and the remote device do not conflict. For example, if you set `on` for the pause-packet send setting on the Switch, pause packet reception on the remote device must be enabled. For details about how the operation mode is determined from the settings on the Switch and remote device, see *Table 16-10: Flow control for sending on the switch*, *Table 16-11: Flow control for receiving on the switch*, and *Table 16-12: Flow control operation determined by the auto-negotiation result*.

Table 16-10: Flow control for sending on the switch

Pause-packet send setting on the Switch	Pause-packet receive setting on the remote device	Flow control operation
on	Enabled	Sending on the remote device is regulated.
off	Disabled	Sending on the remote device is not regulated.
desired	desired	Sending on the remote device is regulated.

Legend:

on: Enabled.

off: Disabled. If either `on` or `off` is set when `desired` is set on the remote device, the flow control operation mode is determined by the negotiation result. For details, see *Table 16-12: Flow control operation determined by the auto-negotiation result*.

desired: Enabled. If auto-negotiation is selected, the flow control operation mode is determined from the negotiation result. For details, see *Table 16-12: Flow control operation determined by the auto-negotiation result*.

Table 16-11: Flow control for receiving on the switch

Pause-packet receive setting on the Switch	Pause-packet send setting on the remote device	Flow control operation
on	Enabled	Sending on the Switch is regulated.
off	Disabled	Sending on the Switch is not regulated.

Pause-packet receive setting on the Switch	Pause-packet send setting on the remote device	Flow control operation
desired	desired	Sending on the Switch is regulated.

Legend:

on: Enabled.

off: Disabled. If either `on` or `off` is set when `desired` is set on the remote device, the flow control operation mode is determined by the negotiation result. For details, see *Table 16-12: Flow control operation determined by the auto-negotiation result*.

desired: Enabled. If auto-negotiation is selected, the flow control operation mode is determined from the negotiation result. For details, see *Table 16-12: Flow control operation determined by the auto-negotiation result*.

Table 16-12: Flow control operation determined by the auto-negotiation result

The Switch		Remote device		Result of auto-negotiation on the Switch		Flow control operation	
Send pause packet	Receive pause packet	Send pause packet	Receive pause packet	Send pause packet	Receive pause packet	Is sending regulated on the Switch?	Is sending regulated on the remote device?
on	desired	Enabled	Enabled	on	on	Yes	Yes
			Disabled	on	off	No	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	No	Yes
			Disabled	on	off	No	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	on	off	No	No
			desired	on	on	Yes	Yes
off		Enabled	Enabled	on	on	Yes	Yes
			Disabled	off	on	Yes	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	No	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	off	on	Yes	No
			desired	on	on	Yes	Yes

The Switch		Remote device		Result of auto-negotiation on the Switch		Flow control operation	
Send pause packet	Receive pause packet	Send pause packet	Receive pause packet	Send pause packet	Receive pause packet	Is sending regulated on the Switch?	Is sending regulated on the remote device?
desired	on	Enabled	Enabled	on	on	Yes	Yes
			Disabled	off	on	Yes	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	No	Yes
			Disabled	off	on	No	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	off	on	No	No
			desired	on	on	Yes	Yes
	off	Enabled	Enabled	off	off	No	No
			Disabled	off	off	No	No
			desired	off	off	No	No
		Disabled	Enabled	on	off	No	Yes
			Disabled	off	off	No	No
			desired	on	off	No	Yes
		desired	Enabled	off	off	No	No
			Disabled	off	off	No	No
			desired	off	off	No	No
	desired	Enabled	Enabled	on	on	Yes	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	No	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes

(4) Automatic MDIX functionality

The automatic MDIX functionality automatically switches between MDI and MDI-X. The functionality enables communication via either a crossover cable or a straight cable, and is available only when auto-negotiation is used. This functionality supported only during auto-negotiation. If the connection mode (full duplex or half duplex) is fixed, MDI-X is always selected. The following table describes the MDI and MDI-X pin mappings.

Table 16-13: MDI and MDI-X pin mappings

RJ45	MDI			MDI-X		
Pin No.	1000BASE-T	100BASE-TX	10BASE-T	1000BASE-T	100BASE-TX	10BASE-T
1	BI_DA+	TD+	TD+	BI_DB+	RD+	RD+
2	BI_DA-	TD-	TD-	BI_DB-	RD-	RD-
3	BI_DB+	RD+	RD+	BI_DA+	TD+	TD+
4	BI_DC+	Unused	Unused	BI_DD+	Unused	Unused
5	BI_DC-	Unused	Unused	BI_DD-	Unused	Unused
6	BI_DB-	RD-	RD-	BI_DA-	TD-	TD-
7	BI_DD+	Unused	Unused	BI_DC+	Unused	Unused
8	BI_DD-	Unused	Unused	BI_DC-	Unused	Unused

Note 1:

For the 10BASE-T and 100BASE-TX cables, separate signal lines are used for sending (TD) and reception (RD).

Note 2:

For the 1000BASE-T cable, because all eight pins are used for both sending and reception (simultaneous bi-directional communication), the signal names are different from other cables. `BI_Dx` indicates a bi-directional data signal.

(5) Jumbo frames

Jumbo frame support allows a switch to forward frames whose total field size from DA (in the MAC header) to DATA is larger than 1518 octets. In addition to using jumbo frames, you can also increase the fragment size of IP packets by using the `ip mtu` configuration command to change the MTU value.

The Switch supports only frames in Ethernet V2 format. The Switch does not support frames in 802.3 format. For details about frame formats, see *16.1.3 Control on the MAC and LLC sublayers*. For details about tagged frame formats, see *20.1.5 VLAN tags*. Note that the switch supports only 100BASE-TX (full duplex) and 1000BASE-T (full duplex) as the physical interface. The following table describes the jumbo frame support status.

Table 16-14: Jumbo frame support status

Item	Frame format		Description
	Ethernet V2#	IEEE 802.3#	
Frame size (octets)	1519-9234	N	Total field size of DA (in the MAC header) to DATA (FCS excluded).

Item	Frame format		Description
	Ethernet V2#	IEEE 802.3#	
Reception	Y	N	Frames in IEEE 802.3 format are discarded when the value of the LENGTH field is 0x05DD (1501 octets) or larger.
Sending	Y	N	Frames in IEEE 802.3 format are not sent.

Legend: Y: Supported, N: Not supported

#: For details about the frame formats, see *16.1.3 Control on the MAC and LLC sublayers*.

(6) Notes on a 10BASE-T, 100BASE-TX, or 1000BASE-T connection

- Make sure that the transmission speed and the duplex mode (full or half) settings on the local and remote devices are the same.

  If these settings on the devices are different, communication might stop. If communication stops, execute the `inactivate` command, and then execute the `activate` command for the relevant ports.
- For details on the cables that can be used, see the *Hardware Instruction Manual*.
- A full-duplex interface is implemented by not using collision detection and loopback functions. Therefore, to use a 10BASE-T or 100BASE-TX connection for a full-duplex interface, always make sure that the remote port is set as a full-duplex interface.
- If 1000BASE-T is used, only full-duplex auto-negotiation mode is supported.
- For AX3830S, if 10BASE-T and 100BASE-TX is used, only full-duplex connection is supported.
- When the 10BASE-T, 100BASE-TX, and 1000BASE-T ports of AX3830S-44X4QW are used with 1000BASE-T, the throughput is limited to 600 Mbit/s according to the packet length, packets may be discarded regardless of the priority, or wrong values may be displayed in the MIB of the relevant line. Therefore, we recommend you use the relevant port under the following conditions:
  - Use the port with 10BASE-T or 100BASE-TX (In the configuration when the switch is initially installed or after the `erase configuration` operation command is executed, `speed auto 10 100` is set).
  - When using the 1000BASE-T port, shape the line speed of local switch and the partner switch at 600 Mbit/s or less.
- When using the 1000BASE-T port, you should use it for, for example, maintenance operations, which cause no problem even if packets are discarded regardless of priority.

16.4.2 SFP for 10BASE-T/100BASE-TX/1000BASE-T

For the Switch, you can establish a 10BASE-T, 100BASE-TX, or 1000BASE-T connection with a 1000BASE-X (SFP) port by using a special SFP.

AX3830S series switches support only 1000BASE-T connections.

For AX3650S series switches, the 1000BASE-X (SFP) port is same as the 10BASE-T, 100BASE-TX, 1000BASE-T ports in an SFP connection.

16.5 Configuration of 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces

16.5.1 Configuring Ethernet settings

(1) Setting the transmission speed and duplex mode

You can set the transmission speed and duplex mode used for communication between the Switch and a remote device. By default, the transmission speed and duplex mode are determined automatically by auto-negotiation.

(a) Connecting to a remote device that does not support auto-negotiation

Points to note

Depending on the remote device, 10BASE-T or 100BASE-TX connection sometimes cannot be established by auto-negotiation. If the connection cannot be established, you need to specify the transmission speed and duplex mode according to the remote device, and establish a connection with fixed settings.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/10
(config-if)# shutdown
(config-if)# speed 10
(config-if)# duplex half
```

Configures the switch so that the connection with the remote device is a 10BASE-T, half-duplex connection.

2.
```
(config-if)# no shutdown
```

(b) Using a specific communication speed even when auto-negotiation is used

Points to note

For the Switch, you can set a specific transmission speed even when auto-negotiation is used for a connection. Note that if auto-negotiation is used and a specific transmission speed is also specified, even if a connection with auto-negotiation is successful, the status of the line is not link-up unless the set transmission speed is assured. This eliminates the risk of the line being connected at an unexpected transmission speed.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/10
(config-if)# shutdown
(config-if)# speed auto 1000
```

Configures the switch so that only a 1000BASE-T connection is used when the switch connects to the remote device via auto-negotiation.

2.
```
(config-if)# no shutdown
```

Notes

Make sure that you set a valid combination for the transmission speed and duplex mode. If you use auto-negotiation, you must set auto-negotiation for both the transmission speed and the duplex mode. If you use fixed settings, you must use fixed settings for both the transmission speed and the duplex mode. If the combination is invalid, a connection with the remote device is established via auto-negotiation.

16.5.2 Configuring flow control [AX3650S]

For details, see *16.2.9 Configuring flow control [AX3650S]*.

16.5.3 Configuring the automatic MDIX functionality

The 10BASE-T, 100BASE-TX, or 1000BASE-T port on the Switch supports the automatic MDIX functionality, which automatically selects MDI or MDI-X according to the cable type (straight or crossover) during auto-negotiation. This functionality can be disabled on the switch. If it is disabled, MDI-X (for hub use) is always selected.

Points to note

If MDI-X is always used for a specific interface, disable the automatic MDIX functionality for the interface.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/24
```
Specifies that Ethernet interface 1/0/24 is to be configured.

2.
```
(config-if)# no mdix auto
(config-if)# exit
```
Disables the automatic MDIX functionality so that MDI-X is always selected.

16.6 Description of the 100BASE-FX interface [AX3650S]

16.6.1 Functionality

This section describes an Ethernet interface that uses a 100BASE-FX optical fiber cable.

(1) Connection interface

(a) 100BASE-FX

The 100BASE-FX interface is supported. A transmission speed of 100 Mbit/s and the duplex mode (full or half) are configured as fixed settings. Auto-negotiation is not supported.

100BASE-FX:

> Uses a two-kilometer multi-mode optical fiber cable that ensures a connection over that distance.
>
> (2 km max. in multi-mode)

You can configure either of the modes shown below. Select the appropriate mode for the network to be connected. The default for the Switch is full duplex (fixed).

- 100BASE-FX full duplex (fixed)
- 100BASE-FX half duplex (fixed)

(b) 100BASE-FX connection specifications

The table below describes the connection specifications for transmission speed and duplex mode (full or half) for a connection between the Switch and a remote device. For details about the physical specifications for the 100BASE-FX interface, see the *Hardware Instruction Manual*.

Table 16-15: Connection specifications for transmission speed and duplex mode (full or half)

Settings on the remote device		Settings on the Switch	
Method	**Interface**	**Fixed settings**	
		100BASE half duplex	**100BASE full duplex**
Fixed settings	100BASE half duplex	100BASE half duplex	N
	100BASE full duplex	N	100BASE full duplex
Auto-negotiation settings	100BASE half duplex	N	N
	100BASE full duplex	N	N

Legend: N: A connection is not possible

(2) Flow control

The flow control functionality sends a pause packet to the remote device to instruct it to temporarily stop sending frames so that received frames are not discarded when the reception buffer on the switch is full. Conversely, when the switch receives a pause packet, it regulates sending to the remote device. Note that flow control is available only in full-duplex mode.

The Switch monitors the usage of the reception buffer, and sends a pause packet to the remote device when sending on the remote device must be regulated. When the Switch receives a pause packet, it regulates sending to the remote device. Whether to enable or disable flow control is set separately for sending and reception. When specifying the flow control settings, make sure that the sending and receiving settings on the Switch and the remote device do not conflict. For example, if you set `on` for the pause-packet send setting on the Switch, pause packet reception on the remote device must be enabled. For details about how the operation mode is determined from the settings on the Switch and remote device, see *Table 16-16: Flow control for sending on the switch* and *Table 16-17: Flow control for receiving on the switch*.

Table 16-16: Flow control for sending on the switch

Pause-packet send setting on the Switch	Pause-packet receive setting on the remote device	Flow control operation
on	Enabled	Sending on the remote device is regulated.
off	Disabled	Sending on the remote device is not regulated.
desired	desired	Sending on the remote device is regulated.

Legend: on: Enabled, off: Disabled, desired: Enabled

Table 16-17: Flow control for receiving on the switch

Pause-packet receive setting on the Switch	Pause-packet send setting on the remote device	Flow control operation
on	Enabled	Sending on the Switch is regulated.
off	Disabled	Sending on the Switch is not regulated.
desired	desired	Sending on the Switch is regulated.

Legend: on: Enabled, off: Disabled, desired: Enabled

(3) Jumbo frames

Jumbo frame support allows a switch to forward frames whose total field size from DA (in the MAC header) to DATA is larger than 1518 octets. In addition to using jumbo frames, you can also increase the fragment size of IP packets by using the `ip mtu` configuration command to change the MTU value.

The Switch supports only frames in Ethernet V2 format. The Switch does not support frames in 802.3 format. For details about frame formats, see *16.1.3 Control on the MAC and LLC sublayers*. For details about tagged frame formats, see *20.1.5 VLAN tags*. Note that switches support only 100BASE-FX (full duplex) as the physical interface. The following table describes the jumbo frame support status.

Table 16-18: Jumbo frame support status

Item	Frame format		Description
	Ethernet V2#	IEEE 802.3#	
Frame size (octets)	1519-9234	N	Total field size of DA (in the MAC header) to DATA (FCS excluded).
Reception	Y	N	Frames in IEEE 802.3 format are discarded when the value of the LENGTH field is 0x05DD (1501 octets) or larger.
Sending	Y	N	Frames in IEEE 802.3 format are not sent.

Legend: Y: Supported, N: Not supported

#: For details about the frame formats, see *16.1.3 Control on the MAC and LLC sublayers*.

(4) Notes on a 100BASE-FX connection

- Only a connection with fixed settings of 100BASE and full-duplex or half-duplex mode is supported.
- If a switch and remote device to be connected do not have the same duplex mode (full or half), the devices cannot be connected.
- If a transceiver not indicated in the *Hardware Instruction Manual* is used, correct operation is not guaranteed.

16.6.2 SFP for a 100BASE-FX connection

For the Switch, you can establish a 100BASE-FX connection with a 1000BASE-X (SFP) port by using a special SFP.

The following switch supports SFPs for 100BASE-FX connections:

- AX3650S-20S6XW#

#: The SFP for a 100BASE-FX connection can be established with SFP slot ports 1 to 20.

16.7 Configuration of the 100BASE-FX interface [AX3650S]

16.7.1 Configuring ports

(1) Setting the transmission speed and duplex mode

You can set the transmission speed and duplex mode used for communication between the Switch and a remote device. By default, the settings are fixed at 100BASE and full-duplex mode.

Points to note

For a 100BASE-FX connection, you must make sure that the same transmission speed and duplex mode settings are configured on both the switch and remote device.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/5
(config-if)# shutdown
(config-if)# speed 100
(config-if)# duplex full
```
Configures a 100BASE, full-duplex connection with the remote device.

2.
```
(config-if)# no shutdown
```

Notes

Always make sure that the transmission speed 100 (100 Mbit/s) is set for `speed`, and `full` (full-duplex mode) is set for `duplex`. If you specify invalid parameters, the defaults are used. The default for `speed` is 100, and the default for `duplex` is `full`.

16.7.2 Configuring flow control

For details, see *16.2.9 Configuring flow control [AX3650S]*.

16.8 Description of the 1000BASE-X interface

16.8.1 Functionality

This section describes an Ethernet interface that uses a 100BASE-X optical fiber cable.

(1) Connection interface

(a) 1000BASE-X

The 1000BASE-SX, 1000BASE-SX2, 1000BASE-LX, 1000BASE-LH, 1000BASE-LHB, and 1000BASE-BX interfaces are supported. The transmission speed and duplex mode settings are fixed at 1000 Mbit/s and full duplex.

1000BASE-SX:

Used for short-distance connections.

(550 m max. in multi-mode)

1000BASE-SX2: **[AX3650S]**

Uses a two-kilometer multi-mode optical fiber cable that ensures a connection over that distance.

(2 km max. in multi-mode)

1000BASE-LX:

Used for medium-distance connections.

(5 km max. in single-mode, 550 m max. in multi-mode)

1000BASE-LH and 1000BASE-LHB:

Used for long-distance connections.

1000BASE-LH (70 km max. in single-mode)

1000BASE-LHB (100 km max. in single-mode)

1000BASE-BX:

A low-cost interface that uses a single-core optical fiber for which different wavelengths are used for sending and reception.

Because the upstream and downstream wavelengths are different, a pair of transceivers must be provided for each upstream and downstream.

The Switch supports the 1000BASE-BX10-D and 1000BASE-BX10-U interfaces, prescribed in IEEE 802.3ah, and the 1000BASE-BX40-D and 1000BASE-BX40-U interfaces, which are vendor-specific interfaces.

1000BASE-BX10-D and 1000BASE-BX10-U:

Used for medium-distance connections.

(10 km max. in single-mode)

1000BASE-BX40-D and 1000BASE-BX40-U:

Used for long-distance connections.

(40 km max. in single-mode)

You can configure either of the modes shown below. Select the appropriate mode for the network to be connected. The default for the Switch is auto-negotiation.

- Auto-negotiation

- 1000BASE-X full duplex (fixed)

(b) 1000BASE-X connection specifications

The table below describes the connection specifications for transmission speed and duplex mode (full or half) for a connection between the Switch and a remote device. For details about the physical specifications for the 1000BASE-X interface, see the *Hardware Instruction Manual*.

Table 16-19: Connection specifications for transmission speed and duplex mode (full or half)

Settings on the remote device		Settings on the Switch	
Method	**Interface**	**Fixed settings**	**Auto-negotiation**
		1000BASE full duplex	**1000BASE full duplex**
Fixed settings	1000BASE half duplex	N	N
	1000BASE full duplex	1000BASE full duplex	N
Auto-negotiation settings	1000BASE half duplex	N	N
	1000BASE full duplex	N	1000BASE full duplex

Legend: N: A connection is not possible

(2) Auto-negotiation

Auto-negotiation is a functionality by which two devices negotiate to determine whether to select full-duplex mode and whether to use flow control.

For details on the connection specifications for the Switch, see *Table 16-19: Connection specifications for transmission speed and duplex mode (full or half)*. Note that if the connection conditions are not determined by auto-negotiation, the Switch attempts to establish a connection until a link is established.

(3) Flow control [AX3650S]

The flow control functionality sends a pause packet to the remote device to instruct it to temporarily stop sending frames so that received frames are not discarded when the reception buffer on the switch is full. Conversely, when the switch receives a pause packet, it regulates sending to the remote device. Note that flow control is available only in full-duplex mode.

The Switch monitors the usage of the reception buffer, and sends a pause packet to the remote device when sending on the remote device must be regulated. When the Switch receives a pause packet, it regulates sending to the remote device. Whether to enable or disable flow control is set separately for sending and reception. The flow control settings for sending and reception are configured separately. Whether to enable or disable flow control depends on these settings and the auto-negotiation result. When specifying the flow control settings, make sure that the sending and receiving settings on the Switch and the remote device do not conflict. For example, if you set `on` for the pause-packet send setting on the Switch, pause packet reception on the remote device must be enabled. For details about how the operation mode is determined from the settings on the Switch and remote device, see *Table 16-20: Flow control for sending on the switch*, *Table 16-21: Flow control for receiving on the switch*, and *Table 16-22: Flow control operation determined by the auto-negotiation result.*

Table 16-20: Flow control for sending on the switch

Pause-packet send setting on the Switch	Pause-packet receive setting on the remote device	Flow control operation
on	Enabled	Sending on the remote device is regulated.
off	Disabled	Sending on the remote device is not regulated.
desired	desired	Sending on the remote device is regulated.

Legend:

on: Enabled.

off: Disabled. If either `on` or `off` is set when `desired` is set on the remote device, the flow control operation mode is determined by the negotiation result. For details, see *Table 16-22: Flow control operation determined by the auto-negotiation result*.

desired: Enabled. If auto-negotiation is selected, the flow control operation mode is determined from the negotiation result. For details, see *Table 16-22: Flow control operation determined by the auto-negotiation result*.

Table 16-21: Flow control for receiving on the switch

Pause-packet receive setting on the Switch	Pause-packet send setting on the remote device	Flow control operation
on	Enabled	Sending on the Switch is regulated.
off	Disabled	Sending on the Switch is not regulated.
desired	desired	Sending on the Switch is regulated.

Legend:

on: Enabled.

off: Disabled. If either `on` or `off` is set when `desired` is set on the remote device, the flow control operation mode is determined by the negotiation result. For details, see *Table 16-22: Flow control operation determined by the auto-negotiation result*.

desired: Enabled. If auto-negotiation is selected, the flow control operation mode is determined from the negotiation result. For details, see *Table 16-22: Flow control operation determined by the auto-negotiation result*.

Table 16-22: Flow control operation determined by the auto-negotiation result

The Switch		Remote device		Result of auto-negotiation on the Switch		Flow control operation	
Send pause packet	Receive pause packet	Send pause packet	Receive pause packet	Send pause packet	Receive pause packet	Is sending regulated on the Switch?	Is sending regulated on the remote device?
on	desired	Enabled	Enabled	on	on	Yes	Yes
			Disabled	on	off	No	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	No	Yes

The Switch		**Remote device**		**Result of auto-negotiation on the Switch**		**Flow control operation**	
Send pause packet	**Receive pause packet**	**Send pause packet**	**Receive pause packet**	**Send pause packet**	**Receive pause packet**	**Is sending regulated on the Switch?**	**Is sending regulated on the remote device?**
			Disabled	on	off	No	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	on	off	No	No
			desired	on	on	Yes	Yes
off		Enabled	Enabled	on	on	Yes	Yes
			Disabled	off	on	Yes	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	No	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	off	on	Yes	No
			desired	on	on	Yes	Yes
desired	on	Enabled	Enabled	on	on	Yes	Yes
			Disabled	off	on	Yes	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	No	Yes
			Disabled	off	on	No	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	off	on	No	No
			desired	on	on	Yes	Yes
	off	Enabled	Enabled	off	off	No	No
			Disabled	off	off	No	No
			desired	off	off	No	No
		Disabled	Enabled	on	off	No	Yes
			Disabled	off	off	No	No
			desired	on	off	No	Yes
		desired	Enabled	off	off	No	No

The Switch		Remote device		Result of auto-negotiation on the Switch		Flow control operation	
Send pause packet	Receive pause packet	Send pause packet	Receive pause packet	Send pause packet	Receive pause packet	Is sending regulated on the Switch?	Is sending regulated on the remote device?
			Disabled	off	off	No	No
			desired	off	off	No	No
	desired	Enabled	Enabled	on	on	Yes	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	No	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes

(4) Jumbo frames

Jumbo frame support allows a switch to forward frames whose total field size from DA (in the MAC header) to DATA is larger than 1518 octets. In addition to using jumbo frames, you can also increase the fragment size of IP packets by using the `ip mtu` configuration command to change the MTU value.

The Switch supports only frames in Ethernet V2 format. The Switch does not support frames in 802.3 format. For details about frame formats, see *16.1.3 Control on the MAC and LLC sublayers*. For details about tagged frame formats, see *20.1.5 VLAN tags*. The following table describes the jumbo frame support status.

Table 16-23: Jumbo frame support status

Item	Frame format		Description
	Ethernet V2#	IEEE 802.3#	
Frame size (octets)	1519-9234	N	Total field size of DA (in the MAC header) to DATA (FCS excluded).
Reception	Y	N	Frames in IEEE 802.3 format are discarded when the value of the LENGTH field is 0x05DD (1501 octets) or larger.
Sending	Y	N	Frames in IEEE 802.3 format are not sent.

Legend: Y: Supported, N: Not supported

#: For details about the frame formats, see *16.1.3 Control on the MAC and LLC sublayers*.

(5) Notes on a 1000BASE-X connection

- Only a connection by using auto-negotiation or a fixed connection in full-duplex mode is supported.

- Make sure that the remote device (such as a switching hub) uses auto-negotiation or the fixed full-duplex mode setting.
- If a transceiver not indicated in the *Hardware Instruction Manual* is used, correct operation is not guaranteed.

16.9 Configuration of the 1000BASE-X interface

16.9.1 Configuring ports

(1) Setting the transmission speed and duplex mode

You can set the transmission speed and duplex mode used for communication between the Switch and a remote device. By default, the transmission speed and duplex mode are determined automatically by auto-negotiation.

Points to note

The Switches connect to remote devices by auto-negotiation. Because auto-negotiation is the default connection method for the Switch, you do not need to set transmission speed and duplex mode. If auto-negotiation is not used, set the transmission speed to 1000 Mbit/s and the duplex mode to full duplex.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# shutdown
(config-if)# speed 1000
(config-if)# duplex full
```

   Configures a switch so that it connects to the remote device at a transmission speed of 1000 Mbit/s in full-duplex mode.

2.
```
(config-if)# no shutdown
```

Notes

If you set a transmission speed of 1000 Mbit/s, always make sure that `duplex` is `full` (full duplex). If the `speed` and `duplex` settings are not specified correctly, auto-negotiation is used to establish a connection.

16.9.2 Configuring flow control [AX3650S]

For details, see *16.2.9 Configuring flow control [AX3650S]*.

16.10 Description of the 10GBASE-R interface

16.10.1 Functionality

This section describes an Ethernet interface that uses a 10GBASE-R optical fiber cable.

(1) Connection interface

(a) 10GBASE-R

The 10GBASE-SR, 10GBASE-LR, and 10GBASE-ER interfaces are supported. The transmission speed and duplex mode settings are fixed at 10 Gbit/s and full duplex.

10GBASE-SR:

Used for short-distance connections (300 m max.# in multi-mode).

#

The maximum distance depends on the cable used. For details about the distance for each cable, see the *Hardware Instruction Manual*.

10GBASE-LR:

Used for medium-distance connections (10 km max. in single-mode).

10GBASE-ER:

Used for long-distance connections (40 km max. in single-mode).

(b) 10GBASE-R connection specifications

For details about the physical specifications for the 10GBASE-R interface, see the *Hardware Instruction Manual*.

(2) Flow control [AX3650S]

The flow control functionality sends a pause packet to the remote device to instruct it to temporarily stop sending frames so that received frames are not discarded when the reception buffer on the switch is full. Conversely, when the switch receives a pause packet, it regulates sending to the remote device.

The Switch monitors the usage of the reception buffer, and sends a pause packet to the remote device when sending on the remote device must be regulated. When the Switch receives a pause packet, it regulates sending to the remote device. Whether to enable or disable flow control is set separately for sending and reception. When specifying the flow control settings, make sure that the sending and receiving settings on the Switch and the remote device do not conflict. For example, if you set on for the pause-packet send setting on the Switch, pause packet reception on the remote device must be enabled. For details about how the operation mode is determined from the settings on the Switch and remote device, see *Table 16-24: Flow control for sending on the switch* and *Table 16-25: Flow control for receiving on the switch*.

Table 16-24: Flow control for sending on the switch

Pause-packet send setting on the Switch	Pause-packet receive setting on the remote device	Flow control operation
on	Enabled	Sending on the remote device is regulated.
off	Disabled	Sending on the remote device is not regulated.
desired	desired	Sending on the remote device is regulated.

Legend: on: Enabled, off: Disabled, desired: Enabled

Table 16-25: Flow control for receiving on the switch

Pause-packet receive setting on the Switch	Pause-packet send setting on the remote device	Flow control operation
on	Enabled	Sending on the Switch is regulated.
off	Disabled	Sending on the Switch is not regulated.
desired	desired	Sending on the Switch is regulated.

Legend: on: Enabled, off: Disabled, desired: Enabled

(3) Jumbo frames

Jumbo frame support allows a switch to forward frames whose total field size from DA (in the MAC header) to DATA is larger than 1518 octets. In addition to using jumbo frames, you can also increase the fragment size of IP packets by using the `ip mtu` configuration command to change the MTU value.

The Switch supports only frames in Ethernet V2 format. The Switch does not support frames in 802.3 format. For details about frame formats, see *16.1.3 Control on the MAC and LLC sublayers*. For details about tagged frame formats, see *20.1.5 VLAN tags*. The following table describes the jumbo frame support status.

Table 16-26: Jumbo frame support status

Item	Frame format		Description
	Ethernet V2#	IEEE 802.3#	
Frame size (octets)	1519-9234	N	Total field size of DA (in the MAC header) to DATA (FCS excluded).
Reception	Y	N	Frames in IEEE 802.3 format are discarded when the value of the LENGTH field is 0x05DD (1501 octets) or larger.
Sending	Y	N	Frames in IEEE 802.3 format are not sent.

Legend: Y: Supported, N: Not supported

#: For details about the frame formats, see *16.1.3 Control on the MAC and LLC sublayers*.

(4) Notes on 10GBASE-R connection

- In the IEEE 802.3ae standard, half-duplex mode and auto-negotiation are not prescribed for the 10GBASE-R interface. Therefore, only fixed full-duplex mode is supported.
- If a transceiver not indicated in the *Hardware Instruction Manual* is used, correct operation is not guaranteed.

16.11 Configuration of the 10GBASE-R interface

16.11.1 Configuring flow control [AX3650S]

For details, see *16.2.9 Configuring flow control [AX3650S]*.

16.12 Description of the 40GBASE-R interface [AX3800S]

16.12.1 Functionality

This section describes an Ethernet interface that uses a 40GBASE-R optical fiber cable.

(1) Connection interface

(a) 40GBASE-R

The 40GBASE-SR4 and 40GBASE-CR4 interfaces are supported. The line speed of both of them is set to 40 Gbit/s. 40GBASE-SR4 supports fixed full-duplex connections; 40GBASE-CR4 supports connections via auto-negotiation. Note that half-duplex connections are not supported.

40GBASE-SR4:

Used for short-distance connections. Only fixed full-duplex connections are supported. (150 m max.# in multi-mode).

40GBASE-CR4:

Used for short-distance connections. Only connections via during auto-negotiation are supported. (7 m max.# in multi-mode).

#

The maximum distance depends on the cable used. For details about the distance for each cable, see the *Hardware Instruction Manual*.

(b) 40GBASE-R connection specifications

For details about the physical specifications for the 40GBASE-R interface, see the *Hardware Instruction Manual*.

(2) Jumbo frames

Jumbo frame support allows a switch to forward frames whose total field size from DA (in the MAC header) to DATA is larger than 1518 octets. In addition to using jumbo frames, you can also increase the fragment size of IP packets by using the `ip mtu` configuration command to change the MTU value.

The Switch supports only frames in Ethernet V2 format. The Switch does not support frames in 802.3 format. For details about frame formats, see *16.1.3 Control on the MAC and LLC sublayers*. For details about tagged frame formats, see *20.1.5 VLAN tags*. The following table describes the jumbo frame support status.

Table 16-27: Jumbo frame support status

Item	Frame format		Description
	Ethernet V2#	IEEE 802.3#	
Frame size (octets)	1519-9234	N	Total field size of DA (in the MAC header) to DATA (FCS excluded).
Reception	Y	N	Frames in IEEE 802.3 format are discarded when the value of the LENGTH field is 0x05DD (1501 octets) or larger.
Sending	Y	N	Frames in IEEE 802.3 format are not sent.

Legend: Y: Supported, N: Not supported

#: For details about the frame formats, see *16.1.3 Control on the MAC and LLC sublayers*.

(3) Notes on 40GBASE-R connection

- In the IEEE 802.3ba standard, half-duplex mode is not prescribed for the 40GBASE-R interface. Therefore, only full-duplex mode is supported.
- If a transceiver not indicated in the *Hardware Instruction Manual* is used, correct operation is not guaranteed.

16.13 Configuration of the 40GBASE-R interface [AX3800S]

16.13.1 Configuring ports

(1) Setting the transmission speed and duplex mode

When using a QSFP+ for 40GBASE-R, it is not necessary to configure transmission speed and duplex settings because these settings are fixed for the interface.

16.14 Description of SFP/SFP+ ports

16.14.1 Functionality

This section describes an SFP/SFP+ port.

(1) Connection interface

The SFP/SFP+ ports support SFP+ transceivers for 10GBASE-R, and SFP transceivers for 10BASE-T, 100BASE-TX, 1000BASE-T, and 1000BASE-X. Note that only AX3830S series switches support SFP transceivers for a 10BASE-T, 100BASE-TX, or 1000BASE-T connection.

Direct attach cables are supported to connect between SFP/SFP+ ports.

(a) 10GBASE-R

The SFP+ modules for 10GBASE-SR, 10GBASE-LR, and 10GBASE-ER interfaces are supported. For details on the 10GBASE-R interface, see *16.10 Description of the 10GBASE-R interface*.

(b) 1000BASE-X

The SFP modules for 1000BASE-SX, 1000BASE-LX, 1000BASE-LH, 1000BASE-LHB, and 1000BASE-BX interfaces are supported. For details on the 1000BASE-X interface, see *16.8 Description of the 1000BASE-X interface*.

(c) 1000BASE-T [AX3800S]

1000BASE-T connections via 10BASE-T/100BASE-TX/1000BASE-T SFP modules are supported. This SFP transceiver does not support a connection via 10BASE-T or 100BASE-TX. For details on the 1000BASE-T interface, see *16.4 Description of the 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces*.

(d) Direct attach cables

Direct attach cables feature SFP+ connectors at both ends and connect between SFP/SFP+ ports. They function in the same way as 10GBASE-R. For details on the 10GBASE-R interface, see *16.10 Description of the 10GBASE-R interface*.

It takes from five to eight seconds to place ports in the link-up status when using a direct connection cable.

16.15 Configuration of SFP/SFP+ ports

16.15.1 Configuring ports

(1) Setting the transmission speed and duplex mode

When using an SFP+ transceiver for 10GBASE-R, it is not necessary to configure transmission speed and duplex settings because these settings are fixed. When using an SFP transceiver for 1000BASE-X, you can configure the transmission speed and duplex settings for this Switch and the remote device. By default, the transmission speed and duplex mode are determined automatically by auto-negotiation.

Only auto-negotiation can be set for SFP transceivers for 10BASE-T, 100BASE-TX, and 1000BASE-T.

Points to note

The settings are the same as other interfaces, and the interface name in the configuration will also be `tengigabitethernet` when using an SFP transceiver for 10BASE-T, 100BASE-TX, and 1000BASE-T or for 1000BASE-X.

The Switches connect to remote devices by auto-negotiation. Because auto-negotiation is the default connection method for the Switch, you do not need to set transmission speed and duplex mode. Configure the connection speed and duplex settings when auto-negotiation is not used.

Command examples

1.
```
(config)# interface tengigabitethernet 1/0/25
(config-if)# shutdown
(config-if)# speed 1000
(config-if)# duplex full
```
Configures a switch so that it connects to the remote device at a transmission speed of 1000 Mbit/s in full-duplex mode.

2.
```
(config-if)# no shutdown
```

Notes

Make sure that you set a valid combination for the transmission speed and duplex mode. If you use auto-negotiation, you must set auto-negotiation for both the transmission speed and the duplex mode. If you use fixed settings, you must use fixed settings for both the transmission speed and the duplex mode. If the combination is invalid, a connection with the remote device is established via auto-negotiation.

16.15.2 Configuring flow control [AX3650S]

For details, see *16.2.9 Configuring flow control [AX3650S]*.

16.16 Description of QSFP+ ports [AX3800S]

16.16.1 Functionality

This section describes a QSFP+ port.

(1) Connection interface

A QSFP+ port supports for a QSFP+ for 40GBASE-R. In addition, it supports the use of direct connection cables to connect between QSFP+ ports.

(a) 40GBASE-R

QSFP+ for 40GBASE-SR4 is supported. For details on the interface, see *16.12 Description of the 40GBASE-R interface [AX3800S]*.

Note that when a QSFP+ for 40GBASE-R is used, it takes three to five seconds to determine the line type for the `show interfaces` operation command from when the transceiver is inserted.

(b) Direct attach cables

Direct attach cables feature QSFP+ connectors at both ends and connect between QSFP+ ports. The cable operates as 40GBASE-CR4. For details on the interface, see *16.12 Description of the 40GBASE-R interface [AX3800S]*.

Note that when a direct attach cable is used, it takes three to five seconds to determine the line type for the `show interfaces` operation command from when the transceiver is inserted. Also, it takes from five to eight seconds for link-up.

Chapter

17. Link Aggregation

This chapter describes link aggregation and its use.

17.1 Description of the basic link aggregation functionality

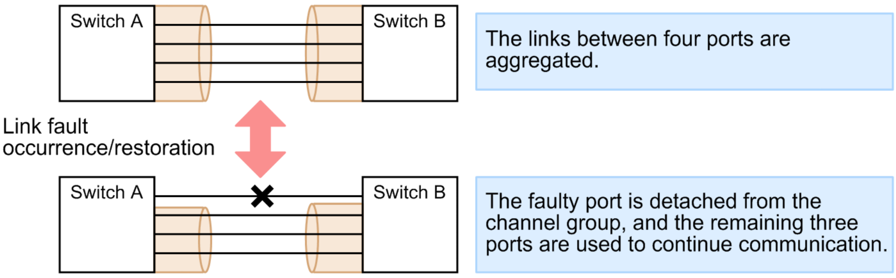
17.1.1 Overview

Link aggregation is functionality that connects devices by establishing multiple links between the Ethernet ports of each device, and that treats these links as one virtual link. The virtual link is called a channel group. Link aggregation can expand bandwidth and ensure redundancy between connected devices.

17.1.2 Link aggregation configuration

The figure below shows an example of a link aggregation configuration. In this example, four ports are aggregated. If a fault occurs on one of these ports, the faulty port is detached from the channel group, and communication continues by using the rest of the ports as the channel group.

Figure 17-1: Example of a link aggregation configuration



The links between four ports are aggregated.

The faulty port is detached from the channel group, and the remaining three ports are used to continue communication.

17.1.3 Supported specifications

(1) Link aggregation modes

The link aggregation of the Switch supports LACP and static modes.

- LACP link aggregation

  LACP link aggregation uses the LACP (Link Aggregation Control Protocol) compliant with IEEE 802.3ad. LACP link aggregation starts operation of a channel group when LACP negotiation is successful. LACP is used to verify consistency and link normality between devices.

- Static link aggregation

  Static link aggregation is link aggregation manually set by using configuration commands. LACP is not used. Operation of a channel group starts when the ports in the channel group are placed in the link-up status.

The following table describes the supported specifications for link aggregation.

Table 17-1: Supported specifications for link aggregation

Item	Supported specifications	Remarks
Number of channel groups per switch	32 (in standalone mode) 52 (in stack mode)	In stack mode, only static is supported.
Maximum number of ports per group	8	--
Link aggregation modes	• LACP • Static	--

Item	Supported specifications	Remarks
Transmission speed between ports	Default: Only the same speed can be used. Mixed-speed mode: Different speeds can be used concurrently.	Default: Slower ports are detached from the group. Mixed-speed mode: No ports are detached from the group due to their transmission speed.
Duplex mode	Only full-duplex mode is supported.	--

Legend: --: Not applicable

17.1.4 MAC address of the channel group

A protocol such as the Spanning Tree Protocol requires the MAC address of a channel group. For the Switch, the MAC address of any of the ports in the channel group is used.

If the port whose MAC address is used is removed from the channel group, the MAC address of the channel group is changed.

During an operation with a stack configured, if the Ethernet interface of the port using the MAC address is deleted along with the deletion of a member switch, the MAC address of the channel group is changed. Also, when the MAC address of the port of the master switch is used for the MAC address of the channel group, if the backup switch becomes a new master switch due to a failure in the current master switch, the MAC address of the channel group is also changed.

17.1.5 Port allocation for sending frames

When link aggregation is used to send frames, to ensure efficient port use, a port is allocated for each frame to distribute the traffic to ports. Ports are allocated based on the information in the frames.

The following table describes the information used for port allocation.

Table 17-2: Port allocation for sending frames (1/2)

Forward	Frame type	Information used for port allocation	port-channel load-balance parameter				
			src-mac	dst-mac	src-dst-mac	src-ip	src-port
Layer 3 forwarding	IP unicast IP broadcast	Destination MAC address	--	Y	Y	--	--
		Source MAC address	Y	--	Y	--	--
		Reception VLAN	Y	Y	Y	--	--
		Destination IP address	--	--	--	--	--
		Source IP address	--	--	--	Y	Y
		Destination TCP/UDP port number	--	--	--	--	--
		Source TCP/UDP port number	--	--	--	--	Y
	IP multicast	Destination IP address	Y	Y	Y	Y	Y
		Source IP address	Y	Y	Y	Y	Y

Forward	Frame type	Information used for port allocation	port-channel load-balance parameter				
			src-mac	dst-mac	src-dst-mac	src-ip	src-port
		Reception port number or reception channel group number	Y	Y	Y	Y	Y
Layer 2 forwarding	Frame for which the MAC address has not been learned yet (unicast, broadcast, and multicast frames)	Destination MAC address	Y	Y	Y	Y	Y
		Source MAC address	Y	Y	Y	Y	Y
		Reception port number or reception channel group number	Y	Y	Y	Y	Y
	IP frame for which the MAC address has been learned	Destination MAC address	--	Y	Y	--	--
		Source MAC address	Y	--	Y	--	--
		VLAN	Y	Y	Y	--	--
		Destination IP address	--	--	--	--	--
		Source IP address	--	--	--	Y	Y
		Destination TCP/UDP port number	--	--	--	--	--
		Source TCP/UDP port number	--	--	--	--	Y
	Non-IP frame for which the MAC address has been learned	Destination MAC address	--	Y	Y	--	--
		Source MAC address	Y	--	Y	Y	Y
		VLAN	Y	Y	Y	Y	Y
		EtherType	Y	Y	Y	Y	Y

Table 17-3: Port allocation for sending frames (2/2)

Forward	Frame type	Information used for port allocation	port-channel load-balance parameter			
			dst-ip	dst-port	src-dst-ip	src-dst-port
Layer 3 forwarding	IP unicast IP broadcast	Destination MAC address	--	--	--	--
		Source MAC address	--	--	--	--
		Reception VLAN	--	--	--	--

Forward	Frame type	Information used for port allocation	port-channel load-balance parameter			
			dst-ip	dst-port	src-dst-ip	src-dst-port
		Destination IP address	Y	Y	Y	Y
		Source IP address	--	--	Y	Y
		Destination TCP/UDP port number	--	Y	--	Y
		Source TCP/UDP port number	--	--	--	Y
	IP multicast	Destination IP address	Y	Y	Y	Y
		Source IP address	Y	Y	Y	Y
		Reception port number or reception channel group number	Y	Y	Y	Y
Layer 2 forwarding	Frame for which the MAC address has not been learned yet (unicast, broadcast, and multicast frames)	Destination MAC address	Y	Y	Y	Y
		Source MAC address	Y	Y	Y	Y
		Reception port number or reception channel group number	Y	Y	Y	Y
	IP frame for which the MAC address has been learned	Destination MAC address	--	--	--	--
		Source MAC address	--	--	--	--
		VLAN	--	--	--	--
		Destination IP address	Y	Y	Y	Y
		Source IP address	--	--	Y	Y
		Destination TCP/UDP port number	--	Y	--	Y
		Source TCP/UDP port number	--	--	--	Y
	Non-IP frame for which the MAC address has been learned	Destination MAC address	Y	Y	Y	Y
		Source MAC address	--	--	Y	Y
		VLAN	Y	Y	Y	Y
		EtherType	Y	Y	Y	Y

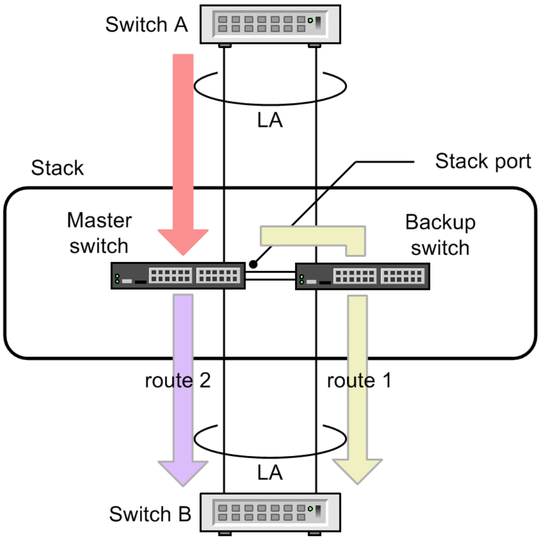
Legend: Y: Allocated; --: Not allocated

Select an appropriate allocation method according to the traffic on the link aggregation to perform efficient load balancing. For example, if sending IP frames to multiple MAC addresses from a host with a single MAC address, you can allocate sending ports more efficiently by selecting the `dst-mac` method instead of selecting the `src-mac` method.

■ Frame sending with priority when a stack is configured

When a stack is configured, frames are first sent to the port of the member switch that received frames in the stack. The following figure shows the frame sending with priority when a stack is configured.

Figure 17-2: Frame sending with priority when a stack is configured



Legend: LA: Link aggregation

The configured stack in the figure shows two routes when frames are forwarded from Switch A to Switch B via the master switch.

1. Route to transmit frames from the stack port to Switch B via the backup switch
2. Route to send frames directly from the master switch's port to Switch B

In this case, the master switch sends frames first to the route 2. If multiple ports that apply to the route 2 exist, ports are selected by following *Table 17-2: Port allocation for sending frames (1/2)* and *Table 17-3: Port allocation for sending frames (2/2)* for sending frames.

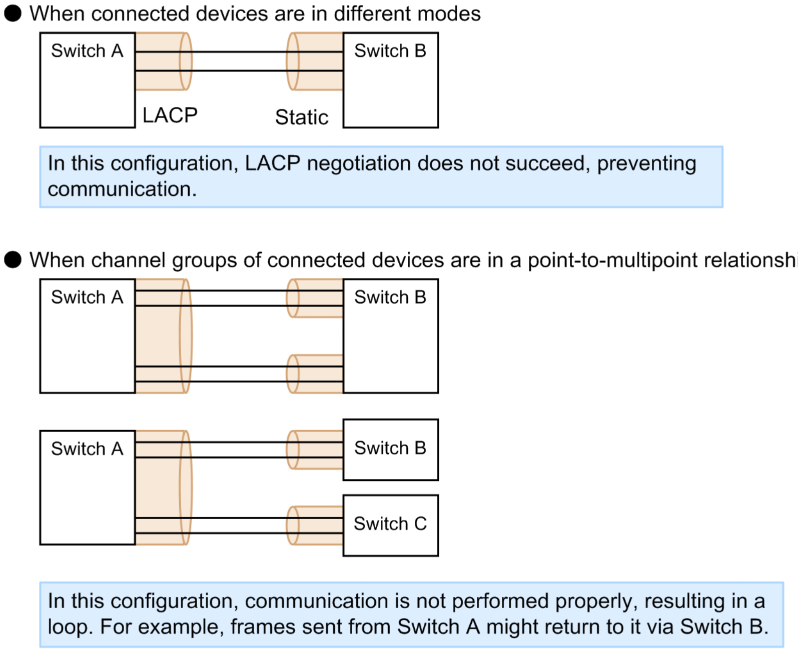
By sending frames first to the port that received frames, switching of the communication route becomes unnecessary even if a failure occurs in other member switch making up the stack. For effectively use of the sending with priority, when using link aggregation for stack, you are recommended to set the sending with priority in other member switch.

17.1.6 Notes on using link aggregation

(1) Configurations in which link aggregation is not possible

To use link aggregation, the settings of the connected devices must match. The following figure shows configurations in which link aggregation is not possible.

Figure 17-3: Examples of configurations in which link aggregation is not possible



● When connected devices are in different modes

In this configuration, LACP negotiation does not succeed, preventing communication.

● When channel groups of connected devices are in a point-to-multipoint relationship

In this configuration, communication is not performed properly, resulting in a loop. For example, frames sent from Switch A might return to it via Switch B.

(2) Configuring link aggregation

To use link aggregation, the settings of the connected devices must match. If the settings of connected devices do not match, a communication loop might occur. When you configure link aggregation, first, change the status of the ports to link-down, and then make sure that the connections between devices are not in a configuration such as those in *(1) Configurations in which link aggregation is not possible*. Next, return the ports to the link-up status.

(3) If CPU load is excessive

If CPU load is excessive when LACP link aggregation mode is used, the LACPDUs (link aggregation control protocol data units) that the Switch sends or receives might be discarded, or the sending or reception might be delayed. If this situation occurs, a timeout message might be output or communication might temporarily stop. If the load is frequently excessive, increase the LACPDU sending interval or use static link aggregation.

17.2 Configuration of the basic link aggregation functionality

17.2.1 List of configuration commands

The following table describes the configuration commands for the basic link aggregation functionality.

Table 17-4: List of configuration commands

Command name	Description
channel-group lacp system-priority	Sets the LACP system priority for each channel group.
channel-group mode	Adds a port to a channel group.
channel-group periodic-timer	Sets the LACPDU sending interval.
description	Sets supplementary information about a channel group.
interface port-channel	Sets up a port channel interface. The parameters of a channel group are also set in port channel interface configuration mode.
lacp port-priority	Sets the LACP port priority.
lacp system-priority	Sets the default for the LACP system priority.
port-channel load-balance	Specifies the allocation method.
shutdown	Stops communication for a channel group

17.2.2 Configuring static link aggregation

Points to note

For static link aggregation, use the `channel-group mode` command to set the channel group number and `on` mode from the Ethernet interface configuration mode. Static link aggregation starts when these settings are set by the `channel-group mode` command.

Command examples

1.
```
(config)# interface range gigabitethernet 1/0/1-2
```
Places the Switch in Ethernet interface configuration mode for configuring ports 1/0/1 and 1/0/2.

2.
```
(config-if-range)# channel-group 10 mode on
```
Adds ports 1/0/1 and 1/0/2 to channel group 10 in static mode.

17.2.3 Configuring LACP link aggregation

(1) Setting the channel group

Points to note

For LACP link aggregation, use the `channel-group mode` command to specify the channel group number, and either `active` or `passive` mode in Ethernet interface configuration mode.

Command examples

1.
```
(config)# interface range gigabitethernet 1/0/1-2
```
Places the Switch in Ethernet interface configuration mode for configuring ports 1/0/1 and 1/0/2.

2.
```
(config-if-range)# channel-group 10 mode active
```
Adds ports 1/0/1 and 1/0/2 to channel group 10 in LACP mode. If `active` mode is specified, the LACP starts sending LACPDUs in active mode, independently of the remote device. If `passive` mode is specified, the LACP starts sending LACPDUs only when LACPDUs are received from the remote device.

(2) Setting the system priority

Set the LACP system priority. For the Switch, the system priority is used for the port detachment restriction functionality, which is an extended function. Normally, you do not need to change the LACP port priority value.

Points to note

The smaller the LACP system priority value set, the higher the priority.

Command examples

1.
```
(config)# lacp system-priority 100
```
Sets the LACP system priority level of the Switch to 100.

2.
```
(config)# interface port-channel 10
(config-if)# channel-group lacp system-priority 50
```
Sets the LACP system priority level of channel group 10 to 50. If this change is not made, the system priority level of the switch (100) is used.

(3) Setting port priority

Set the LACP port priority. For the Switch, the LACP port priority is used for the standby link functionality, which is an extended function. Normally, you do not need to change the LACP port priority value.

Points to note

The smaller the LACP port priority value set, the higher the priority.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# lacp port-priority 100
```
Sets the LACP port priority level of port 1/0/1 to 100.

(4) Setting the LACPDU sending interval

Points to note

The example below shows how to set the interval at which the remote device sends LACPDUs to the Switch. The Switch receives LACPDUs at the set interval.

For the LACPDU sending interval, set `long` (30 seconds) or `short` (1 second). The default is `long` (30 seconds). Setting `short` makes it possible to detect a timeout earlier if a link fault occurs, shortening the length of the communication stoppage.

Command examples

1.
```
(config)# interface port-channel 10
(config-if)# channel-group periodic-timer short
```
Sets the LACPDU sending interval of channel group 10 to `short` (1 second).

Notes

Although fault detection is earlier with the `short` setting (1 second), the increased LACPDU traffic adds to the burden of the link aggregation program. If a timeout message is output or if communication often stops temporarily by setting `short` (1 second), use either the default value of `long` (30 seconds) or static mode.

(5) Specifying the allocation method

Points to note

The example below shows how to specify the channel group allocation method for each Switch.

Command examples

1.
```
(config)# port-channel load-balance src-ip
```
Sets the channel group allocation method to allocate frames according to the source IP addresses.

17.2.4 Configuring a port channel interface

A port channel interface is used to set the functions that operate on a channel group.

A port channel interface is set up manually by using configuration commands or generated automatically when the `channel-group mode` command is executed in Ethernet interface configuration mode.

(1) Relationship between the port channel and Ethernet interfaces

A port channel interface is used to configure the functionality that operates on a channel group. The same functionality can also be configured from the Ethernet interface in configuration mode. Some of the commands provided by these interfaces are related as follows:

- The settings of the related commands of the port channel and Ethernet interfaces must match.
- If the `channel-group mode` command is specified by using an Ethernet interface when a port channel interface has not been set up, the port channel interface is automatically generated. At this time, related commands must not be specified in the Ethernet interface in which the `channel-group mode` command is specified.
- If the `channel-group mode` command is specified by using an Ethernet interface when a port channel interface has already been set up, the settings of the related commands must match.
- If a related command is set by using a port channel interface, the setting is also applied to a related command registered in an Ethernet interface by using the `channel-group mode` command.

The following table describes the port channel interface commands whose settings must be identical with the settings of the related Ethernet interface commands.

Table 17-5: Related commands for a port channel interface

Functionality	Command
VLAN	switchport mode
	switchport access
	switchport trunk
	switchport protocol
	switchport mac
	switchport vlan mapping
	switchport vlan mapping enable
Spanning Tree Protocols	spanning-tree portfast
	spanning-tree bpdufilter
	spanning-tree bpduguard
	spanning-tree guard
	spanning-tree link-type
	spanning-tree port-priority
	spanning-tree cost
	spanning-tree vlan port-priority
	spanning-tree vlan cost
	spanning-tree single port-priority
	spanning-tree single cost
	spanning-tree mst port-priority
	spanning-tree mst cost
IEEE 802.1X	dot1x port-control
	dot1x force-authorize-port
	dot1x multiple-hosts
	dot1x multiple-authentication
	dot1x max-supplicant
	dot1x reauthentication
	dot1x timeout reauth-period
	dot1x timeout tx-period
	dot1x timeout supp-timeout
	dot1x timeout server-timeout
	dot1x timeout keep-unauth
	dot1x timeout quiet-period
	dot1x max-req

Functionality	Command
	dot1x ignore-eapol-start
	dot1x supplicant-detection
DHCP snooping	ip dhcp snooping trust
	ip arp inspection trust
	ip verify source
GSRP	gsrp direct-link
	gsrp reset-flush-port
	gsrp no-flush-port
	gsrp exception-port
L2 loop detection	loop-detection
OADP	oadp enable

(2) Configuration of the functionality that operates on a channel group

Points to note

The port channel interface is used to set up the VLAN, Spanning Tree Protocols, and other functionality used for channel group operations. In this example, you set up a trunk port.

Command examples

1.
```
(config)# interface range gigabitethernet 1/0/1-2
(config-if-range)# channel-group 10 mode on
(config-if-range)# exit
```
Adds ports 1/0/1 and 1/0/2 to channel group 10 in static mode. The port channel interface for channel group 10 is automatically generated.

2.
```
(config)# interface port-channel 10
```
Switches channel group 10 to port channel interface configuration mode.

3.
```
(config-if)# switchport mode trunk
```
Sets channel group 10 as a trunk port.

(3) Shutdown of a port channel interface

Points to note

When `shutdown` is set for a port channel interface, communication over all ports registered in the channel group stops. Ports in the link-up status stop communication, preserving the status.

Command examples

1.
```
(config)# interface range gigabitethernet 1/0/1-2
(config-if-range)# channel-group 10 mode on
(config-if-range)# exit
```

Adds ports 1/0/1 and 1/0/2 to channel group 10 in static mode.

2.
```
(config)# interface port-channel 10
(config-if)# shutdown
```

Changes the mode to port channel interface configuration mode, and sets `shutdown`. Channel group 10 is shut down, so communication over ports 1/0/1 and 1/0/2 stops.

17.2.5 Deleting a channel group

Before you remove ports from a channel group or delete an entire channel group, you must set `shutdown` in Ethernet interface configuration mode for the ports that will be removed. If you do not set `shutdown`, a communication loop might occur.

(1) Removing ports from a channel group

Points to note

The example below shows how to remove a port from a channel group. Because the removed port can operate independently of the channel group, `shutdown` is set beforehand to prevent a communication loop.

Be careful when using a removed port for another purpose because the related commands that were set for the port by using the `interface port-channel` command before the port was removed remain after the removal. (For details about the related commands, see *Table 17-5: Related commands for a port channel interface.*)

The `interface port-channel` command settings are not deleted even if all of the ports in the channel group are deleted. For details about deleting an entire channel group, see *(2) Deleting an entire channel group.*

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# shutdown
```

Sets `shutdown` for port 1/0/1 to place the port in the link-down status so that the port can be removed safely from the channel group.

2.
```
(config-if)# no channel-group
```

Deletes the channel group settings from port 1/0/1.

(2) Deleting an entire channel group

Points to note

The example below shows how to delete an entire channel group. Because the ports in the deleted channel group can operate independently, `shutdown` is set beforehand to prevent a communication loop.

An entire channel group is deleted by deleting the `interface port-channel` command. After this deletion, the `channel-group mode` command is automatically deleted from each port registered in the channel group. Be careful when using the ports for another purpose because the related commands that were set for the ports by using the `interface port-channel` command before the port group was deleted remain after the removal. (For details about the related commands, see *Table 17-5: Related commands for a port channel interface.*)

Command examples

1.
```
(config)# interface range gigabitethernet 1/0/1-2
(config-if-range)# shutdown
(config-if-range)# exit
```

Sets `shutdown` for all ports in the channel group to place these ports in the link-down status so that the entire channel group can be deleted safely.

2.
```
(config)# no interface port-channel 10
```

Deletes channel group 10. The `channel-group mode` command settings configured for ports 1/0/1 and 1/0/2 are also deleted automatically.

17.3 Description of the link aggregation extended functionality

17.3.1 Standby link functionality

(1) Description

The standby link functionality replaces a faulty port with a standby port in the same channel group to maintain the number of active ports in the channel group. This functionality can prevent a reduction of available bandwidth if a fault occurs.

This functionality is available only when static link aggregation is used.

(2) How a standby link is selected

The maximum number of active ports in a channel group is set in the configuration. The rest of the ports in the channel group are standby ports.

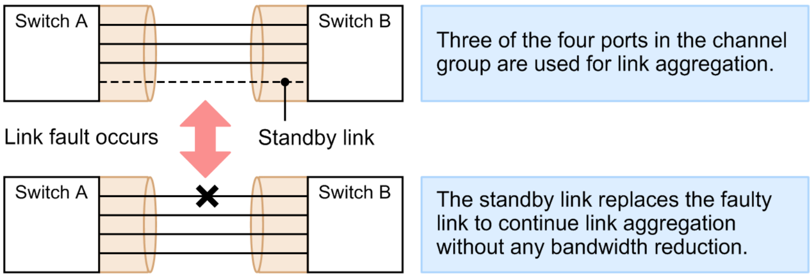
Standby ports are determined based on the port priority, switch number, and port number set in the configuration. The following table describes the selection principle.

Table 17-6: Standby port selection principle

Priority	Parameter	Remarks
High ↑	Port priority	Ports in the channel group are selected as standby ports in ascending order of port priority level (port with the lowest priority is selected first).
	Switch number	Ports in the channel group are selected as standby ports in descending order of switch number.
↓ Low	Port number	Ports in the channel group are selected as standby ports in descending order of port number (the port with the largest port number is selected first).

The figure below shows an example that explains how the standby link functionality works. In this example, four ports belong to a channel group, and the maximum number of active ports is three.

Figure 17-4: Example of standby link functionality operation



Three of the four ports in the channel group are used for link aggregation.

The standby link replaces the faulty link to continue link aggregation without any bandwidth reduction.

(3) Standby link modes

The standby link functionality has the following two modes:

- Link-down mode

  In link-down mode, the status of the standby links changes to link-down. Ports on the remote device that do not support the standby link functionality can also be used as standby ports.

- Link-not-down mode

In link-not-down mode, sending from standby links stops, but the status of the standby links does not change to link-down. Because the standby links are in the link-up status, monitoring of faults can also be performed for these standby ports. Note that in this mode, standby ports do not send data, but can receive data. A device that does not support the standby link functionality does not detect the link-down status on the partner device, and can continue sending to the partner device. In link-not-down mode, connecting to the device is possible.

In link-down mode, if there is only one active port in a channel group and a fault occurs on that port, the channel group is temporarily shut down when the faulty port is replaced with a standby port. In link-not-down mode, the standby port replaces the faulty port without the channel group shutting down.

The status in which only one port is active in a channel group arises in either of the following cases:

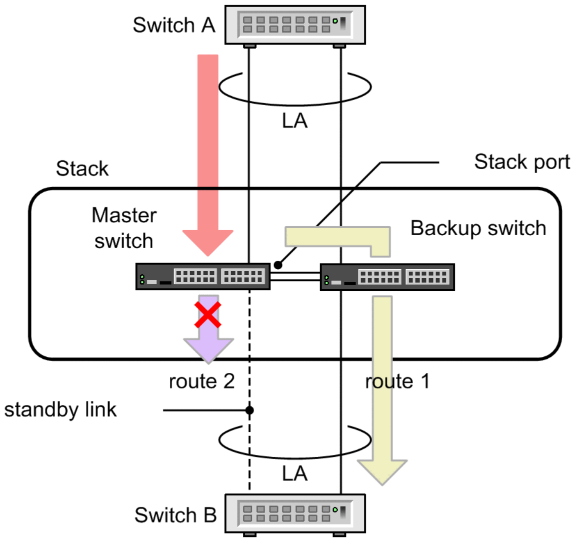
- The maximum number of active ports is set to 1 by using the `max-active-port` configuration command.
- There are multiple ports, only one of which provides the highest transmission speed, and mixed-speed mode is not set.

(4) Notes on stack configurations

Keep the following in mind when using the standby link functionality.

- When the standby link functionality is used in the link-down mode and when a port on the backup switch side is selected as the standby port, if a failure occurs in the master switch or the stack link which in turn causes the backup switch to become a new master switch, the standby port remains down. In this case, use the `activate` operation command to activate the port.
- When a stack is configured, frames are first sent to the port of the member switch that received frames. However, as shown in the following figure, if the port where frames are to be sent is selected as the standby port and thus the route 2 becomes standby link, the sending with priority functionality does not work. Because of this, if a failure occurs in the backup switch, the communication is temporarily disconnected to switch the standby link.

Figure 17-5: Standby link functionality when a stack is configured



Legend: LA: Link aggregation

17.3.2 Port detachment restriction functionality

The port detachment restriction functionality suppresses the functionality that detaches a faulty port so that link aggregation with the rest of the ports can continue if a link fault occurs. If the port detachment restriction functionality is used and a fault occurs on any port in a channel group, operation of the entire channel group stops on the assumption that a group-wide fault has occurred. If no ports in the channel group are faulty, then operation of the channel group is restarted.

If this functionality is used with redundancy functionality such as the GSRP, the connection route can be switched on a group basis even if the fault occurs on only one port in the channel group.

This functionality is available only when LACP link aggregation is used.

The port detachment restriction functionality permits the channel groups of connected devices to perform link aggregation between them if the device with the higher priority judges that all ports in both channel groups are usable for aggregation. Because this functionality never permits link aggregation when any ports are detached, the intended bandwidth is guaranteed.

The priority is determined based on the LACP system priority set in configuration mode and the MAC address of the channel group. The table below describes the principle for this determination. As described in the table, if both devices have the same LACP system priority, then the MAC address of the channel group is used as the condition for determination.

Table 17-7: Principle for determining the device that judges whether all the ports in channel groups are usable for aggregation

Priority	Parameter	Remarks
High ↑	LACP system priority	The device with the smaller LACP system priority value performs judgment.
↓ Low	MAC address of the channel group	The device with the smaller MAC address value performs judgment.

17.3.3 Mixed-speed mode

Normally, a channel group consists of ports whose transmission speed is the same. In mixed-speed mode, however, ports with different transmission speeds can be used concurrently in one channel group. This mode allows you to use a slow-speed port for a standby link or more flexibly change the configuration of a channel group. Usage examples of this mode are provided below.

Note that the port transmission speed is not applied to port allocation when frames are sent. For example, when a 1 Gbit/s port and a 10 Gbit/s port are used in mixed-speed mode, the difference of transmission speed is not applied to the allocation of frames to ports. Normally, we recommend that you use ports whose transmission speed is the same.

(1) Example of using mixed-speed mode for the standby link functionality

You can use a slower standby port for a faster port. For example, if you use a 10 Gbit/s port for communication, you can enable the standby link functionality by setting the maximum number of active ports to 1, and setting a 1 Gbit/s port as a standby port. In this case, if a fault occurs on the 10 Gbit/s port, you can continue communication by using the standby 1 Gbit/s port.

If you use the standby link functionality in mixed-speed mode, we recommend that you set the maximum number of active ports to 1. If the maximum number of active ports is 2 or more, ports with different transmission speeds might be used for normal operation. Also, if you set the maximum number of active ports to 1, we recommend that you use link-not-down mode. If you use link-down mode when the maximum number of active ports is 1, the channel group is temporarily shut down when the channel group is switched.

(2) Example of using mixed-speed mode when changing the configuration of a channel group

You can change the transmission speeds of ports in a channel group (network reconfiguration) without shutting down the channel group.

To do so, use the procedure below to change the transmission speeds of ports in a channel group by using mixed-speed mode.

1. Operate link aggregation with a channel group that consists of ports whose transmission speed is the same (two 1 Gbit/s ports).
2. Set mixed-speed mode.
3. Add two 10 Gbit/s ports to the channel group.

   If mixed-speed mode is not set, link aggregation temporarily stops with this step.
4. Place the two 10 Gbit/s ports you added in step 3 in the link-up status.
5. Place the two 1 Gbit/s ports in the link-down status.
6. Remove the two 1 Gbit/s ports from the channel group.
7. The channel group now consists of two 10 Gbit/s ports.

17.4 Configuration of the link aggregation extended functionality

17.4.1 List of configuration commands

The following table describes the configuration commands for the link aggregation extended functionality.

Table 17-8: List of configuration commands

Command name	Description
channel-group lacp system-priority	Sets the system priority for a channel group. The system priority is used to determine which device evaluates the aggregation condition for the port detachment restriction functionality.
channel-group max-active-port	Enables the standby link functionality, and sets how many ports in the channel group can be used for link aggregation.
channel-group max-detach-port	Enables the port detachment restriction functionality.
channel-group multi-speed	Sets mixed-speed mode.
lacp port-priority	Sets the port priority. The port priority is used to select standby links.
lacp system-priority	Sets the default value for the system priority. The system priority is used to determine which device evaluates the aggregation condition for the port detachment restriction functionality.

17.4.2 Configuration of the standby link functionality

Points to note

The standby link functionality is used to enable a channel group, and to set the maximum number of active ports in the channel group. In addition, either link-down mode or link-not-down mode can be set. The standby link functionality is available only when static link aggregation is used.

Standby ports are set on a port priority basis, whereby a port with a lower priority level is selected for a standby link earlier. Note that the smaller the port priority value, the higher its priority.

Command examples

1.
```
(config)# interface port-channel 10
```
Switches channel group 10 to port channel interface configuration mode.

2.
```
(config-if)# channel-group max-active-port 3
```
Enables the standby link functionality for channel group 10, and sets the maximum number of active ports in the channel group to 3. Channel group 10 operates in link-down mode.

3.
```
(config-if)# exit
```
Changes the mode to global configuration mode.

4.
```
(config)# interface port-channel 20
(config-if)# channel-group max-active-port 1 no-link-down
(config-if)# exit
```

Changes the mode to port channel interface configuration mode for channel group 20, enables the standby link functionality for the channel group, sets the maximum number of active ports to 1, and sets link-not-down mode.

5.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# channel-group 20 mode on
(config-if)# lacp port-priority 300
```

Adds port 1/0/1 to channel group 20, and sets the port priority value to 300. Note that a smaller port priority value indicates a higher priority. Therefore, a port with the port priority value of 300, which is larger than the default value of 128, is selected for a standby link earlier than a port with the default priority.

17.4.3 Configuration of the port detachment restriction functionality

Points to note

The port detachment restriction functionality is used to enable a channel group. For the command that enables this functionality, set either 0 or 7 as the maximum number of ports that can be detached. Specifying 7 is equivalent to disabling the functionality.

If a switch is to be connected to a device that supports the port detachment restriction functionality, make sure that the settings of the functionality on both devices match. If a switch is to be connected to a device that does not support this functionality, set a higher LACP system priority level on the Switch. A smaller LACP system priority value indicates a higher priority.

The port detachment restriction functionality is available only when LACP link aggregation is used.

Command examples

1.
```
(config)# interface port-channel 10
```

Switches channel group 10 to port channel interface configuration mode.

2.
```
(config-if)# channel-group max-detach-port 0
```

Enables the port detachment restriction functionality for channel group 10, and set the maximum number of ports that can be detached from the channel group to 0. If at least one port in the channel group becomes faulty, the entire channel group is assumed to be faulty.

3.
```
(config-if)# channel-group lacp system-priority 100
```

Sets 100 as the system priority for channel group 10.

17.4.4 Configuration of mixed-speed mode

Points to note

The example below shows how to set mixed-speed mode for a channel group. In mixed-speed mode, the transmission speed of ports is excluded from detachment conditions.

Command examples

1.
```
(config)# interface port-channel 10
```

Switches channel group 10 to port channel interface configuration mode.

2. `(config-if)# channel-group multi-speed`

   Sets mixed-speed mode for channel group 10.

17.5 Operation for link aggregation

17.5.1 List of operation commands

The following table describes the operation commands for link aggregation.

Table 17-9: List of operation commands

Command name	Description
show channel-group	Shows link aggregation information.
show channel-group statistics	Shows link aggregation statistics.
clear channel-group statistics lacp	Clears the statistics for sent and received LACPDUs.
restart link-aggregation	Restarts the link aggregation program.
dump protocols link-aggregation	Exports the detailed event trace information and control table information for link aggregation to a file.

17.5.2 Checking link aggregation information

(1) Checking the connection status for link aggregation

When the `show channel-group` command is executed, information about link aggregation for a channel group is displayed. In the command execution result, `CH Status` indicates the connection status of the channel group. You can use the execution result to check whether the settings are correct.

The following figure shows an example of executing the `show channel-group` command.

Figure 17-6: Results of executing the show channel-group command

```
> show channel-group 1
Date 20XX/12/10 13:13:38 UTC
channel-group Counts:1
ChGr:1    Mode:LACP
  CH Status    :Up        Elapsed Time:10:10:39
  Multi Speed  :Off       Load Balance:src-dst-port
  Max Active Port:8
  Max Detach Port:7
  MAC address: 0012.e2ac.8301     VLAN ID:10
  Periodic Timer:Short
  Actor   information: System Priority:1     MAC: 0012.e212.ff02
                       KEY:1
  Partner information: System Priority:10000 MAC: 0012.e2f0.69be
                       KEY:10
  Port(4)        :1/0/5-8
  Up Port(2)     :1/0/5-6
  Down Port(2)   :1/0/7-8
>
```

(2) Checking the operating status of each port

When the `show channel-group detail` command is executed, detailed status information of each port is displayed. In the command execution result, `Status` indicates the communication status of a port. For a port whose `Status` is `Down`, the reason is also indicated.

The following figure shows an example of executing the `show channel-group detail` command.

Figure 17-7: Results of executing the show channel-group detail command

```
> show channel-group detail
Date 20XX/12/10 13:13:38 UTC
channel-group Counts:1
ChGr:1    Mode:LACP
```

```
  CH Status    :Up        Elapsed Time:00:13:51
  Multi Speed  :Off       Load Balance:src-dst-port
  Max Active Port:8
  Max Detach Port:7
  MAC address: 0012.e205.0545     VLAN ID:10
  Periodic Timer:Long
  Actor   information: System Priority:128   MAC: 0012.e205.0540
                       KEY:1
  Partner information: System Priority:128   MAC: 0012.e2c4.2b5b
                       KEY:1
  Port Counts:4        Up Port Counts:2
  Port:1/0/5   Status:Up    Reason:-
               Speed :100M  Duplex:Full  LACP Activity:Active
               Actor   Priority:128     Partner Priority:128
  Port:1/0/6   Status:Up    Reason:-
               Speed :100M  Duplex:Full  LACP Activity:Active
               Actor   Priority:128     Partner Priority:128
  Port:1/0/7   Status:Down  Reason:Duplex Half
               Speed :100M  Duplex:Half  LACP Activity:Active
               Actor   Priority:128     Partner Priority:0
  Port:1/0/8   Status:Down  Reason:Port Down
               Speed :-     Duplex:-     LACP Activity:Active
               Actor   Priority:128     Partner Priority:0
>
```

Chapter

18. Layer 2 Switching Overview

This chapter provides an overview of the Layer 2 switch functionality used to forward data over Layer 2 of the OSI model for the Switch.

18.1 Overview

18.1.1 MAC address learning

When a Layer 2 switch receives a frame, it registers the source MAC address in a MAC address table. Each entry in the MAC address table contains the MAC address and port on which the frame was received, as well as an aging timer. Each time a frame is received, the entry corresponding to the source MAC address is updated.

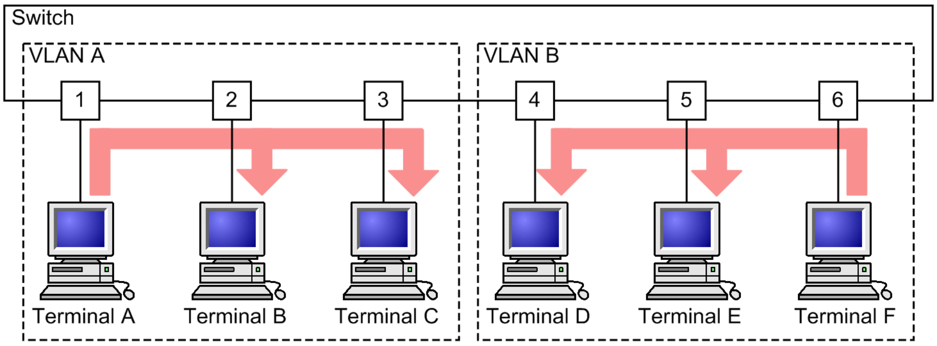
Layer 2 switches forward frames according to the entries in the MAC address table. When an entry matches the destination MAC address, the frame is forwarded to the port in the entry only if the port in the entry matches the port on which the frame was received. If no entries match, the frame is forwarded to all ports other than the one on which the frame was received. This kind of forwarding is called flooding.

18.1.2 VLAN

VLAN functionality divides a switch into virtual groups. A switch can be internally grouped into multiple VLANs to partition broadcast domains. This allows enhanced broadcast frame control and security.

The figure below provides a VLAN overview. Because the broadcast domain is divided between VLAN A and VLAN B, no frames will arrive.

Figure 18-1: VLAN overview



Because VLAN A and VLAN B have been split, broadcast packets from terminals on VLAN A are forwarded to terminals B and C, but not to terminals D, E, and F on VLAN B.

18.2 Supported functionality

The table below describes the Layer 2 switch functionality supported by the Switch.

Some types of functionality can be combined, but others cannot. The limitations regarding functionality combinations are shown below.

Table 18-1: Supported Layer 2 switch functionality

Supported functionality		Overview
MAC address learning		The learning of MAC addresses registered in the MAC address table
VLAN	Port VLAN	The division of switches into virtual internal groups by port
	Protocol VLAN	The division of switches into virtual internal groups by protocol
	MAC VLAN	The division of switches into virtual internal groups by source MAC address
	Default VLAN	The VLAN to which ports belong by default when the configuration is not set
	Native VLAN	Another name for the port VLAN that handles untagged frames on trunk ports, protocol ports, and MAC ports
	Tunneling	The aggregation, and tunneling, of the VLANs of multiple users on another VLAN
	Tag translation	The conversion of VLAN tags for forwarding to another VLAN
	L2 protocol frame transparency functionality	The forwarding of frames with the Layer 2 protocol. Spanning Tree Protocols (BPDUs) and IEEE 802.1X (EAP) are forwarded.
	Per-VLAN MAC addresses	The mapping of Layer 3 interface MAC addresses to different addresses at the VLAN level
Spanning Tree Protocols	PVST+	The prevention of looping between switches at the VLAN level
	Single Spanning Tree	The prevention of looping between switches at the terminal level
	Multiple Spanning Tree	The prevention of looping between switches at the MST instance level
Ring Protocol		The use of the ring topology to provide redundancy for Layer 2 networks
IGMP snooping or MLD snooping		The control of multicast traffic within a VLAN on a Layer 2 switch
Inter-port relay blocking functionality		The blocking of all communication between specified ports

18.3 Compatibility between Layer 2 switch functionality and other functionality

When the Layer 2 switch functionality is used, other functionality might be restricted or disabled. The following table describes the restrictions regarding combinations of functionality.

Note that only functionality with compatibility restrictions is shown in the table.

Table 18-2: Restrictions on VLANs

Functionality used		Functionality	Available
VLAN type	Port VLAN	VLAN tunneling	Partial#1
		Layer 2 authentication	Partial#2
		Port mirroring (mirrored ports)	No
	Protocol VLAN	Default VLAN	No
		VLAN tunneling	
		PVST+	
		Layer 2 authentication	Partial#2
		Port mirroring (mirrored ports)	No
	MAC VLAN	Default VLAN	No
		VLAN tunneling	
		PVST+	
		Layer 2 authentication	Partial#2
		Port mirroring (mirrored ports)	No
Default VLAN		Protocol VLAN	No
		MAC VLANs	
		IGMP snooping	
		MLD snooping	
		Layer 2 authentication	Partial#2
		Port mirroring (mirrored ports)	No
VLAN extended functionality	Tag translation	PVST+	No
		IGMP snooping	
		MLD snooping	
		Uplink redundancy	Partial#3
	VLAN tunneling	Port VLAN	Partial#1
		Protocol VLAN	No
		MAC VLAN	
		PVST+	

Functionality used		Functionality	Available
		Single Spanning Tree	
		Multiple Spanning Tree	
		IGMP snooping	
		MLD snooping	
		Layer 2 authentication	Partial[#2]
		DHCP snooping	No
		Uplink redundancy	Partial[#3]
	L2 protocol frame transparency functionality (BPDU)	PVST+	No
		Single Spanning Tree	
		MSTP	
	L2 protocol frame transparency functionality (EAP)	Layer 2 authentication	Partial[#2]
	Inter-port relay blocking functionality	DHCP snooping	Partial[#4]

#1

When using the VLAN tunneling functionality, do not use a native VLAN on a trunk port.

#2

For details, see *5.2.1 Using Layer 2 authentication with other functionality* in the manual *Configuration Guide Vol. 2 For Version 11.10*.

#3

Cannot be used on an uplink port.

#4

When DHCP snooping is enabled, even if the inter-port relay blocking functionality is set up, none of the DHCP packets received by the Switch will be subject to blocking. Also, when dynamic ARP testing is enabled, none of the ARP packets received by the Switch will be subject to blocking.

Table 18-3: Restrictions on Spanning Tree Protocols

Functionality used	Functionality	Available
PVST+	Protocol VLAN	No
	MAC VLAN	
	VLAN tunneling	
	Tag translation	
	L2 protocol frame transparency functionality (BPDU)	
	Multiple Spanning Tree	

Functionality used	Functionality	Available
	GSRP	
	Layer 2 authentication	Partial[#]
	Uplink redundancy	No
Single Spanning Tree	VLAN tunneling	No
	L2 protocol frame transparency functionality (BPDU)	
	Multiple Spanning Tree	
	GSRP	
	Layer 2 authentication	Partial[#]
	Uplink redundancy	No
Multiple Spanning Tree	VLAN tunneling	No
	L2 protocol frame transparency functionality (BPDU)	
	Single Spanning Tree	
	PVST+	
	Loop guard	
	GSRP	
	Layer 2 authentication	Partial[#]
	Uplink redundancy	No

#

For details, see *5.2.1 Using Layer 2 authentication with other functionality* in the manual *Configuration Guide Vol. 2 For Version 11.10.*

Table 18-4: Restrictions on the Ring Protocol

Functionality used	Functionality	Available
Ring Protocol	Layer 2 authentication	Partial[#1]
	Uplink redundancy	Partial[#2]

#1

For details, see *5.2.1 Using Layer 2 authentication with other functionality* in the manual *Configuration Guide Vol. 2 For Version 11.10.*

#2

Cannot be used with a ring port.

Table 18-5: Restrictions on IGMP or MLD snooping

Functionality used	Functionality	Available
IGMP snooping	Default VLAN	No
	Tag translation	

Functionality used	Functionality	Available
	VLAN tunneling	
	Layer 2 authentication	Partial#
MLD snooping	Default VLAN	No
	Tag translation	
	VLAN tunneling	

#

For details, see *5.2.1 Using Layer 2 authentication with other functionality* in the manual *Configuration Guide Vol. 2 For Version 11.10*.

Chapter
19. MAC Address Learning

This chapter describes the MAC address learning functionality and its use.

19.1 Description of MAC address learning

The Switch performs Layer 2 switching, in which frames are forwarded to specific ports based on destination MAC address. Forwarding frames to specific ports according to their destination MAC address can prevent unnecessary traffic caused by unicast frame flooding.

MAC address learning treats a channel group as a single port.

19.1.1 Source MAC address learning

All received frames are subject to MAC address learning, in which the source MAC address is learned and registered in the MAC address table. Registered MAC addresses are kept until an aging timeout occurs. Learning is performed per VLAN, and the MAC address table is managed using pairs of MAC addresses and VLANs. The same MAC address can also be learned for different VLANs.

19.1.2 Detecting a move for MAC address learning

When a frame with a learned source MAC address is received from a port other than that from when it was learned, the MAC address is considered to have moved, and the entry is re-registered in the MAC address table as an overwrite with the port to which it moved.

A MAC address learned for a channel group is considered to have moved when a frame is received from a port that the channel group does not contain.

19.1.3 Aging and MAC address learning

A learned entry is deleted when no frames are received from the source MAC address within the given aging time. This prevents entries from unnecessarily accumulating. When a frame is received within the aging time the aging timer is updated and the entry is kept. The range within which the aging time can be set is as follows:

- Aging time range: 0 or 10 to 1000000 (seconds)

  0 indicates eternity, with no aging performed.
- Default value: 300 (seconds)

At a maximum, twice the maximum aging time might be necessary for a learned entry to be deleted.

Note that if a port goes down, all entries learned for the port are deleted. Entries learned for channel groups are deleted when their channel group goes down.

19.1.4 Layer 2 switching by MAC address

Layer 2 switching is performed based on the results of MAC address learning. If an entry corresponding to the destination MAC address has been kept, forwarding is performed only to the learned port.

The following table explains the specification by which Layer 2 switching operates.

Table 19-1: Specification for Layer 2 switching operation

Type of destination MAC address	Operational overview
Learned unicast	Forwarding is performed to the learned port.
Unlearned unicast	Forwarding is performed to all ports belonging to the received VLAN.
Broadcast	Forwarding is performed to all ports belonging to the received VLAN.

Type of destination MAC address	Operational overview
Multicast	Forwarding is performed to all ports belonging to the received VLAN. However, for IGMP snooping or MLD snooping, forwarding is performed according to the learning results of the snooping functionality.

19.1.5 Limiting MAC address learning [AX3650S]

You can manage entries in the MAC address table you are using by limiting dynamic learning by incoming frames.

You can limit the number of MAC addresses to be learned for each VLAN. Once the MAC addresses learning count reaches the maximum number, a log message is output and dynamic MAC address learning is disabled. Incoming frames with source MAC addresses left unlearned due to restriction on the MAC addresses learning count will be discarded without forwarding.

By limiting the MAC addresses learning count, you can limit the number of PCs connected to a VLAN.

Already learned MAC address table entries remain after reaching the maximum MAC addresses learning count and disabling MAC address learning unless they are aged out or deleted by using an operation command.

Once the number of MAC address table entries become smaller than the maximum number, MAC address learning is enabled again.

Note that, when using the MAC address learning restriction functionality, the maximum number of entries that can be used in the Switch is decreased by one.

19.1.6 Registering static entries

In addition to dynamic learning by received frame, MAC addresses can be registered statically by user specification. One port or channel group can be specified for a unicast MAC address. Also, frames can be specified for discarding, instead of specified for a port, in which case frames for the specified destination MAC address or source MAC address are discarded without being forwarded to any port.

When a unicast MAC address is statically registered, dynamic learning is not performed for the address. Already learned entries are deleted from the MAC address table and registered as static entries. Also, any frames whose source is the specified MAC address are discarded when received from outside the port or channel group. The following table describes the parameters specified for static entries.

Table 19-2: Parameters specified for static entries

No.	Specified parameter	Description
1	MAC address	Specifies a unicast MAC address.
2	VLAN	Specifies the VLAN for registering this entry.
3	Transmission destination port/discarding specification	Specifies one port or channel group. Alternatively, frames corresponding to 1 or 2 above can be specified for discarding.

19.1.7 Clearing the MAC address table

The Switch clears the MAC address table through operation commands and protocol usage. The following table describes when the MAC address table is cleared.

Table 19-3: When the MAC address table is cleared

Trigger	Description
Port down#1	Learned entries are deleted from the corresponding port.
Channel group down#2	Learned entries are deleted from the corresponding channel group.
Execution of the clear mac-address-table operation command	The MAC address table is cleared according to the parameters.
Clear MIB set for the MAC address table (private MIB)	The MAC address table is cleared at setup.
Spanning Tree topology changed	When Spanning Tree Protocols are configured on the Switch: The MAC address table is cleared when a topology change is detected.
	When the Switch runs as a ring node in a network configuration using a Spanning Tree Protocol and Ring Protocol: The MAC address table is cleared when a flush control frame sent during a topology change for a switch using the Ring Protocol is received.
GSRP master/backup switched	When the Switch runs as a GSRP switch: The MAC address table is cleared when the switch becomes the backup.
	When the Switch runs GSRP-aware: The MAC address table is cleared when the GSRP Flush request frame sent when the GSRP switch becomes the master is received.
	When the Switch uses both GSRP and the Ring Protocol: The MAC address table is cleared when the switch becomes the master.
	When the Switch runs as a ring node in a network configuration using both GSRP and the Ring Protocol: The MAC address table is cleared when the flush control frame sent when a switch using the Ring Protocol becomes the master is received.
Route switched by the Ring Protocol	When the Switch runs as the master node: The MAC address table is cleared when path switching is performed.
	When the Switch runs as a transit node: The MAC address table is cleared when the flush control frame sent from the master node when path switching is performed is received. The MAC address table is cleared when the maintenance time for waiting for the flush control frame times out.
	When the multi-fault monitoring functionality is enabled, if receiving flush control frames sent from a shared node when switching to or switching back from a backup ring, the MAC address table is cleared.
	The MAC address table is cleared when the neighboring-ring flush control frame sent from the master node when path switching is performed is received.
VRRP virtual router master/ backup switched	The MAC address table is cleared when the Flush Request frame sent when the VRRP virtual router becomes the master is received.
Primary port and secondary port switched due to uplink/ redundancy functionality	The MAC address table is cleared when the flush control frame sent on switching from the primary port to the secondary port or on switching back from the secondary port to the primary port is received.

#1

Downed ports such as those that are down due to a line failure, execution of the `inactivate` operation command, or the settings in the `shutdown` configuration command.

#2

Downed channel groups such as those that are down due to the LACP, a line failure, or the settings in the `shutdown` configuration command.

19.1.8 Notes

(1) MAC address learning and ARP or NDP

Because the Switch requires that NextHop MAC addresses resolved using ARP or NDP in Layer 3 forwarding be registered in the MAC address table, keep the following in mind:

- When MAC address learning information is cleared by a command or aging, any ARP or NDP information for the MAC addresses is also cleared. Cleared ARP and NDP entries can be re-resolved by communication if necessary.
- When the aging time for MAC address learning is shorter than the ARP or NDP aging time, the corresponding ARP and NDP entries are cleared by the aging for MAC address learning. This situation can be avoided by setting the aging time for MAC address learning so that it is longer than or equal to the ARP or NDP aging time.

(2) Using Layer 3 forwarding with MAC address learning restriction [AX3650S]

To restrict MAC address learning on a VLAN that performs Layer 3 forwarding, make sure to use the hardware discard functionality for packets with unlearned addresses.

19.2 MAC address learning configuration

19.2.1 List of configuration commands

The following table describes the configuration commands for MAC address learning.

Table 19-4: List of configuration commands

Command name	Description
mac-address-table aging-time	Sets the aging time for MAC address learning.
mac-address-table limit	Sets the maximum for dynamic MAC address learning.
mac-address-table static	Sets a static entry.

19.2.2 Configuring the aging time

Points to note

The aging time for MAC address learning can be changed. The setting is configured for each switch. If no value is set, 300 seconds is used as the aging time.

Command examples

1. `(config)# mac-address-table aging-time 100`

   Sets the aging time to 100 seconds.

19.2.3 Configuring static entries

Because address learning is not performed for a specified MAC address, static entries can be registered to avoid flooding due to MAC address aging. When static entries are set, frames are always forwarded according to the registered entries. This functionality is useful for high-traffic terminals whose ports do not move, such as servers connected directly to the Switch.

A MAC address, VLAN, and output destination are specified for a static entry. The output destination can be specified as a port or channel group, or for discarding.

(1) Static entries specifying a port as the output destination

Points to note

The example below shows how to specify a port as the output destination.

Command examples

1.
```
(config)# mac-address-table static 0012.e200.1122 vlan 10
interface gigabitethernet 1/0/1
```

   Sets the destination for frames for the destination MAC address 0012.e200.1122 to port 1/0/1 on VLAN 10.

Notes

On VLAN 10, any frames from source MAC address 0012.e200.1122 received by a means other than port 1/0/1 are discarded.

(2) Static entries specifying a link aggregation as the output destination

Points to note

The example below shows how to specify a link aggregation as the output destination.

Command examples

1. `(config)# mac-address-table static 0012.e200.1122 vlan 10 interface port-channel 5`

   Sets the output destination for frames for the destination MAC address 0012.e200.1122 to channel group 5 on VLAN 10.

Notes

On VLAN 10, any frames from source MAC address 0012.e200.1122 received by a means other than channel group 5 are discarded.

(3) Static entries for which discarding is specified

Points to note

The example below shows how to specify a MAC address so that the frames sent to or from the MAC address are to be discarded.

Command examples

1. `(config)# mac-address-table static 0012.e200.1122 vlan 10 drop`

   For VLAN 10, sets the MAC address 0012.e200.1122 so that the frames sent to or from the MAC address are to be discarded.

19.2.4 Configuring the number of MAC address learning [AX3650S]

Points to note

Sets the maximum number of MAC addresses for each VLAN.

Command examples

1. **`(config)# mac-address-table limit vlan 200 maximum 2500`**

   Sets the maximum number of MAC addresses to 2500.

19.3 MAC address learning operation

19.3.1 List of operation commands

The following table describes the operation commands for MAC address learning.

Table 19-5: List of operation commands

Command name	Description
show mac-address-table	Shows information about the MAC address table. When the learning-counter parameter is specified, the learning address count for MAC address learning is displayed for each port.
clear mac-address-table	Clears the MAC address table.

19.3.2 Checking the status of MAC address learning

The show mac-address-table command displays information about MAC address learning. Use it to check the MAC addresses registered in the MAC address table, as well as to check the forwarding destination for frames with the MAC address used as the destination. Any frames with a destination other than the MAC addresses displayed by this command are flooded to the entire VLAN.

The show mac-address-table command displays the entries registered by MAC address learning, static entries, and IEEE 802.1X, and entries registered by IGMP snooping and MLD snooping.

Figure 19-1: Results of executing the show mac-address-table command

```
> show mac-address-table
Date 20XX/10/14 12:08:41 UTC
MAC address         VLAN    Type     Port-list
0012.e22d.eefa         1    Dynamic  1/0/2
0012.e212.2e5f         1    Dynamic  1/0/5
0012.e205.0641      4094    Dynamic  1/0/24
0012.e28e.0602      4094    Dynamic  1/0/24
>
```

19.3.3 Checking the MAC address learning count

The show mac-address-table command (with the learning-counter parameter specified) can be used to display the number of dynamic entries registered by MAC address learning for each port, and to check the number of terminals connected per port.

When link aggregation is used, the same value is displayed for all ports in the same channel group. The displayed value is the number of learned addresses in the channel group.

Figure 19-2: Results of executing the show mac-address-table command (with the learning-counter parameter specified)

```
> show mac-address-table learning-counter port 1/0/1-12
Date 20XX/10/14 12:09:40 UTC
Port counts:12
Port         Count
1/0/1            0
1/0/2            1
1/0/3            0
1/0/4            0
1/0/5            1
1/0/6            0
1/0/7            0
1/0/8           20
1/0/9            0
1/0/10           0
```

```
1/0/11           0
1/0/12           0
>
```

By executing the `show mac-address-table` command with `learning-counter` and `vlan` parameters specified, the number of dynamic entries is displayed for each VLAN.

Figure 19-3: Results of executing the show mac-address-table command (with the learning-counter parameter and the vlan parameter specified)

```
> show mac-address-table learning-counter vlan
Date 20XX/09/24 20:00:57 UTC
VLAN counts:4
ID         Count  Maximum
   1           3        -
 100        1000     1000
 200           0        -
4094          90      100
```

Chapter

20. VLANs

VLAN functionality divides a switch internally into virtual groups. This chapter describes VLANs and their use.

20.1 Description of the basic VLAN functionality

This section provides an overview of VLANs.

20.1.1 VLAN type

The following table describes the types of VLAN supported by the Switch.

Table 20-1: Supported VLAN types

Item	Overview
Port VLAN	Divides a VLAN group by port.
Protocol VLAN	Divides a VLAN group by protocol.
MAC VLAN	Divides a VLAN group by source MAC address.

20.1.2 Port type

(1) Description

The VLANs that can be used by the Switch differ depending on the port settings. The type of each port needs to be set according to the type of VLAN to be used. The following table describes the types of ports.

Table 20-2: Port type

Port type	Overview	VLANs used
Access port	Handles an untagged frame as a port VLAN. With this port, all untagged frames are handled as a single port VLAN.	Port VLAN MAC VLAN
Protocol port	Handles an untagged frame as a protocol VLAN. With this port, the VLAN is determined by the frame protocol.	Protocol VLAN Port VLAN
MAC port	Handles an untagged frame as a MAC VLAN. With this port, the VLAN is determined by the source MAC address in the frame.	MAC VLAN Port VLAN
Trunk port	Handles all VLAN types as tagged frames. With this port, the VLAN is determined by the VLAN tag.	VLANs of all types
Tunneling port	Handles everything as a port VLAN for VLAN tunneling, regardless of whether the frame is tagged. With this port, all frames are handled as a single port VLAN.	Port VLAN

Access ports, protocol ports, and MAC ports handle untagged frames, but cannot handle tagged frames. Any received tagged frames are discarded, and cannot be sent.

It is possible to have tagged frames handled by only trunk ports. Untagged frames for a trunk port are handled by native VLANs.

A tunneling port is a port that performs VLAN tunneling, regardless of whether frames are tagged.

The table below describes the types of VLANs that can be used for each port type. A protocol VLAN and a MAC VLAN cannot use the same port. Trunk ports that handle all VLAN tags can use the same port on all VLANs.

Table 20-3: VLAN availability by port

Port type	VLAN type		
	Port VLAN	Protocol VLAN	MAC VLAN
Access port	Y	N	Y
Protocol port	Y	Y	N
MAC port	Y	N	Y
Trunk port	Y	Y	Y
Tunneling port	Y	N	N

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

(2) Native VLAN for ports

Ports other than access ports or tunneling ports (protocol ports, MAC ports, and trunk ports) might receive frames for which the respective settings do not match, such as when an IPv6 frame is received after the protocol port was set for only the IPv4 protocol. A single port VLAN can be set up to handle this kind of frame on any port other than an access port or tunneling port. This VLAN is called the native VLAN on each port.

On each port other than access ports and tunneling ports, the port VLAN already created for each port can be set in the native VLAN. VLAN 1 (the default VLAN) is used as the native VLAN for ports that cannot be specified by configuration.

20.1.3 Default VLAN

(1) Overview

The Switch allows Layer 2 forwarding immediately after startup, even when the configuration has not been set up yet. In this case, all ports are access ports belonging to VLAN ID 1, which is known as the default VLAN. The default VLAN always exists, and its VLAN ID of 1 cannot be changed.

(2) Removing ports from the default VLAN

Access ports belong to VLAN 1 (the default VLAN) when their configuration has not been set up. However, depending on the configuration, they might be excluded from automatic ownership by the default VLAN. The following ports do not automatically belong to the default VLAN:

- Ports for which anything other than VLAN 1 is specified for the access port
- All ports, when VLAN tunneling is configured
- Mirror ports

Ports other than access ports (protocol ports, MAC ports, trunk ports, and tunneling ports) cannot be automatically assigned to a VLAN.

20.1.4 VLAN priority

(1) VLAN judgment priority when frames are received

When a frame is received, its VLAN is determined. The following table describes the priority for determining the VLAN.

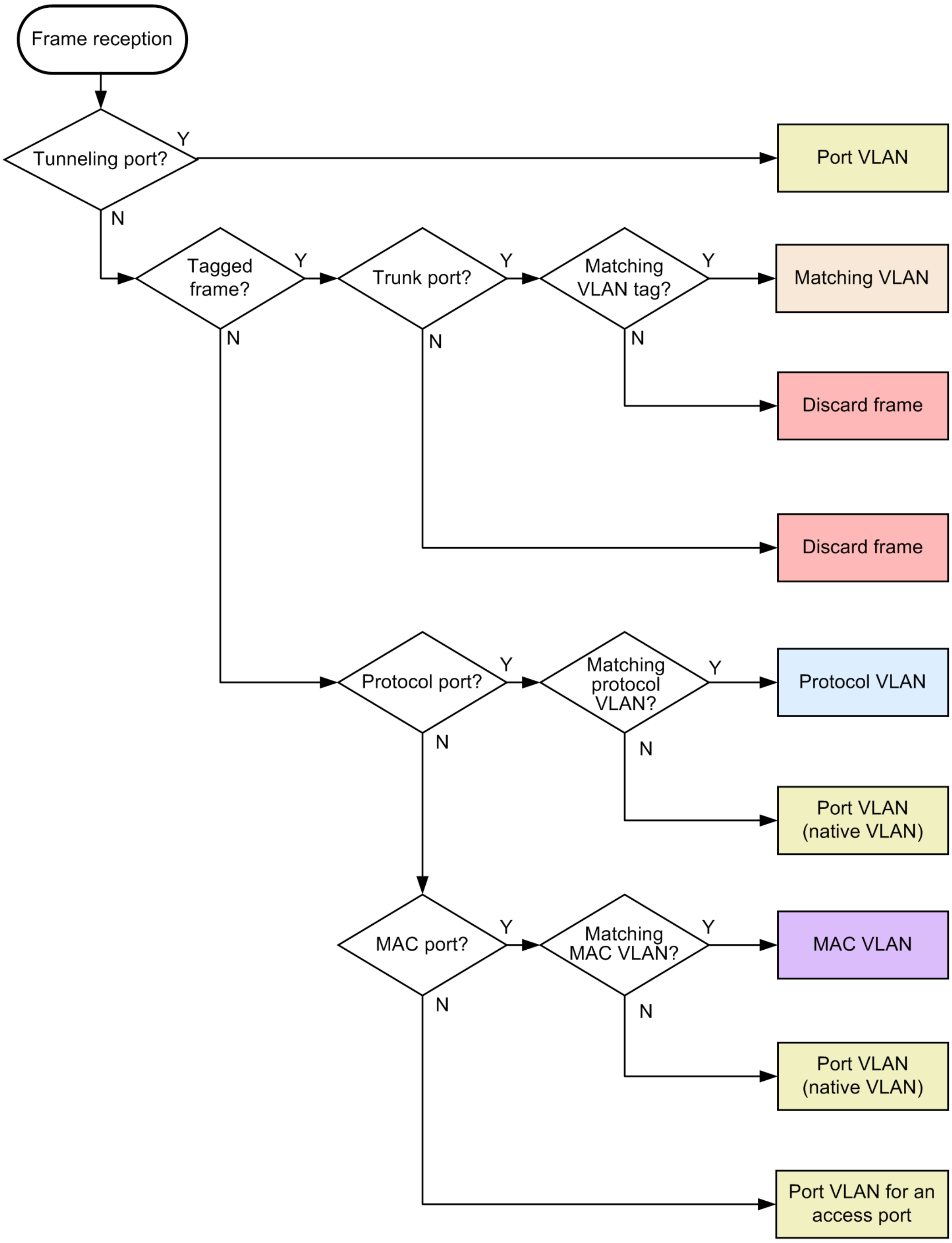
Table 20-4: Priority for determining the VLAN

Port type	Priority
Access port	Port VLAN
Protocol port	Protocol VLAN > port VLAN (native VLAN)

Port type	Priority
MAC port	MAC VLAN > port VLAN (native VLAN)
Trunk port	VLAN tag > port VLAN (native VLAN)
Tunneling port	Port VLAN

The following figure shows the algorithm for determining the VLAN.

Figure 20-1: Algorithm for determining the VLAN



20.1.5 VLAN tags

(1) Overview

VLAN tagging based on the IEEE 802.1Q standard, in which IDs called tags are inserted into Ethernet frames, can be used to configure multiple VLANs on one port.

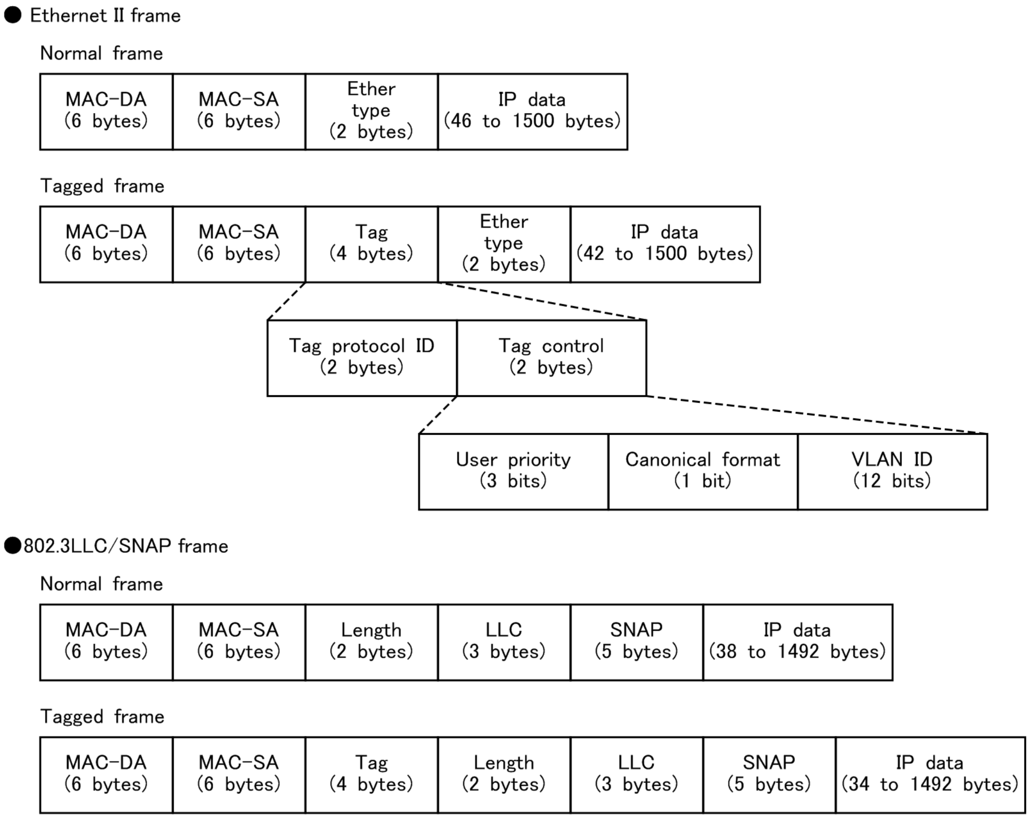
VLAN tags use the trunk port. In addition to the opposing switch, trunk ports must also recognize VLAN tags.

(2) Protocol specification

VLAN tags can embed an ID called a tag into an Ethernet frame. These tags are used to report VLAN information (a VLAN ID) to separate segments.

The figure below shows the tagged-frame format. There are two formats for Ethernet frames into which VLAN tag are inserted: Ethernet V2 and 802.3.

Figure 20-2: Tagged-frame format



The following table describes the fields for VLAN tags.

Table 20-5: VLAN tag fields

Field	Description	Conditions for the Switch
TPID (Tag Protocol ID)	An Ether Type value indicating that the IEEE 802.1Q VLAN tag continues	Any value can be set for a port.
User Priority	Indicates the IEEE 802.1D priority.	Eight priority levels can be selected for configuration.
CF (Canonical Format)	Indicates whether the MAC address in the MAC header follows a standard format.	The Switch supports only standard (0) formats.

Field	Description	Conditions for the Switch
VLAN ID	Indicates the VLAN ID#.	VLAN IDs from 1 to 4094 can be used.

#: When tag translation is used, the VLAN ID set for tag translation is used. For details, see *21.3 Description of tag translation*. When VLAN ID=0 is received, it is handled the same way as an untagged frame. VLAN ID=0 cannot be sent.

The Switch uses the same user priority for frames forwarded by Layer 2 that are used for received frames. If a received frame is untagged, the user priority is the default value of 3. Also, the user priority for sent frames can be changed by configuration. For details about changing the user priority and the user priority of frames forwarded by the Switch for Layer 3, see *3.7 Description of marking* in the manual *Configuration Guide Vol. 2 For Version 11.10*.

20.1.6 Notes on VLAN usage

(1) Notes on use with other functionality

For details, see *18.3 Compatibility between Layer 2 switch functionality and other functionality*.

20.2 Configuration of the basic VLAN functionality

20.2.1 List of configuration commands

The following table describes the configuration commands for the basic VLAN functionality.

Table 20-6: List of configuration commands

Command name	Description
name	Sets a VLAN name.
state	Sets the VLAN status (started/stopped).
switchport access	Sets the access port VLAN.
switchport dot1q ethertype	Sets the VLAN tag TPID for port.
switchport mode	Sets the port type (access, protocol, MAC, trunk, or tunneling).
switchport trunk	Sets the VLAN for a trunk port.
vlan	Creates a VLAN. Also, sets items pertaining to a VLAN in VLAN configuration mode.
vlan-dot1q-ethertype	Sets the default value for VLAN tag TPIDs.
vlan-up-massage	The `no vlan-up-message` command is used to prevent operation log messages and LinkUp/LinkDown traps from being issued when VLAN is Up or Down.

20.2.2 Configuring VLANs

Points to note

The example below shows how to create a VLAN. To create a new VLAN, specify the VLAN ID and VLAN type. If the VLAN type is omitted, a port VLAN is created. A VLAN ID list can also be used to perform batch setup of multiple VLANs.

The `vlan` command is used to switch to VLAN configuration mode. If a created VLAN is specified, only the mode is switched. The VLAN configuration mode allows VLAN parameters to be set.

Note that the following explains common settings that do not depend on the VLAN type. For details about port VLANs, protocol VLANs, and MAC VLANs, see the subsequent chapters.

Command examples

1.
```
(config)# vlan 10
```
Creates a port VLAN with VLAN ID 10, and switches to the VLAN configuration mode for VLAN 10.

2.
```
(config-vlan)# name "PORT BASED VLAN 10"
(config-vlan)# exit
```
Sets the name of the created port VLAN 10 to `PORT BASED VLAN 10`.

3.
```
(config)# vlan 100-200
```
Creates port VLANs in batch mode by using VLAN IDs 100 to 200. The command then switches to VLAN configuration mode for VLANs 100 to 200.

4. `(config-vlan)# state suspend`

   Stops in batch mode the port VLANs created with VLAN IDs 100 to 200.

20.2.3 Configuring ports

Points to note

The example below shows how to use the Ethernet interface configuration mode and port channel interface configuration mode to set the port type. Set the VLAN type according to the type of VLAN to be used.

For details about configuring port VLANs, protocol VLANs, and MAC VLANs, see the subsequent sections.

Command examples

1. `(config)# interface gigabitethernet 1/0/1`

   Switches to the Ethernet interface configuration mode for port 1/0/1.

2.
   ```
   (config-if)# switchport mode access
   (config-if)# exit
   ```

   Sets port 1/0/1 as an access port. Port 1/0/1 handles untagged frames for the port VLAN.

3. `(config)# interface port-channel 10`

   Switches channel group 10 to port channel interface configuration mode.

4. `(config-if)# switchport mode trunk`

   Sets channel group 10 as a trunk port. Port channel 10 handles tagged frame.

20.2.4 Configuring trunk ports

Points to note

The trunk port handles tagged frames, and can be used for all VLANs regardless of VLAN type, as well as with Ethernet interfaces and port channel interfaces.

The trunk port does not belong to any VLAN because it is set only with the `switchport mode` command. The VLANs handled by this port are set using the `switchport trunk allowed vlan` command.

To add VLANs, the `switchport trunk allowed vlan add` command is used. To remove VLANs, the `switchport trunk allowed vlan remove` command is used. If the `switchport trunk allowed vlan` command is executed again after having already been used to configure settings, it is replaced in the list of specified VLAN IDs.

Command examples

1.
   ```
   (config)# vlan 10-20,100,200-300
   (config-vlan)# exit
   (config)# interface gigabitethernet 1/0/1
   ```

```
(config-if)# switchport mode trunk
```

Creates VLANs 10 to 20, 100, and 200 to 300. This sequence of commands also switches to the Ethernet interface configuration mode for port 1/0/1, and sets it as a trunk port. At this point, port 1/0/1 does not belong to any VLAN.

2. `(config-if)# switchport trunk allowed vlan 10-20`

   Sets VLANs 10 to 20 for port 1/0/1. Port 1/0/1 handles tagged frames for VLANs 10 to 20.

3. `(config-if)# switchport trunk allowed vlan add 100`

   Adds VLAN 100 to the VLANs handled by port 1/0/1.

4. `(config-if)# switchport trunk allowed vlan remove 15,16`

   Deletes VLAN 15 and VLAN 16 from the VLANs handled by port 1/0/1. At this point, port 1/0/1 handles tagged frames for VLAN 10 to 14, 17 to 20, and VLAN 100.

5. `(config-if)# switchport trunk allowed vlan 200-300`

   Sets VLANs 200 to 300 as VLANs to be handled by port 1/0/1. All previous settings are overwritten, so that the port handles tagged frames for VLANs 200 to 300.

Notes

A native VLAN is configured to handle untagged frames on the trunk port. For details, see *20.4.3 Configuring native VLANs for trunk ports*.

On a trunk port, when the number of deleted VLANs reaches 30, and the mode is changed to anything other than trunk port while the number of member VLANs is 30 or above, the MAC address table, ARP information, and NDP information are deleted for the corresponding port. Accordingly, keep in mind that when L3 forwarding is performed, the ARP and NDP are relearned, and communication is stopped.

20.2.5 Configuring TPIDs for VLAN tags

Points to note

The Switch can set the TPID of a VLAN tag to any value. The `vlan-dot1q-ethertype` command can be used to set the default value for the switch, and the `switchport dot1q ethertype` command can be used to set the value for each port. Ports for which no value is set are run using the default value for the switch.

The TPID setting for each port is set using the Ethernet interface configuration mode.

Command examples

1. `(config)# vlan-dot1q-ethertype 9100`

   Sets the default value for the Switch to 0x9100. All ports will run with a VLAN tag TPID of 9100.

2. `(config)# interface gigabitethernet 1/0/1`

   Switches to the Ethernet interface configuration mode for port 1/0/1.

3. `(config-if)# switchport dot1q ethertype 8100`

   Sets the TPID of port 1/0/1 to 0x8100. Port 1/0/1 recognizes 0x8100 as the VLAN tag. Other ports run using 0x9100, which is the default value for the switch.

Notes

Because TPIDs use the same position in a frame as an untagged frame EtherType, for 0x8000 and other IPv4 EtherTypes. It might not be possible to configure networks properly when values used as an EtherType are set. Therefore, set values that are not used as EtherType values.

20.3 Description of port VLANs

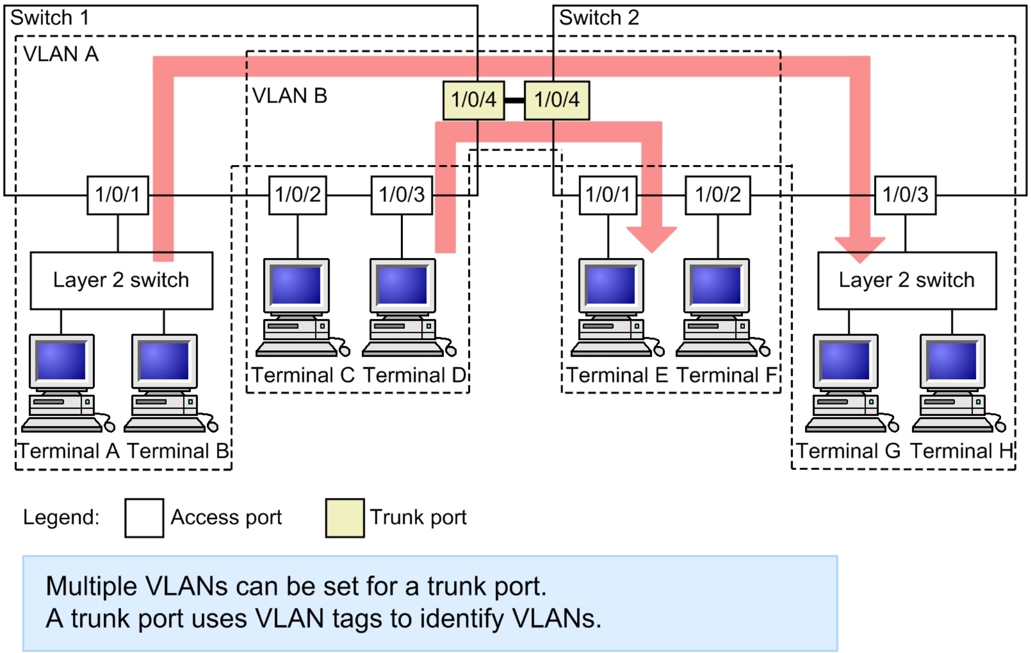
A port VLAN divides a VLAN into groups by port.

20.3.1 Access ports and trunk ports

A port VLAN allocates a single VLAN to a single port. The ports used for a port VLAN are set as access ports. A trunk port is used to connect multiple port VLANs to other LAN switches. Because a trunk port uses VLAN tags to identify VLANs, multiple VLANs can be set for a single port.

The figure below shows an example port VLAN configuration. Ports 1/0/1 to 1/0/3 set port VLANs as access ports. These two Switches are connected by a trunk port (port 1/0/4). VLAN tags are used in this case.

Figure 20-3: Example port VLAN configuration



Multiple VLANs can be set for a trunk port.
A trunk port uses VLAN tags to identify VLANs.

20.3.2 Native VLANs

Protocol ports, MAC ports, and trunk ports have a native VLAN to handle frames that do not match the configuration. The native VLAN for each port is VLAN 1 (the default VLAN) unless otherwise specified in the configuration. It can also be changed to another port VLAN.

For example, when VLAN B is set as the native VLAN for the trunk port in *Figure 20-3: Example port VLAN configuration*, VLAN B forwards untagged frames, even for the trunk port.

20.3.3 Notes on regarding port VLAN usage

(1) Note on tagged frames on access ports

Access ports handle untagged frames, discard any received tagged frames, and cannot perform transmission. Note that if the VLAN tag value matches the VLAN ID or is 0, the handling during reception is the same as for untagged frames. These frames are not sent.

(2) Note on usage with MAC VLANs

For notes on multicast when both a port VLAN and MAC VLAN exist on the same port. For details, see *20.7.5 Multicast when different VLANs are used together*.

20.4 Configuration of port VLANs

20.4.1 List of configuration commands

The following table describes the configuration commands for port VLANs.

Table 20-7: List of configuration commands

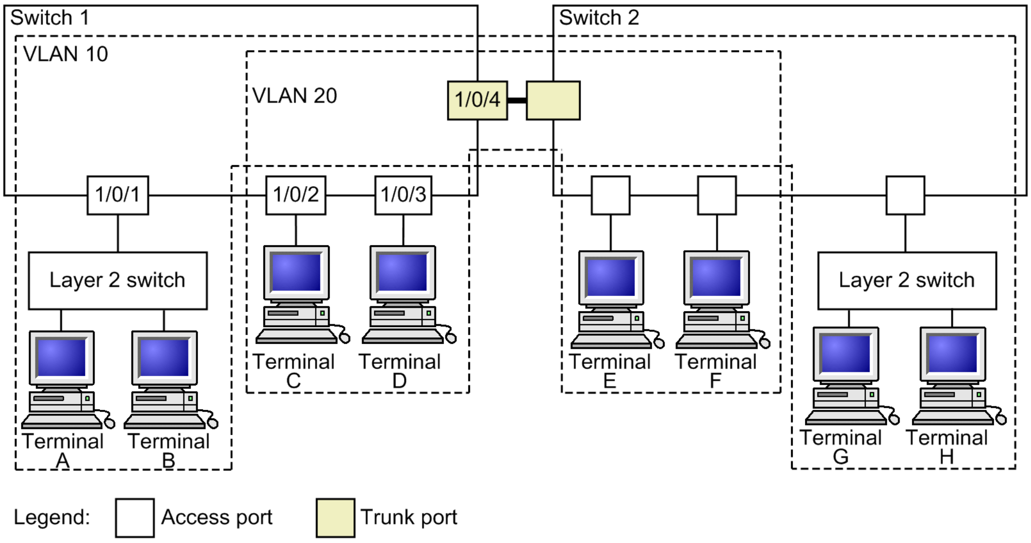
Command name	Description
switchport access	Sets the access port VLAN.
switchport mode	Sets the port type (access or trunk).
switchport trunk	Sets the VLAN for a trunk port.
vlan	Creates a port VLAN. Also, sets items pertaining to a VLAN in VLAN configuration mode.

20.4.2 Configuring a port VLAN

The following explains how to set a port VLAN. It provides example settings for Switch 1 shown in the figure below.

Port 1/0/1 is set for port VLAN 10. Ports 1/0/2 and 1/0/3 are set for port VLAN 20. Port 1/0/4 is the trunk port, and all VLANs are set for it.

Figure 20-4: Example port VLAN settings



(1) *Creating a port VLAN*

Points to note

The example below shows how to create a port VLAN. When a VLAN is created, if a VLAN ID is specified but a VLAN type is not, the VLAN becomes a port VLAN.

Command examples

1.
```
(config)# vlan 10,20
```

Creates VLAN ID 10 and VLAN ID 20 as port VLANs. This command switches to VLAN configuration mode.

(2) Setting access ports

When a single VLAN is set to a single port and untagged frames are handled, it is set as an access port.

Points to note

The example below shows how to set a port for the access port, and set the VLANs handled by the access port.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
```
Switches to the Ethernet interface configuration mode for port 1/0/1.

2.
```
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# exit
```
Sets port 1/0/1 as an access port. Then, sets VLAN 10.

3.
```
(config)# interface range gigabitethernet 1/0/2-3
```
Switches ports 1/0/2 and 1/0/3 to Ethernet interface configuration mode. Because the configuration is the same for ports 1/0/2 and 1/0/3, setting is done as a batch operation.

4.
```
(config-if-range)# switchport mode access
(config-if-range)# switchport access vlan 20
```
Sets ports 1/0/2 and 1/0/3 as access ports. Then, sets VLAN 20.

(3) Setting trunk ports

Points to note

The example below shows how to set the port that handles tagged frames as the trunk port, and set the VLANs for the trunk port.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/4
```
Switches to the Ethernet interface configuration mode for port 1/0/4.

2.
```
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 10,20
```
Sets port 1/0/4 as a trunk port. Then, sets VLAN 10 and VLAN 20.

20.4.3 Configuring native VLANs for trunk ports

Points to note

Set a native VLAN for handling untagged frames on a trunk port. Only port VLANs can be set for a native VLAN.

When the VLAN ID of a native VLAN is specified for the `switchport trunk allowed vlan` command, the VLAN handles untagged frames on the trunk port. The native VLAN is VLAN 1 (the default VLAN) unless explicitly specified otherwise in the configuration.

To handle tagged frames (where the VLAN tag has a VLAN ID of 1) for the default VLAN on a trunk port, change the native VLAN to another VLAN.

Command examples

1.
```
(config)# vlan 10,20
(config-vlan)# exit
```
Creates VLAN ID 10 and VLAN ID 20 as port VLANs.

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# switchport mode trunk
```
Switches to the Ethernet interface configuration mode for port 1/0/1. Then, sets the port as a trunk port. At this point, the native VLAN for trunk port 1/0/1 is the default VLAN.

3.
```
(config-if)# switchport trunk native vlan 10
(config-if)# switchport trunk allowed vlan 1,10,20
```
Sets the native VLAN for trunk port 1/0/1 to VLAN 10. Then, sets VLANs 1, 10, and 20. VLAN 10 (the native VLAN) handles untagged frames, and VLAN 1 (the default VLAN) and VLAN 20 handle tagged frames.

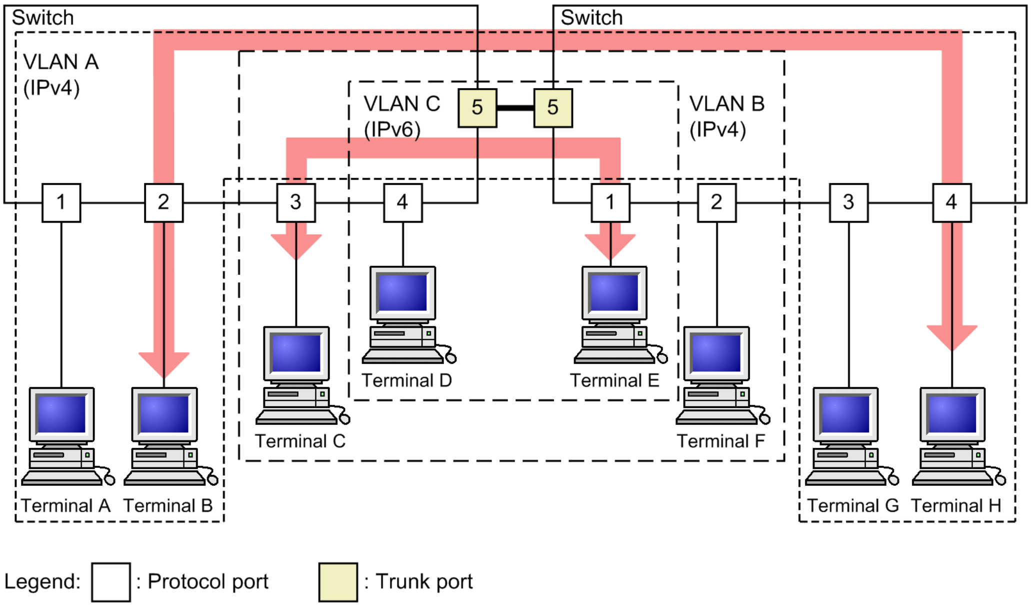
20.5 Description of protocol VLANs

20.5.1 Overview

A protocol VLAN divides VLANs by protocol. Different VLANs can be configured for each protocol, such as IPv4 and IPv6. Multiple protocols can be set for the same protocol VLAN.

The figure below shows an example protocol VLAN configuration. In the following example, VLANs A and B are configured with the IPv4 protocol, and VLAN C is configured with the IPv6 protocol.

Figure 20-5: Example protocol VLAN configuration



- VLANs A and B are IPv4 protocol VLANs.
- VLAN C is an IPv6 protocol VLAN.
- Terminals D and E belong to both VLANs B and C.
- The arrows between terminal B and terminal H, and between terminal C and terminal E are examples of communication using the same VLAN.

20.5.2 Distinguishing protocols

The following table describes the three types of values that can be used to distinguish protocols.

Table 20-8: Values for distinguishing protocols

Distinguishing value	Overview
Ether-type value	Protocols are distinguished by the Ether-type value of Ethernet V2-format frames.
LLC value	Protocols are distinguished by the LLC value (DSAP or SSAP) of 802.3-format frames.
SNAP Ether-type value	Protocols are distinguished by the Ether-type value of 802.3-format frames. This applies only to frames with an LLC value of `AA AA 03`.

Protocols are created by configuration and are associated with VLANs. Multiple VLANs can be associated with a single protocol.

20.5.3 Protocol ports and trunk ports

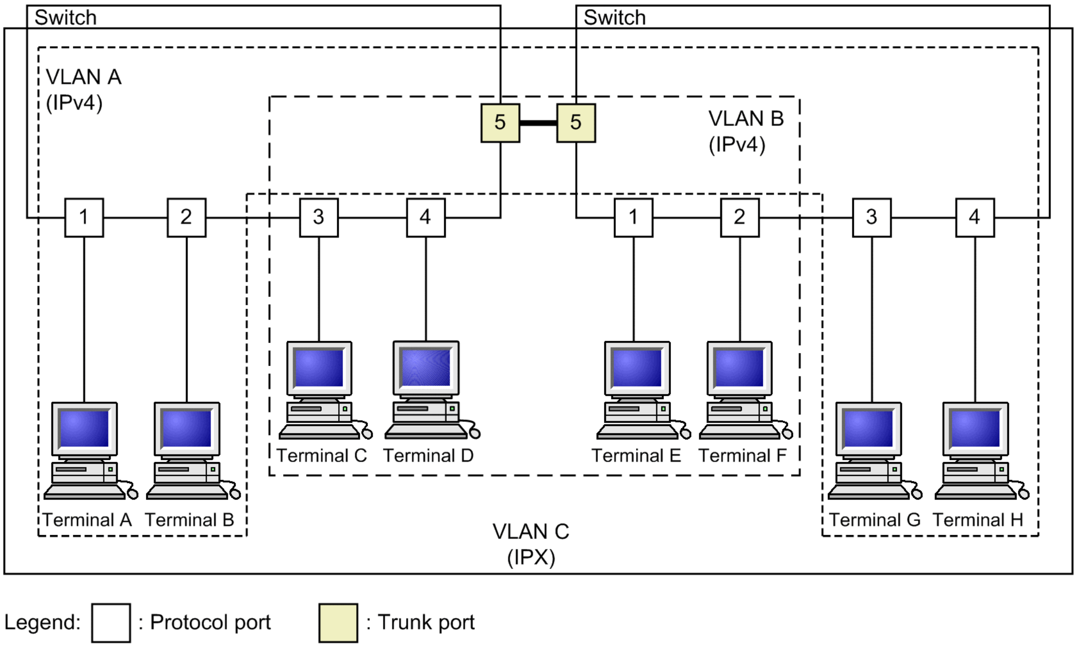
Protocol ports identify the protocol for untagged frames. Ports used as protocol VLANs set a protocol port. Different VLANs over multiple protocols can be assigned to a protocol port. Trunk ports are used to connect multiple protocol VLANs to another LAN switch. Note that because trunk ports distinguish VLANs by their VLAN tag, they do not distinguish according to protocol.

20.5.4 Native VLANs for protocol ports

When a frame with a protocol that does not match the configuration is received on a protocol port, it is handled by the native VLAN. The native VLAN is VLAN 1 (the default VLAN) unless otherwise specified in the configuration. It can also be changed to another port VLAN.

The figure below shows an example of a configuration in which the native VLAN is used for the protocol port. In this configuration, the IPX protocol is used for a single VLAN over the entire network, and other protocols such as IPv4 are split by VLAN for the port VLAN. VLAN A and VLAN B are set as the native VLAN for each port. Note that in this example configuration, both VLAN A and VLAN B can be set as IPv4 protocol VLANs.

Figure 20-6: Example configuration using the native VLAN for the protocol port



- VLANs A and B are set as native VLANs on the port VLAN.
- VLAN C is an IPX protocol VLAN.
- All terminals belong to IPX protocol VLANs.
- Terminals A, B, G, and H belong to a different port VLAN than terminals C, D, E, and F.

20.6 Configuration of protocol VLANs

20.6.1 List of configuration commands

The following table describes the configuration commands for protocol VLANs.

Table 20-9: List of configuration commands

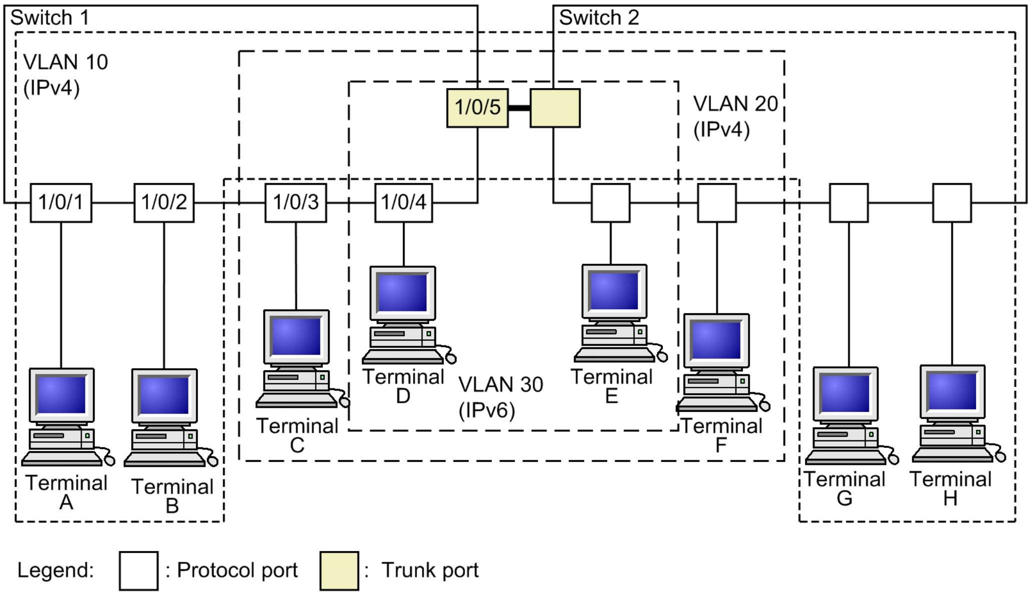
Command name	Description
protocol	Sets the protocol for identifying VLANs in protocol VLANs.
switchport mode	Sets the port type (protocol or trunk).
switchport protocol	Sets the VLAN for protocol ports.
switchport trunk	Sets the VLAN for a trunk port.
vlan	Specifies the `protocol-based` parameter to create a protocol VLAN.
vlan-protocol	Sets the protocol name and protocol value for a protocol VLAN.

20.6.2 Creating protocol VLANs

The following explains how to set a protocol VLAN. It provides example settings for Switch 1 shown in the figure below.

Ports 1/0/1 and 1/0/2 are set for IPv4 protocol VLAN 10. Ports 1/0/3 and 1/0/4 are set for IPv4 protocol VLAN 20. Port 1/0/4 belongs to both VLAN 20 and IPv6 protocol VLAN 30 at the same time. Port 1/0/5 is the trunk port, and all VLANs are set for it.

Figure 20-7: Example settings for protocol VLANs



(1) Creating protocols to distinguish VLANs

Points to note

When a protocol VLAN is set, the `vlan-protocol` command sets the distinguishing protocol before VLAN creation. A protocol name and a protocol value are set for a protocol. Multiple protocol values can be associated with a single name.

Because the IPv4 protocol requires that both an IPv4 Ether-type and ARP Ether-type are specified at the same time, two protocol values are associated with IPv4.

Command examples

1.
```
(config)# vlan-protocol IPV4 ethertype 0800 ethertype 0806
```

Creates a protocol named IPV4. The IPv4 Ether-type value 0800 and ARP Ether-type value 0806 are associated as protocol values.

Note that protocol judgment for this setting is only for frames in Ethernet V2 format.

2.
```
(config)# vlan-protocol IPV6 ethertype 86dd
```

Creates a protocol named IPV6. The IPv6 Ether-type value 86DD is associated as the protocol value.

(2) Creating protocol VLANs

Points to note

The example below shows how to create a protocol VLAN. When a VLAN is created, a VLAN ID and the `protocol-based` parameter are specified. The created protocol is specified as the protocol for distinguishing VLANs.

Command examples

1.
```
(config)# vlan 10,20 protocol-based
```

Creates VLANs 10 and 20 as protocol VLANs. Because VLANs 10 and 20 are used as the same IPv4 protocol VLAN, setting is done in a batch operation. This command switches to VLAN configuration mode.

2.
```
(config-vlan)# protocol IPV4
(config-vlan)# exit
```

Specifies the created IPv4 protocol as the protocol for distinguishing VLANs 10 and 20.

3.
```
(config)# vlan 30 protocol-based
(config-vlan)# protocol IPV6
```

Creates VLAN 30 as a protocol VLAN. The created IPv6 protocol is specified as a protocol for distinguishing VLAN 30.

(3) Setting protocol ports

Points to note

The protocol port set as the port for distinguishing VLANs by protocol for protocol VLANs handles untagged frames.

Command examples

1.
```
(config)# interface range gigabitethernet 1/0/1-2
```

Switches ports 1/0/1 and 1/0/2 to Ethernet interface configuration mode. Because ports 1/0/1 and 1/0/2 use the same configuration, they are specified in a batch operation.

2.
```
(config-if-range)# switchport mode protocol-vlan
```

```
(config-if-range)# switchport protocol vlan 10
(config-if-range)# exit
```

Sets ports 1/0/1 and 1/0/2 as protocol ports. Then, sets VLAN 10.

3.
```
(config)# interface range gigabitethernet 1/0/3-4
(config-if-range)# switchport mode protocol-vlan
(config-if-range)# switchport protocol vlan 20
(config-if-range)# exit
```

Sets ports 1/0/3 and 1/0/4 as protocol ports. Then, sets VLAN 20.

4.
```
(config)# interface gigabitethernet 1/0/4
(config-if)# switchport protocol vlan add 30
```

Adds VLAN 30 to port 1/0/4. Two types of protocol VLAN, IPv4 and IPv6 are set for port 1/0/4.

Notes

The `switchport protocol vlan` command does not add to the previous configuration. Instead, it replaces the settings in the specified <*vlan id list*>. To add and remove VLANs for ports on which protocol VLANs are already running, use the `switchport protocol vlan add` command and `switchport protocol vlan remove` command.

(4) Setting trunk ports

Points to note

For protocol VLANs, ports handling tagged frames are set as trunk ports, and VLANs are set for the trunk ports.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/5
```

Switches to the Ethernet interface configuration mode for port 1/0/5.

2.
```
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 10,20,30
```

Sets port 1/0/5 as a trunk port. Then, sets VLAN 10, VLAN 20 and VLAN 30.

20.6.3 Configuring native VLAN for protocol ports

Points to note

Set a native VLAN for handling untagged frames that do not match the protocol set for a protocol port. Only port VLANs can be set for a native VLAN.

When the VLAN ID of a native VLAN is specified for the `switchport protocol native vlan` command, it becomes the VLAN for handling untagged frames that do not match the protocol on the protocol port. The native VLAN is VLAN 1 (the default VLAN) unless explicitly specified otherwise in the configuration.

If status suspend is set for a native VLAN, frames that do not match the set protocol are not forwarded.

Command examples

1.
```
(config)# vlan 10,20 protocol-based
(config-vlan)# exit
(config)# vlan 30
(config-vlan)# exit
```
Creates VLANs 10 and 20 as protocol VLANs. Then, creates VLAN 30 as a port VLAN.

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# switchport mode protocol-vlan
```
Switches to the Ethernet interface configuration mode for port 1/0/1. Then, sets the port as a protocol port.

3.
```
(config-if)# switchport protocol native vlan 30
(config-if)# switchport protocol vlan 10,20
```
Sets the native VLAN for protocol port 1/0/1 to port VLAN 30, making it the VLAN that handles untagged frames that do not match the set protocol. The command also sets protocol VLANs 10 and 20.

20.7 Description of MAC VLANs

20.7.1 Overview

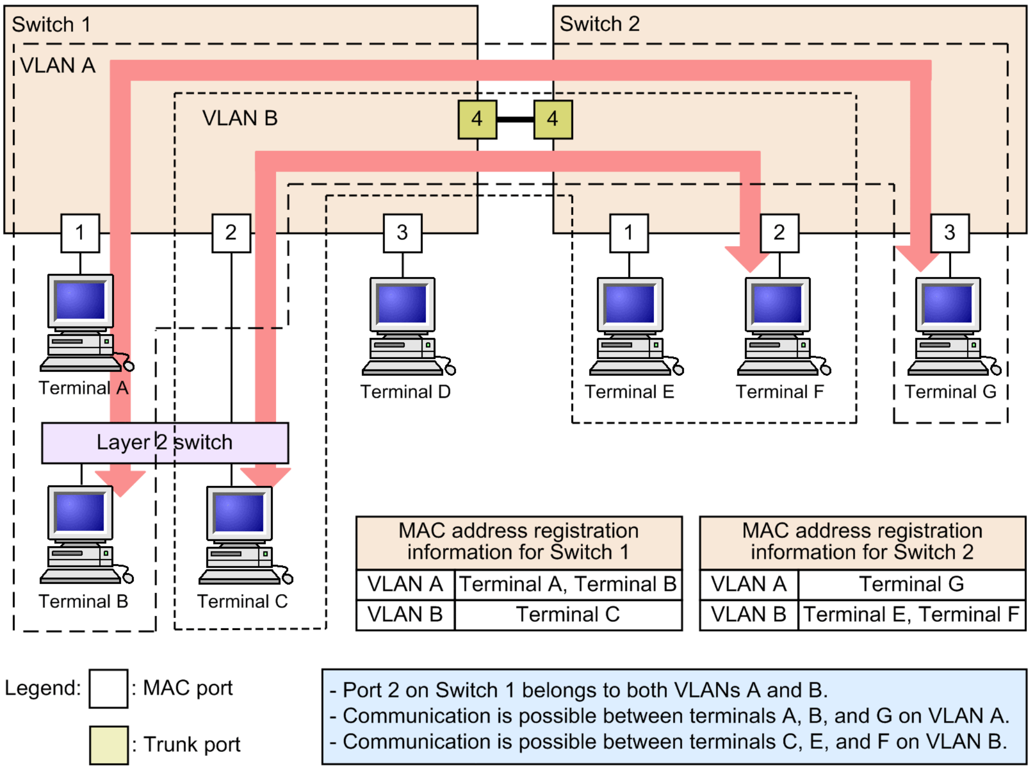
MAC VLANs divide VLAN groups by source MAC address. MAC addresses can be registered with VLANs by configuration, or dynamically through the Layer 2 authentication functionality.

MAC VLANs can be set to allow communication only with terminals permitted to connect by registering MAC addresses of permitted terminals during configuration, or by registering MAC addresses authenticated using the Layer 2 authentication functionality.

In addition, if the `mac-based-vlan static-only` configuration command is set, the `mac-address` configuration command can be used to set as many MAC addresses as the maximum allowable MAC VLAN count permits. In this case, the Layer 2 authentication functionality cannot be run.

The figure below shows an example MAC VLAN configuration. When a trunk port is set between switches comprising a VLAN, VLANs are determined by VLAN tags regardless of source MAC addresses. Therefore, all switches do not need to be set with the same MAC address. The MAC address of the terminal connected to the MAC port is set for each switch.

Figure 20-8: Example MAC VLAN configuration



MAC address registration information for Switch 1	
VLAN A	Terminal A, Terminal B
VLAN B	Terminal C

MAC address registration information for Switch 2	
VLAN A	Terminal G
VLAN B	Terminal E, Terminal F

Legend: □ : MAC port

🟨 : Trunk port

- Port 2 on Switch 1 belongs to both VLANs A and B.
- Communication is possible between terminals A, B, and G on VLAN A.
- Communication is possible between terminals C, E, and F on VLAN B.

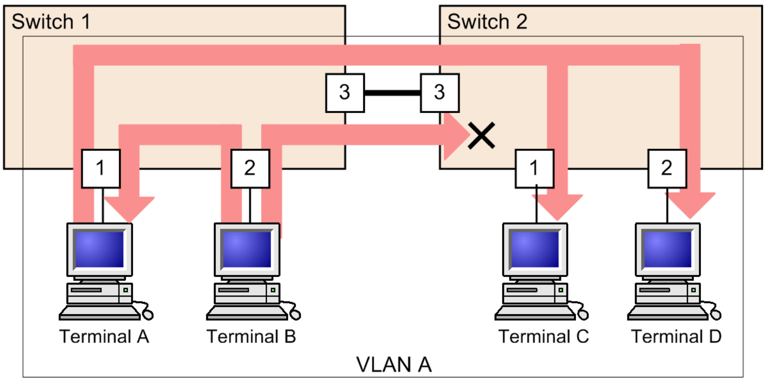
20.7.2 Connections between switches and MAC address settings

When a MAC VLAN is configured on multiple switches, we recommend that you use a trunk port for connections between the switches. VLAN judgment for frames received on trunk ports is performed by VLAN tags. This allows communication by MAC VLAN, even when no source MAC address is set for a VLAN. For details about using a trunk port to connect switches, see *Figure 20-8: Example MAC VLAN configuration*.

When a MAC port is used to connect switches, all MAC addresses belonging to the VLAN need to be set on all switches. If a router exists, register the MAC address of the router. Also, when using VRRP, register the MAC address of the virtual router.

The following figure shows switches connected by MAC port.

Figure 20-9: Switches connected by MAC port



MAC address registration information for Switch 1	
VLAN A	Terminal A, Terminal B Terminal C, Terminal D

MAC address registration information for Switch 2	
VLAN A	Terminal A, Terminal C, Terminal D

Legend: □ : MAC port

- Because terminal A is set on both Switches 1 and 2, it can perform communication with terminal C and terminal D.
- Because there are no settings for terminal B on Switch 2, it cannot perform communication with terminal C and terminal D.
  Communication is possible with terminal A.

20.7.3 Linkage with the Layer 2 authentication functionality

MAC VLANs can link with the Layer 2 authentication functionality to dynamically registered MAC addresses with a VLAN. The following are types of the Layer 2 authentication functionality that can be linked:

- IEEE 802.1X
- Web authentication
- MAC-based authentication
- Authentication VLAN

The MAC addresses of printers, servers, and other terminals that connect to a MAC port without using the Layer 2 authentication functionality are registered with VLANs during configuration.

When the same MAC address is set for configuration and the Layer 2 authentication functionality, the configuration MAC address is registered.

20.7.4 VLAN settings for MAC ports

VLANs can be set for MAC ports using the `switchport mac vlan` configuration command, or dynamically using the Layer 2 authentication functionality.

Note that VLAN settings by configuration and dynamic VLAN settings by the Layer 2 authentication functionality cannot both exist on the same MAC port. If VLANs are set dynamically using the Layer 2 authentication functionality for a MAC port set to be authenticated, and then the `switchport mac vlan` configuration command is set, the all VLANs dynamically set for the corresponding port are deleted.

The following table describes the Layer 2 authentication functionality and authentication modes that can be set dynamically for VLANs.

Table 20-10: Layer 2 authentication functionality and authentication modes that permit dynamic VLAN assignment

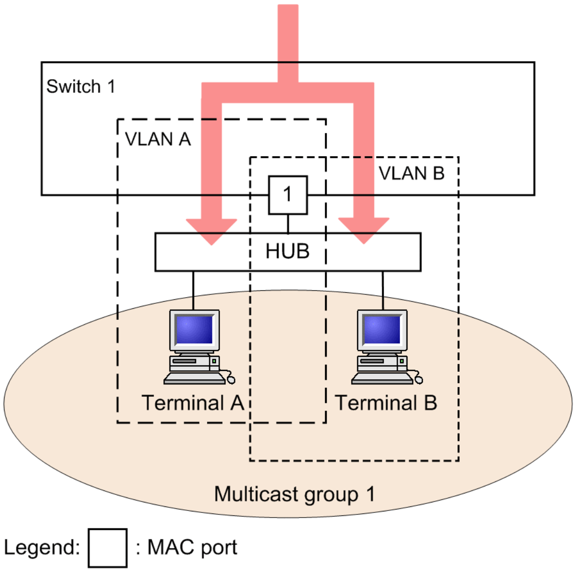
Layer 2 authentication functionality	Authentication mode
IEEE 802.1X	VLAN-based authentication (dynamic)
Web authentication	Dynamic VLAN mode
MAC-based authentication	Dynamic VLAN mode

20.7.5 Multicast when different VLANs are used together

When multiple MAC VLANs exist on the same port, or a port VLAN and MAC VLAN are both on the same port, if the terminals belonging to each VLAN also belong to the same multicast group, the terminals will receive the same frames more than once. This is because the same multicast frames are sent for each VLAN.

The following figure shows an example network configuration in which terminals receive multicast data more than once.

Figure 20-10: Multicast when VLANs are mixed



- Port 1 on Switch 1 belongs to both VLANs A and B.
- Terminals A and B belong to the same multicast group 1.
- Multicasts are sent from port 1 to each of VLAN A and VLAN B.

20.8 Configuration of MAC VLANs

20.8.1 List of configuration commands

The following table describes the configuration commands for MAC VLANs.

Table 20-11: List of configuration commands

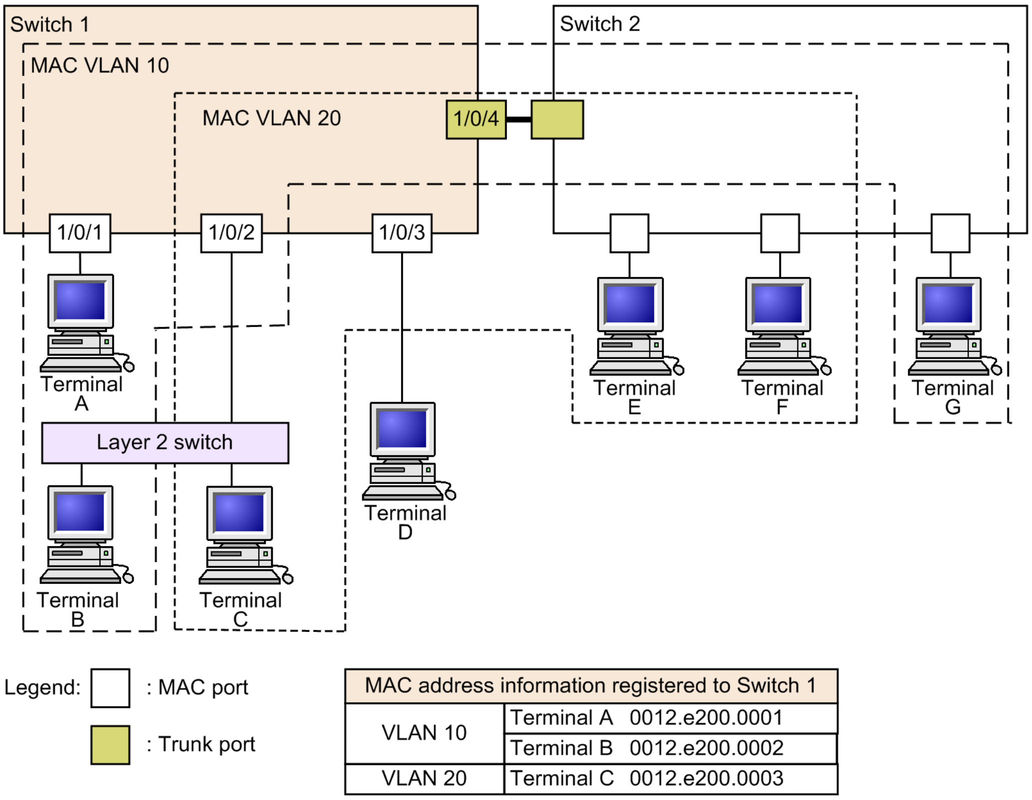
Command name	Description
mac-address	Sets the MAC address, by configuration, for terminals belonging to VLANs for a MAC VLAN.
switchport mac	Sets the VLAN of a MAC port.
switchport mode	Sets the port type (MAC or trunk).
switchport trunk	Sets the VLAN for a trunk port.
vlan	Specifies the `mac-based` parameter to create a MAC VLAN.

20.8.2 Configuring MAC VLANs

The following explains how to set a MAC VLAN. It includes an example for setting the MAC address belonging to MAC VLANs and VLANs by configuration. For details about linkage with IEEE 802.1X, see *7. Settings and Operation for IEEE 802.1X* in the manual *Configuration Guide Vol. 2 For Version 11.10*.

The figure below shows example settings for Switch 1. Port 1/0/1 is set for MAC VLAN 10. Port 1/0/2 is set for MAC VLANs 10 and 20, and port 1/0/3 is set for MAC VLAN 20. Note that terminal D, for which no MAC address is registered, is connected to port 1/0/3.

Figure 20-11: Example MAC VLAN settings



MAC address information registered to Switch 1		
VLAN 10	Terminal A	0012.e200.0001
	Terminal B	0012.e200.0002
VLAN 20	Terminal C	0012.e200.0003

(1) Creating MAC VLANs and registering MAC addresses

Points to note

The example below shows how to create a MAC VLAN. When a VLAN is created, a VLAN ID and the `mac-based` parameter are specified.

As shown here, the MAC address belonging to the VLAN is also set. VLANs are registered for each terminal from A to C in the example configuration. Because communication with the MAC VLAN is not permitted for terminal D, it is not registered.

Command examples

1.
```
(config)# vlan 10 mac-based
(config-vlan)# name MACVLAN10
```
Creates VLAN 10 as a MAC VLAN. This command switches to VLAN configuration mode.

2.
```
(config-vlan)# mac-address 0012.e200.0001
(config-vlan)# mac-address 0012.e200.0002
(config-vlan)# exit
```
Registers terminal A (0012.e200.0001) and terminal B (0012.e200.0002) for MAC VLAN 10.

3.
```
(config)# vlan 20 mac-based
(config-vlan)# name MACVLAN20
(config-vlan)# mac-address 0012.e200.0003
```
Creates VLAN 20 as a MAC VLAN, and registers terminal C (0012.e200.0003) for MAC VLAN 20.

Notes

When MAC addresses are registered for MAC VLANs, the same MAC address cannot be registered for multiple VLANs.

(2) Setting MAC ports

Points to note

The MAC port set for distinguishing VLANs by source MAC address for the MAC VLAN handles untagged frames.

Command examples

1.
```
(config)# interface range gigabitethernet 1/0/1-2
```
Switches ports 1/0/1 and 1/0/2 to Ethernet interface configuration mode.

2.
```
(config-if-range)# switchport mode mac-vlan
(config-if-range)# exit
```
Sets ports 1/0/1 and 1/0/2 for the MAC port. VLANs are registered dynamically for ports 1/0/1 and 1/0/2 by the Layer 2 authentication functionality.

3.
```
(config)# interface gigabitethernet 1/0/3
```

```
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 20
```

Sets port 1/0/3 as a MAC port. Then, sets VLAN 20.

Notes

The `switchport macvlan` command does not add to the previous configuration. Instead, it replaces the settings in the specified <*vlan id list*>. To add and remove VLANs for ports on which protocol VLANs are already running, use the `switchport mac vlan add` command and `switchport mac vlan remove` command.

(3) Setting trunk ports

Points to note

Even for MAC VLANs, trunk ports are set to handle tagged frames, and VLANs are set for this trunk port.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/4
```

Switches to the Ethernet interface configuration mode for port 1/0/4.

2.
```
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 10,20
```

Sets port 1/0/4 as a trunk port. Then, sets VLAN 10 and VLAN 20.

20.8.3 Configuring native VLANs for MAC ports

Points to note

Set native VLANs to handle untagged frames that do not match the MAC addresses registered for MAC VLANs on a MAC port. Only port VLANs can be set for native VLANs.

When the VLAN ID of a native VLAN is specified by the `switchport mac native vlan` command, the VLAN handles untagged frames that do not match the MAC addresses registered for the MAC port. The native VLAN is VLAN 1 (the default VLAN) unless explicitly specified otherwise in the configuration.

When `status suspend` is set for a native VLAN, frames that do not match the registered MAC addresses are not forwarded.

Command examples

1.
```
(config)# vlan 10,20 mac-based
(config-vlan)# exit
(config)# vlan 30
(config-vlan)# exit
```

Creates VLAN 10 and 20 as MAC VLANs. Then, creates VLAN 30 as a port VLAN.

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# switchport mode mac-vlan
```

Switches to the Ethernet interface configuration mode for port 1/0/1. Also, sets the port as a MAC port.

3. `(config-if)# switchport mac native vlan 30`

   Sets the native VLAN of port 1/0/1 as port VLAN 30. VLAN 30 handles untagged frames from MAC addresses not registered for port 1/0/1.

20.9 VLAN interfaces

20.9.1 Interface for setting IP addresses

To use the Switch as a Layer 3 switch, set an IP address for the VLAN. When multiple VLANs are created, an IP address can be set for each VLAN to run the Switch as a Layer 3 switch.

IP addresses can be set using the `interface vlan` configuration command. This interface is called a VLAN interface.

20.9.2 MAC addresses of VLAN interfaces

VLAN interfaces for which an IP address is set use one of the MAC addresses of the Switch as the MAC address of the interface. The MAC addresses used are as follows:

- Switch MAC addresses
- MAC addresses for each VLAN

By default, the device MAC address is used, but can be set by configuration to the MAC address for each VLAN.

The MAC address for a VLAN interface can be changed during operation by configuration. Keep in mind that when the address is changed during operation, because the MAC addresses learned through ARP or NDP by the neighboring Layer 3 switches (routers, Layer 3 switches, or terminals) no longer match the MAC address of the Switch, communication might not be possible temporarily.

20.10 Configuration of VLAN interfaces

20.10.1 List of configuration commands

The following table describes the basic configuration commands for setting IP addresses for VLAN interfaces, for use as Layer 3 switches.

Table 20-12: List of configuration commands

Command name	Description
interface vlan	Sets a VLAN interface and switches to the interface mode.
vlan-mac	Sets MAC addresses to be used for each VLAN.
vlan-mac-prefix	Sets an individual MAC address prefix for each VLAN.
ip address#	Sets the IPv4 address of an interface.

#

See *2. IPv4, ARP, and ICMP* in the manual *Configuration Command Reference Vol. 2 For Version 11.10*.

20.10.2 Configuring VLANs as Layer 3 interfaces

Points to note

VLANs can be used as Layer 3 interfaces by setting an IP address. Various Layer 3 functionality settings can be performed by the `interface vlan` command and in the VLAN interface configuration mode.

The following describes an example of setting an IPv4 address for a VLAN interface. For details about the Layer 3 functionality that can be set for a VLAN interface, see the chapter for the respective functionality used.

Command examples

1.
```
(config)# interface vlan 10
```

Switches to the VLAN interface configuration mode for VLAN 10. If the VLAN ID specified for the `interface vlan` command is not yet set, a port VLAN is automatically created and set using the `vlan` command.

2.
```
(config-if)# ip address 192.168.1.1 255.255.255.0
```

Sets the IPv4 address 192.168.1.1 and the subnet mask 255.255.255.0 for VLAN 10.

20.10.3 Configuring MAC addresses for VLAN interfaces

By default, the MAC address for the VLAN interface of the Switch is used for the device MAC address of all VLANs. Usually, because a LAN switch learns MAC addresses for each VLAN, the same MAC address can be used for different VLANs. However, if a LAN switch managing a single MAC address table per switch, and not per VLAN, is used on the same network, when the same MAC address is used for different VLANs, MAC address learning might become unstable. In this case, the network can be stabilized by changing the MAC address of the VLAN interface for each VLAN.

Points to note

When a VLAN is used as a Layer 3 interface, the MAC addresses for VLAN interfaces can be changed. MAC addresses are set using the `vlan-mac-prefix` command and `vlan-mac` command.

For the MAC address of each VLAN, the `vlan-mac-prefix` command specifies a prefix (the highest 34 bits), and the `vlan-mac` command is used for each VLAN to set that MAC addresses are to be used per VLAN. The VLAN ID is used for the lowest 12 bits of a MAC address.

Command examples

1. `(config)# vlan-mac-prefix 0012.e200.0000 ffff.ffff.c000`

   Specifies the prefix (highest 34 bits) used for MAC addresses for each VLAN. When 34 bits are specified, ffff.ffff.c000 is used for the mask.

2. `(config)# vlan 10`

   Switches to the VLAN configuration mode for VLAN 10.

3. `(config-vlan)# vlan-mac`

   Sets that MAC addresses are to be used for each VLAN on VLAN 10. The VLAN ID is used for the lowest 12 bits of the MAC address. In this case, the MAC address for VLAN 10 is 0012.e200.000a.

   The value of a MAC address can be checked using the `show vlan` operation command.

Notes

The MAC address for a VLAN interface is changed by the MAC address setting for each VLAN. In this case, because the MAC addresses learned through ARP or NDP by the neighboring Layer 3 switches (routers, Layer 3 switches, or terminals) no longer match the MAC address of the Switch, communication might not be possible temporarily. We recommend that you use this functionality either before starting VLAN interface operation, or at a time of minimal impact.

Note that MAC address settings for each VLAN are take effect only when an IP address is set for the corresponding VLAN interface.

20.11 VLAN operation

20.11.1 List of operation commands

The following table describes the operation commands for VLANs.

Table 20-13: List of operation commands

Command name	Description
show vlan	Shows information about VLANs.
show vlan mac-vlan	Shows the MAC addresses registered for MAC VLANs.
restart vlan	Restarts the VLAN program.
dump protocols vlan	Outputs to a file detailed event trace information and control tables collected for a VLAN program.

20.11.2 Checking VLAN status

(1) Checking the status of VLAN settings

VLAN information can be checked by using the `show vlan` command. Check `VLAN ID`, `Type`, and `IP Address` to make sure that the VLAN settings are correct. `Untagged` indicates the port handling untagged frames for the VLAN, and `Tagged` indicates the port handling tagged frames for the VLAN. Make sure that the ports set for the VLAN are correct.

Figure 20-12: Results of executing the show vlan command

```
> show vlan
Date 20XX/01/26 17:01:40 UTC
VLAN counts:4
VLAN ID:1     Type:Port based      Status:Up
  Learning:On            Tag-Translation:
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN0001
  IP Address:10.215.201.1/24
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0001
  Spanning Tree:PVST+(802.1D)
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Untagged(18)   :1/0/1-4,13-26
VLAN ID:3     Type:Port based      Status:Up
  Learning:On            Tag-Translation:On
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN0003
  IP Address:10.215.196.1/23
             3ffe:501:811:ff08::5/64
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0003
  Spanning Tree:Single(802.1D)
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Untagged(8)    :1/0/5-12
  Tagged(2)      :1/0/25-26
  Tag-Trans(2)   :1/0/25-26
VLAN ID:120   Type:Protocol based  Status:Up
  Protocol VLAN Information  Name:ipv6
  EtherType:08dd  LLC:  Snap-EtherType:
  Learning:On            Tag-Translation:On
  BPDU Forwarding:       EAPOL Forwarding:
```

```
  Router Interface Name:VLAN0120
  IP Address:
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0120
  Spanning Tree:
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Untagged(3)   :1/0/5,7,9
  Tagged(2)     :1/0/25-26
  Tag-Trans(2)  :1/0/25-26
VLAN ID:1340  Type:Mac based       Status:Up
  Learning:On            Tag-Translation:On
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN1340
  IP Address:10.215.202.1/24
  Source MAC address: 0012.e2de.053c(VLAN)
  Description:VLAN1340
  Spanning Tree:
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Untagged(6)   :1/0/13-18
  Tagged(2)     :1/0/25-26
  Tag-Trans(2)  :1/0/25-26
>
```

(2) Checking the status of VLAN communication

The status of VLAN communication can be checked by using the `show vlan detail` command. Check `Port Information` to see the `Up/Down` and `Forwarding/Blocking` values for the port. If the status is `Blocking`, the cause of the blocking is displayed in parentheses.

Figure 20-13: Results of executing the show vlan detail command

```
> show vlan 3,1000-1500 detail
Date 20XX/01/26 17:01:40 UTC
VLAN counts:2
VLAN ID:3     Type:Port based      Status:Up
  Learning:On            Tag-Translation:On
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN0003
  IP Address:10.215.196.1/23
             ee80::220:afff:fed7:8f0a/64
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0003
  Spanning Tree:Single(802.1D)
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Port Information
   1/0/5          Up   Forwarding      Untagged
   1/0/6          Up   Blocking(STP)   Untagged
   1/0/7          Up   Forwarding      Untagged
   1/0/8          Up   Forwarding      Untagged
   1/0/9          Up   Forwarding      Untagged
   1/0/10         Up   Forwarding      Untagged
   1/0/11         Up   Forwarding      Untagged
   1/0/12         Up   Forwarding      Untagged
   1/0/25(CH:9)   Up   Forwarding      Tagged   Tag-Translation:103
   1/0/26(CH:9)   Up   Blocking(CH)    Tagged   Tag-Translation:103
VLAN ID:1340  Type:Mac based       Status:Up
  Learning:On            Tag-Translation:On
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN1340
  IP Address:10.215.202.1/24
  Source MAC address: 0012.e2de.053c(VLAN)
  Description:VLAN1340
  Spanning Tree:
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Port Information
   1/0/13         Up   Forwarding      Untagged
   1/0/14         Up   Forwarding      Untagged
   1/0/15         Up   Forwarding      Untagged
   1/0/16         Up   Forwarding      Untagged
   1/0/17         Up   Forwarding      Untagged
   1/0/18         Up   Forwarding      Untagged
   1/0/25(CH:9)   Up   Forwarding      Tagged   Tag-Translation:104
   1/0/26(CH:9)   Up   Blocking(CH)    Tagged   Tag-Translation:104
>
```

(3) Checking the VLAN ID list

The `show vlan summary` command can be used to check the set VLAN types, as well as their count and VLAN IDs.

Figure 20-14: Results of executing the show vlan summary command

```
> show vlan summary
Date 20XX/10/14 12:14:38 UTC
Total(4)            :1,10,20,4094
Port based(2)       :1,4094
Protocol based(1)   :10
MAC based(1)        :20
>
```

(4) Checking through VLAN list display

The `show vlan list` command provides an overview of the status of VLAN settings on one line. This command can be used to list the statuses of VLAN settings, Layer 2 redundancy functionality, and IP address settings. Also, a VLAN, port, or channel group can be specified as a parameter to check a list of only the VLAN statuses specified for the parameter.

Figure 20-15: Results of executing the show vlan list command

```
> show vlan list
Date 20XX/01/26 17:01:40 UTC
VLAN counts:4
ID   Status  Fwd/Up /Cfg Name             Type  Protocol       Ext.    IP
   1 Up       16/ 18/ 18 VLAN0001         Port  STP PVST+:1D   - - - - 4
   3 Up        9/ 10/ 10 VLAN0003         Port  STP Single:1D  - - T - 4/6
 120 Up        4/  5/  5 VLAN0120         Proto -              - - - - -
1340 Disable   0/  8/  8 VLAN1340         Mac   -              - - - - 4
     AXRP (Control-VLAN)
     GSRP GSRP ID:VLAN Group ID(Master/Backup)
     S:IGMP/MLD snooping  T:Tag Translation
     4:IPv4 address configured  6:IPv6 address configured
>
```

(5) Checking MAC addresses registered for MAC VLANs

The `show vlan mac-vlan` command can be used to check the MAC addresses registered for MAC VLANs.

The functionality that registered a MAC address is displayed in parentheses.

- `static` indicates a MAC address registered by configuration
- `dot1x` indicates a MAC address registered by IEEE 802.1X

Figure 20-16: Results of executing the show vlan mac-vlan command

```
> show vlan mac-vlan
Date 20XX/10/14 12:16:04 UTC
VLAN counts:2    Total MAC Counts:5
VLAN ID:20   MAC Counts:4
   0012.e200.0001 (static)    0012.e200.0002 (static)
   0012.e200.0003 (static)    0012.e200.0004 (dot1x)
VLAN ID:200  MAC Counts:1
   0012.e200.1111 (dot1x)
>
```

Chapter

21. VLAN Extended Functionality

This chapter describes the VLAN extended functionality and its use.

21.1 Description of VLAN tunneling

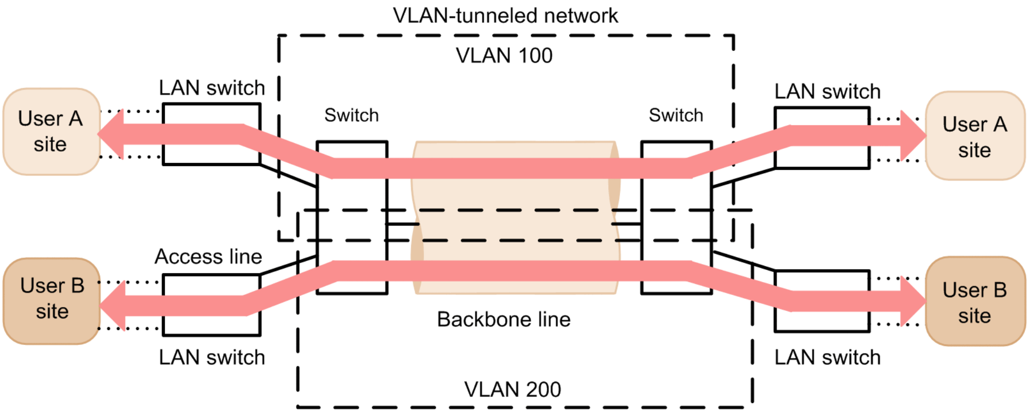
21.1.1 Overview

VLAN tunneling functionality aggregates, or tunnels, VLANs for multiple users into another VLAN. IEEE 802.1Q VLAN tags can be stacked to transparently forward frames belonging to other VLANs, within a single VLAN. Tunnels are capable of multipoint connections that connect three or more locations.

The figure below provides an overview of VLAN tunneling, including an example application of wide-area Ethernet service. With VLAN tunneling, VLAN tags can be stacked to distinguish VLANs within a VLAN-tunneled network.

This example application uses a Layer 2 VPN service, which is a wide-area Ethernet service. VLAN tunneling functionality is used for the Switch. With VLAN tunneling, VLAN tags can be stacked to distinguish VLANs within a VLAN-tunneled network. A port handling a user site is called an access line, and a port connected within the VLAN-tunneled network is called a backbone line. VLAN tags are added to frames from an access line, and the frames are then forwarded to the backbone line. Likewise, VLAN tags are removed from frames from a backbone line, and the frames are then forwarded to an access line.

Figure 21-1: VLAN tunneling overview (example wide-area Ethernet service application)



21.1.2 Requirements for using VLAN tunneling

The use of the VLAN tunneling functionality requires a network configured to meet all of the following conditions:

- A port VLAN is used.
- On the VLAN implementing the VLAN tunneling functionality, the tunneling port is on the access line, and the trunk port is on the backbone line.
- Because VLAN tags are stacked on the backbone line within the VLAN-tunneled network, frames that are 4 bytes larger than usual need to be handled.
- Access ports and tunneling ports cannot both exist within a switch. When at least one tunneling port is set, ports set as access ports also run as tunneling ports.

21.1.3 Notes on VLAN tunneling usage

(1) Notes on use with other functionality

For details, see *18.3 Compatibility between Layer 2 switch functionality and other functionality*.

(2) Default VLANs

Because default VLANs are not automatically installed, set all VLANs explicitly.

(3) Native VLANs for trunk ports

The trunk port for VLAN tunneling is the port that stacks VLAN tags, but VLAN tags are not stacked with a native VLAN. When frames are sent from the Switch, operation is the same as that for an access port, and when frames are received, only untagged frames are handled. Because this operation is different than other VLANs, native VLANs cannot be used as the VLAN for the backbone line of a VLAN-tunneled network. When VLAN tunneling is used, we recommend that you suspend the native VLAN for the trunk port.

The native VLAN for the trunk port is the default VLAN unless set otherwise using the `switchport trunk native vlan` configuration command. When using VLAN tunneling functionality for the default VLAN, use the `switchport trunk native vlan` command to set a VLAN other than the default VLAN for the native VLAN.

(4) User priority for frames

For details about user priority when VLAN tunneling is used, see *3.7 Description of marking* in the manual *Configuration Guide Vol. 2 For Version 11.10*.

21.2 Configuration of VLAN tunneling

21.2.1 List of configuration commands

The following table describes the configuration commands for VLAN tunneling.

Table 21-1: List of configuration commands

Command name	Description
switchport access	Sets an access line for a tunneling port.
switchport mode	Sets the port type for setting an access line or backbone line.
switchport trunk	Sets a backbone line.
mtu#	Sets jumbo frames for a backbone line.

#

For details, see *10. Ethernet* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.

21.2.2 Configuring VLAN tunneling

(1) Setting access lines and backbone lines

Points to note

The VLAN tunneling functionality uses a port VLAN to set an access line as a tunneling port, and a backbone line as a trunk port.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
```
Switches to the Ethernet interface configuration mode for port 1/0/1.

2.
```
(config-if)# switchport mode dot1q-tunnel
(config-if)# switchport access vlan 10
```
Sets port 1/0/1 as a tunneling port. Then, sets VLAN 10.

For details about trunk port configuration, see *20.4 Configuration of port VLANs*.

(2) Setting jumbo frames for backbone lines

Points to note

Because backbone lines stack VLAN tags, they handle frames at least 4 bytes larger than usual. Accordingly, jumbo frames need to be set.

Command examples

For details about jumbo frame configuration, see *16.2.5 Configuring jumbo frames*.

21.3 Description of tag translation

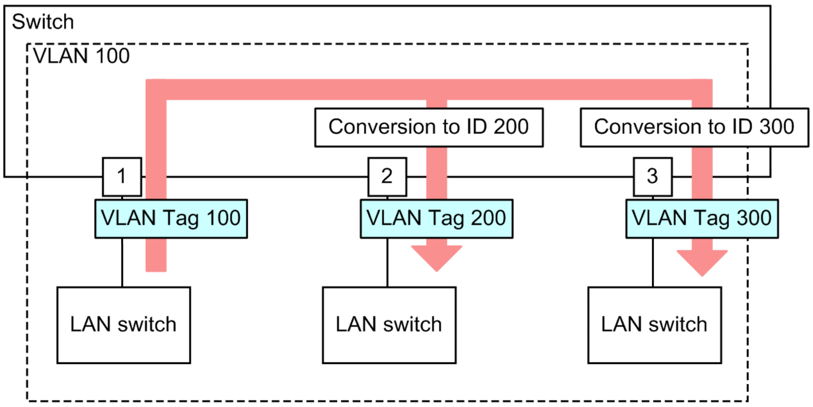
21.3.1 Overview

The tag translation functionality converts the VLAN ID field in the VLAN tag of a frame to another value when Layer 2 switch forwarding is performed for tagged frames. This functionality allows existing VLANs with different VLAN IDs set to be connected as a single VLAN.

The tag translation functionality is specified for the trunk port. When the tag translation functionality is not used, the VLAN ID of a given VLAN is used as the VLAN ID field of the VLAN tag. When the tag translation functionality is used, the ID is used.

The figure below shows an example configuration for the tag translation functionality. In the figure, the tag translation functionality is unspecified for port 1, but set for port 2 and port 3, so that the VLAN ID fields of VLAN tags are converted and their frames are forwarded. Also, when frames are received, those with VLAN tags whose ID is that set for each port are handled by VLAN 100.

Figure 21-2: Example configuration for tag translation



21.3.2 Notes on using tag translation

(1) Notes on use with other functionality

For details, see *18.3 Compatibility between Layer 2 switch functionality and other functionality*.

(2) TPIDs when tag translation is used

Do not set the TPID to a value other than 0x8100 for a port using tag translation.

21.4 Configuration of tag translation

21.4.1 List of configuration commands

The following table describes the configuration commands for tag translation.

Table 21-2: List of configuration commands

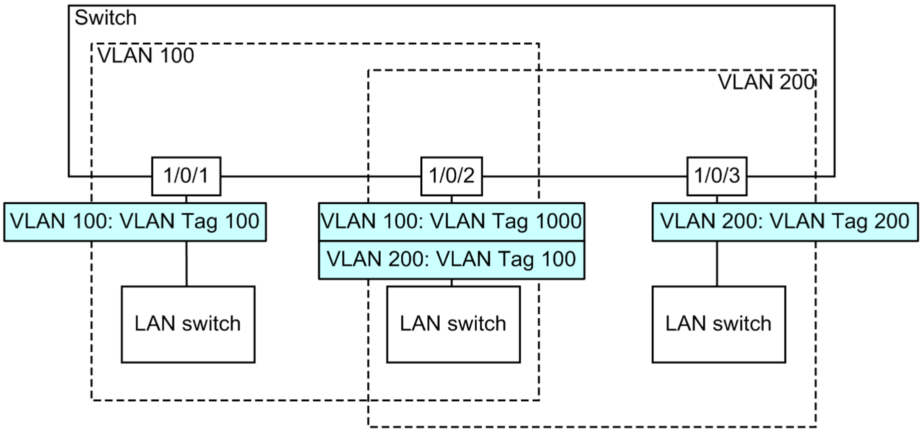
Command name	Description
switchport vlan mapping	Sets the ID to be converted.
switchport vlan mapping enable	Enables tag translation on the specified port.

21.4.2 Configuring tag translation

The figure below shows how tag translation is set. In the configuration in this example, port 1/0/2 is set.

In this example configuration, tag translation is applied to port 1/0/2. On port 1/0/2, I/O for VLAN 100 frames is performed using VLAN tag 1000, and I/O for VLAN 200 frames is performed using VLAN tag 100. This way, when tag translation is performed for VLAN 100, VLAN tag 100 can also be used for other VLANs. Also, VLAN tag 200 frames can be discarded as unset VLAN tags on port 1/0/2, instead of being handled as VLAN 200.

Figure 21-3: Example tag translation setting



Points to note

Tag translation works by enabling the tag translation functionality, and setting the ID to be converted. Tag translation settings only take effect for trunk ports.

Tag translation is set by the `switchport vlan mapping` command. Tag translation is enabled by the `switchport vlan mapping enable` command. When tag translation is enabled, frame I/O is stopped for VLANs for which translation is not set for the port.

Command examples

1.

```
(config)# interface gigabitethernet 1/0/2
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 100,200
```

Sets port 1/0/2 for the trunk port, and sets VLANs 100 and 200.

2.
```
(config-if)# switchport vlan mapping 1000 100
(config-if)# switchport vlan mapping 100 200
```

Sets tag translation on port 1/0/2 for VLANs 100 and 200. This sequence sets frames to be sent and received with VLAN tag 1000 on VLAN 100, and sent and received with VLAN tag 100 on VLAN 200.

3.
```
(config-if)# switchport vlan mapping enable
```

Enables tag translation on port 1/0/2. Tag translation is not enabled until this command is set.

Notes

Tag translation must be set on all VLANs of the ports for which tag translation is used. For VLANs for which translation is not performed, set translation to be performed to the same value. Note that the setting count for the capacity limits for tag translation is 768, including settings for translation to the same value.

21.5 Description of L2 protocol frame transparency functionality

21.5.1 Overview

L2 protocol frame transparency functionality forwards Layer 2 protocol frames. The frames that are forwarded include Spanning Tree BPDUs, and EAPOL for IEEE 802.1X. Usually, protocol frames for these layers are not forwarded.

The frames forwarded are handled as simple multicast frames on the Switch, and are not used as protocols by the Switch.

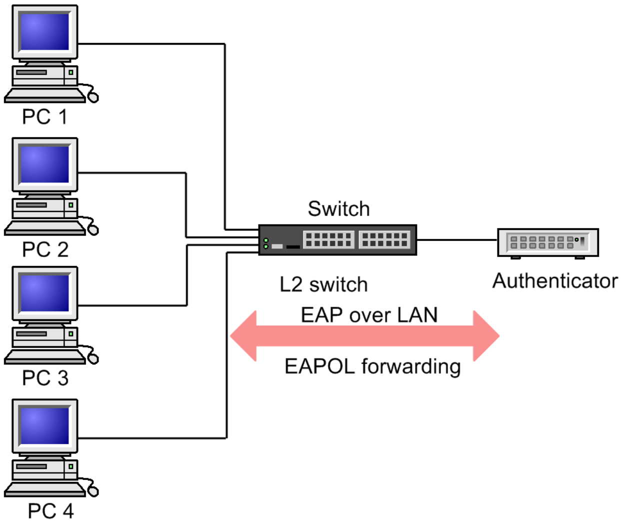
(1) BPDU forwarding functionality

The Switch can forward BPDUs when Spanning Tree Protocols are not used. When this functionality is used with VLAN tunneling, user BPDUs can be forwarded. In this case, BPDU forwarding functionality needs to be set for all edge switches and core switches on the VLAN-tunneled network.

(2) EAPOL forwarding functionality

The Switch can forward EAPOLs when IEEE 802.1X is not used. This functionality is used for the Switch when an L2 switch is used between the Authenticator and terminal (Supplicant).

Figure 21-4: Example application of EAPOL forwarding functionality



21.5.2 Notes on L2 protocol frame transparency functionality

(1) Notes on use with other functionality

For details, see *18.3 Compatibility between Layer 2 switch functionality and other functionality*.

21.6 Configuration of the L2 protocol frame transparency functionality

21.6.1 List of configuration commands

The following table describes the configuration commands for the L2 protocol frame transparency functionality.

Table 21-3: List of configuration commands

Command name	Description
l2protocol-tunnel eap	Forwards EAPOL frames for IEEE 802.1X.
l2protocol-tunnel stp	Forwards Spanning Tree BPDUs.

21.6.2 Configuring the L2 protocol frame transparency functionality

(1) Setting BPDU forwarding functionality

Points to note

The settings for this functionality take effect for each switch. When set, BPDUs are forwarded for all VLANs.

BPDU forwarding functionality needs to be set after stopping the Spanning Tree Protocol for the Switch.

Command examples

1.
```
(config)# spanning-tree disable
(config)# l2protocol-tunnel stp
```

Sets BPDU forwarding functionality. The Spanning Tree Protocol is stopped first, and then the BPDU forwarding functionality is set. The Switch forwards BPDUs without handling them as protocol frames.

(2) Setting EAPOL forwarding functionality

Points to note

The settings for this functionality take effect for each switch. When set, EAPOL frames are forwarded for all VLANs.

EAPOL forwarding functionality and IEEE 802.1X cannot be used at the same time.

Command examples

1.
```
(config)# l2protocol-tunnel eap
```

Sets EAPOL forwarding functionality. The Switch forwards EAPOL frames without handling them as protocol frames.

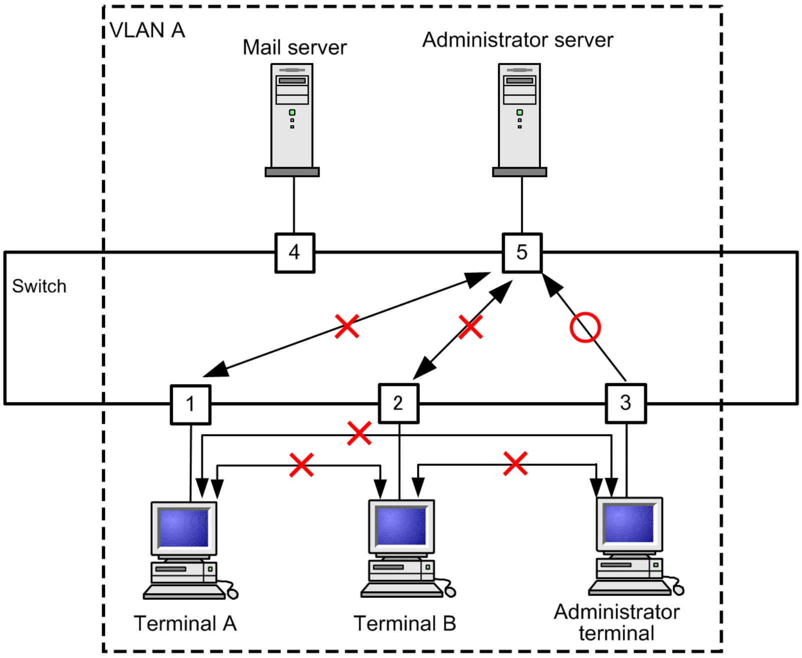
21.7 Description of the inter-port relay blocking functionality

21.7.1 Overview

The inter-port relay blocking functionality blocks communication on all specified ports. This can improve security when applied to connections with servers for which only access from specific ports is allowed, and connections with terminals for which direct communication is to be blocked.

The figure below shows an example application. In this example, administrator servers block access from normal terminals, allowing access only from other administrator servers. Also, direct communication between terminals is blocked, to enhance the security of each terminal.

Figure 21-5: Example application of inter-port relay blocking functionality



- The Switch permits communication only from the administrator terminal, blocking communication from other terminals.
- The Switch blocks direct communication between terminals.
- The Switch permits communication from all terminals to the mail server.

21.7.2 Notes on using the inter-port relay blocking functionality

(1) Notes on use with other functionality

For details, see *18.3 Compatibility between Layer 2 switch functionality and other functionality*.

(2) Blocking between ports with multiple VLANs set for a single port

The inter-port relay blocking functionality blocks all communications for both Layer 2 forwarding within a VLAN, and Layer 3 forwarding between VLANs. When communication is blocked between ports with multiple VLANs set on a single port, such as on a trunk port, Layer 3 forwarding between VLANs is also blocked between those ports.

(3) Note on use with Spanning Tree Protocols

When a Spanning Tree Protocol is run on a port that is blocking communication, communication might no longer be possible, depending on the topology.

21.8 Configuration of the inter-port relay blocking functionality

21.8.1 List of configuration commands

The following table describes the configuration command for the inter-port relay blocking functionality.

Table 21-4: List of configuration commands

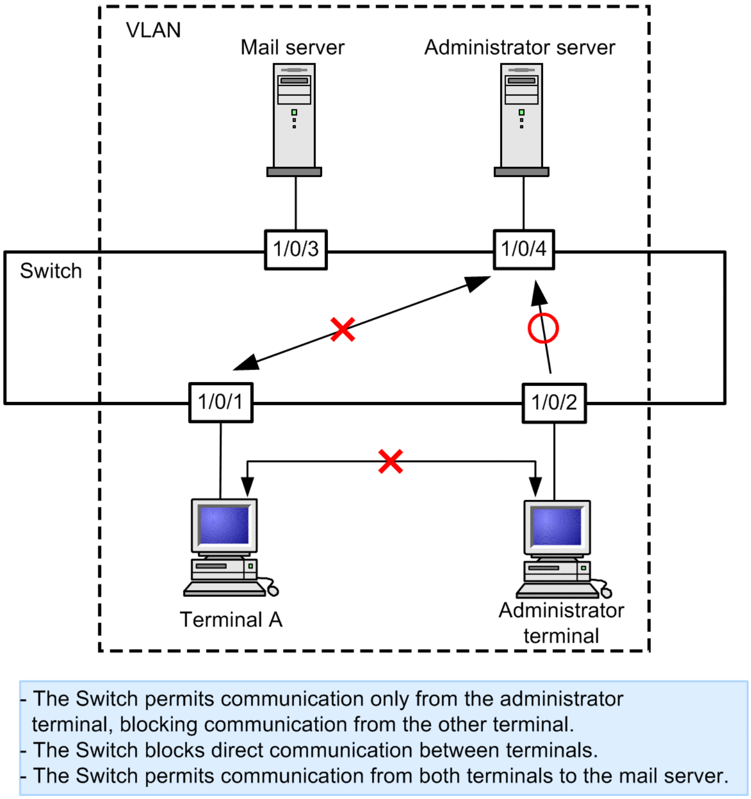
Command name	Description
switchport isolation	Blocks forwarding to the specified port.

21.8.2 Configuring the inter-port relay blocking functionality

The following describes how to set the inter-port relay blocking functionality. The example settings correspond to the configuration in the figure.

In the example configuration communication from port 1/0/1 to port 1/0/4 is blocked. Communication is also blocked between ports 1/0/1 and 1/0/2. Port 1/0/3 can communicate with any port.

Figure 21-6: Example settings for the inter-port relay blocking functionality



- The Switch permits communication only from the administrator terminal, blocking communication from the other terminal.
- The Switch blocks direct communication between terminals.
- The Switch permits communication from both terminals to the mail server.

Points to note

The inter-port relay blocking functionality is set using the Ethernet interface configuration mode by specifying a port to which communication from other ports is not allowed. For each port to be blocked, communication needs to be blocked in both directions.

Command examples

1. `(config)# interface gigabitethernet 1/0/1`

Switches to the Ethernet interface configuration mode for port 1/0/1.

2.
```
(config-if)# switchport isolation interface gigabitethernet 1/
0/2, gigabitethernet 1/0/4
(config-if)# exit
```

Blocks forwarding from ports 1/0/2 and 1/0/4 on port 1/0/1. With this setting, one-way forwarding is blocked for transmission from port 1/0/1.

3.
```
(config)# interface gigabitethernet 1/0/2
(config-if)# switchport isolation interface gigabitethernet 1/
0/1
(config-if)# exit
```

Switches to the Ethernet interface configuration mode for port 1/0/2, and blocks forwarding from port 1/0/1 on port 1/0/2. With this setting, communication is blocked both ways between ports 1/0/1 and 1/0/2.

4.
```
(config)# interface gigabitethernet 1/0/4
(config-if)# switchport isolation interface gigabitethernet 1/
0/1
```

Switches to the Ethernet interface configuration mode for port 1/0/4, and blocks forwarding from port 1/0/1 on port 1/0/4. With this setting, communication is blocked both ways between ports 1/0/1 and 1/0/4.

21.8.3 Changing blocked ports

Points to note

The `switchport isolation add` command and `switchport isolation remove` command are used to change the ports blocked by the inter-port relay blocking functionality. When `switchport isolation` <*interface-id list*> is used to batch specify ports already set, the specified settings are replaced.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# switchport isolation interface gigabitethernet 1/
0/2-10
```

Switches to the Ethernet interface configuration mode for port 1/0/1, and blocks forwarding from port 1/0/1 to ports 1/0/2 to 1/0/10.

2.
```
(config-if)# switchport isolation interface add
gigabitethernet 1/0/11
(config-if)# switchport isolation interface remove
gigabitethernet 1/0/5
```

Adds port 1/0/11 to the ports blocked from port 1/0/1, and removes the port 1/0/5 setting. Port 1/0/1 now blocks communication to ports 1/0/2 to 1/0/4 and 1/0/6 to 1/0/11.

3. `(config-if)# switchport isolation interface gigabitethernet 1/0/3-4`

   Sets forwarding from port 1/0/1 to be blocked for ports 1/0/3 to 1/0/4. All previous settings are overwritten, only ports 1/0/3 to 1/0/4 are blocked, and communication remains possible on other ports.

21.9 Description of the VLAN Debounce functionality

21.9.1 Overview

A VLAN interface goes up when communication is possible for the VLAN, and goes down when the VLAN port goes down, or a Spanning Tree Protocol or other functionality causes blocking and prevents communication.

The VLAN Debounce functionality delays when VLAN interfaces go up or down, to reduce network topology changes, log messages, and SNMP traps.

When failure occurs for redundant configurations using a Spanning Tree Protocol or Ring Protocol on a Layer 2, the time required to switch routes is less than a normal Layer 3 topology change. The VLAN Debounce functionality keeps the VLAN interface from going down for the time that it takes to switch routes on the layer, which preserves communication availability without changing the Layer 3 topology.

When a redundant configuration is used for Layer 3, and recovery is performed after failure occurs on the master, the VLAN Debounce functionality can be used to delay when the VLAN interface goes up, which prevents both nodes from running as the master.

21.9.2 Relationship between the VLAN Debounce functionality and other functionality

(1) Spanning Tree Protocols

With Spanning Tree Protocols, the time required to change the Spanning Tree topology elapses before failure occurs on the port and it is switched to the alternate route. To prevent the VLAN interface from going down during this interval, set the VLAN interface down-determination time to a value greater than or equal to the time required to change the topology.

(2) Ring Protocol

When the Ring Protocol is used, the primary port is forwarded and the secondary port is blocked on the master node. If the VLAN Debounce functionality is not used and a failure occurs on the primary port, the VLAN interface goes down immediately, and goes back up once blocking is removed on the secondary port.

To prevent the VLAN from going down immediately in cases like this, set the VLAN interface down-determination time to a value greater than or equal to the protection time set by the `health-check holdtime` command.

(3) Other redundancy functionality

Even when redundancy functionality other than a Spanning Tree Protocol or Ring Protocol is used, when a VLAN repeatedly goes up and down in short intervals, the VLAN Debounce functionality can be used to suppress these events.

21.9.3 Notes on using the VLAN Debounce functionality

(1) Notes on the down-determination time

When a down-determination time is set, the time at which VLANs a VLAN goes down is delayed even when an unrecovered failure occurs. Because communication is not possible during these kinds of delays caused by the VLAN Debounce functionality, set the required value according to the network configuration and operational requirements.

When VLAN communication is no longer possible without a configuration change, such as when `suspend` is set for a VLAN by the `status` command, or all VLAN ports are deleted, the time that the VLAN goes down will not be delayed, even when a down-determination time is set.

(2) Notes on the up-determination time

When an up-determination time is set, if a VLAN that is already up goes down, the time at which it goes back up is delayed. Because a VLAN is initialized when the switch is restarted or the VLAN program is restarted by the `restart vlan` command, the time that the VLAN goes up will not be delayed, even when an up-determination time is set.

(3) Notes on lags in determination time

Because a software timer is used for the up and down determination times, the actual determination times might be greater than the time set when CPU usage is high.

21.10 Configuration of the VLAN Debounce functionality

21.10.1 List of configuration commands

The following table describes the configuration commands for the VLAN Debounce functionality.

Table 21-5: List of configuration commands

Command name	Description
down-debounce	Specifies the down-determination time for the VLAN interface.
up-debounce	Specifies the up-determination time for the VLAN interface.

21.10.2 Configuring the VLAN Debounce functionality

The following describes how to set the VLAN Debounce functionality.

Points to note

Set the VLAN Debounce functionality determination time to values appropriate to the configuration and operation of the network.

Command examples

1.
```
(config)# interface vlan 100
```
Switches to the VLAN interface mode for VLAN 100.

2.
```
(config-if)# down-debounce 2
(config-if)# exit
```
Sets the down-determination time for VLAN 100 to 2 seconds.

3.
```
(config)# interface range vlan 201-300
```
Switches to the multiple VLAN interface mode for VLANs 201 to 300.

4.
```
(config-if-range)# down-debounce 3
(config-if-range)# exit
```
Sets the down-determination time for VLANs 201-300 to 3 seconds.

21.11 Description of the Layer 2 relay blocking functionality

21.11.1 Overview

The Layer 2 relay blocking functionality only performs Layer 3 forwarding on the Switch. It does not perform Layer 2 forwarding. When this functionality is used, Layer 2 forwarding is not performed for any frames within the VLAN, including broadcast frames and multicast frames.

This functionality is useful for isolating communication between terminals, such as in a hotel or apartment building. It also assists IP address utilization when set to handle multiple terminals on a single VLAN.

21.12 Configuration of the Layer 2 relay blocking functionality

21.12.1 List of configuration commands

The following table describes the configuration command for the Layer 2 relay blocking functionality.

Table 21-6: List of configuration commands

Command name	Description
l2-isolation	Blocks Layer 2 forwarding within a VLAN.

21.12.2 Configuring the Layer 2 relay blocking functionality

The following describes how to set the Layer 2 relay blocking functionality.

Command examples

1.
```
(config)# l2-isolation
```
   Sets the Layer 2 relay blocking functionality.

21.13 Operation for the VLAN extended functionality

21.13.1 List of operation commands

The following table describes the operation command for the VLAN extended functionality.

Table 21-7: List of operation commands

Command name	Description
show vlan	Checks the status of the settings for the VLAN extended functionality.

21.13.2 Checking VLAN extended functionality

(1) Checking the status of VLAN communication

The status of the settings for the VLAN extended functionality can be checked by using the `show vlan detail` command. The following table describes how to use the `show vlan detail` command to check the VLAN extended functionality.

Table 21-8: Using the show vlan detail command to check the VLAN extended functionality

Functionality	How to check
VLAN tunneling	`VLAN tunneling enabled` is displayed at the beginning of the results.
Tag translation	`Tag-Translation` is displayed for `Port Information`.
L2 protocol frame transparency functionality	Information is displayed in `BPDU Forwarding` and `EAPOL Forwarding`.

Figure 21-7: Results of executing the show vlan detail command

```
>show vlan 10 detail
Date 20XX/10/15 16:28:23 UTC
VLAN counts:1   VLAN tunneling enabled                                   ...1
VLAN ID:10    Type:Port based      Status:Up
  Learning:On            Tag-Translation:On
  BPDU Forwarding:On     EAPOL Forwarding:                               ...3
             .
             .
             .
             .
  Port Information
   1/0/5          Up   Forwarding      Tagged   Tag-Translation:1000    ...2
   1/0/6          Down -               Tagged   Tag-Translation:2000    ...2
   1/0/7          Up   Forwarding      Tagged
>
```

1. Indicates that VLAN tunneling is enabled.
2. Indicates that tag translation is set for this port.
3. Indicates that BPDU forwarding functionality is set and EAPOL forwarding functionality is not set.

Chapter

22. Spanning Tree Protocols

This chapter describes the Spanning Tree functionality and its use.

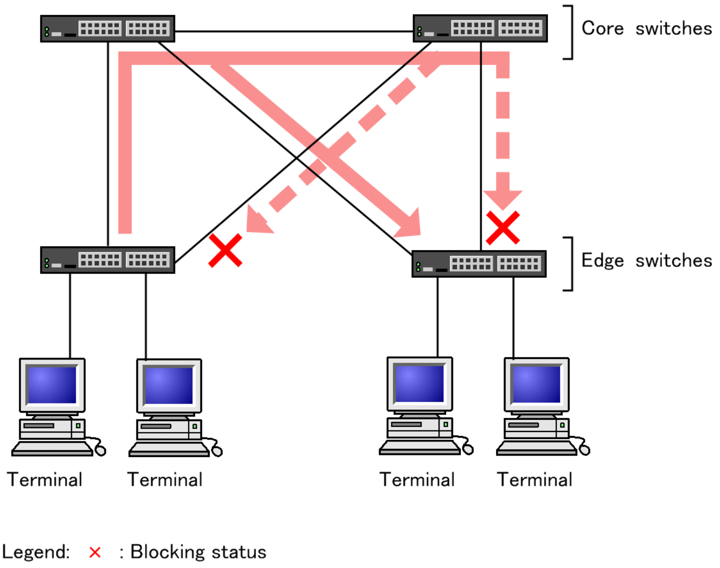
22.1 Overview of Spanning Tree Protocols

22.1.1 Overview

The Spanning Tree Protocol is a Layer 2 loop prevention protocol. The Spanning Tree Protocol can be used to make Layer 2 networks redundant, and prevent loops.

The following figure provides an overview of a network with a Spanning Tree Protocol applied.

Figure 22-1: Overview of a network with a Spanning Tree Protocol applied



In the configuration in the diagram, the switches responsible for the network core are made redundant, as are the communication paths from the edge switch handling the terminals. By making the switches and communication paths redundant, transmission can carry over to an alternate path when a fault occurs on the normal communication path.

A Layer 2 loop configuration is one in which a Layer 2 network is made redundant. Layer 2 loops cause broadcast storms and destabilize MAC address learning. Spanning Tree Protocols are protocols that prevent loops on Layer 2 networks in redundant loop configurations, by choosing locations in which to stop communication, and putting them in `Blocking` status.

22.1.2 Types of Spanning Tree Protocols

The Switch supports three types of Spanning Tree Protocols: PVST+, Single Spanning Tree, and Multiple Spanning Tree. Each Spanning Tree Protocol is built differently. The following table provides an overview of the types of Spanning Tree Protocols.

Table 22-1: Types of Spanning Tree Protocols

Name	Build unit	Overview
PVST+	Per-VLAN	This kind of tree is built per VLAN. If multiple VLANs belong to a single port, different tree build results are applied to each VLAN.
Single Spanning Tree	Per-switch	This kind of tree is built with all ports on the switch as targets. The tree build results are applied to all ports on the switch regardless of the VLAN configuration.

Name	Build unit	Overview
Multiple Spanning Tree	Per-MST-instance	This kind of Spanning Tree Protocol is built by groups of multiple VLANs, called MST instances. If multiple VLANs belong to a single port, different tree build results are applied to each MST instance.

The Switch allows the above Spanning Tree Protocols to be used as standalone or together. The following table describes which Spanning Tree combinations can be applied.

Table 22-2: Spanning Tree combinations and applicability

Tree building condition	Applicable topology calculation results
Standalone PVST+	A Spanning Tree Protocol for each VLAN is applied to VLANs for which PVST+ is running. The Spanning Tree Protocol is not applied to other VLANs. PVST+ runs by default on port VLANs for the Switch.
Standalone Single Spanning Tree	Single Spanning Tree is applied to all VLANs. All PVST+ instances are stopped in this configuration.
Combination of PVST+ and Single Spanning Tree	A Spanning Tree Protocol for each VLAN is applied to VLANs for which PVST+ is running. Single Spanning Tree is applied to other VLANs.
Standalone Multiple Spanning Tree	Multiple Spanning Tree is applied to all VLANs.

Note: Multiple Spanning Tree cannot be used in combination with other trees.

22.1.3 Spanning Tree Protocols and rapid Spanning Tree Protocols

There are two types of PVST+ and Single Spanning Tree: IEEE 802.1D Spanning Tree Protocols and IEEE 802.1w rapid Spanning Tree Protocols. These are called PVST+ and Rapid PVST+, and STP and Rapid STP.

When a communication path changes, the topology calculation for the Spanning Tree Protocol immediately puts the port in `Blocking` status (communication is not possible), switches to multiple statuses, and then puts it in `Forwarding` status (communication is possible). Because IEEE 802.1D Spanning Tree Protocols perform this status transition by a timer, a set time is required until communication is possible. IEEE 802.1w rapid Spanning Tree Protocols omit this timer-based waiting time for status transitions to perform high-speed status transitions, minimizing the time for which communication stops due to topology changes.

Note that because Multiple Spanning Tree is standardized under IEEE 802.1s, the status transition times is the same as for IEEE 802.1w. The following table describes the status transitions for each protocol, and their corresponding required times.

Table 22-3: Status transitions for PVST+ and STP (Single Spanning Tree)

Status	Status overview	Transition to the next status
Disable	Status in which a port cannot be used. This transitions to `Blocking` as soon as the port becomes available.	--
Blocking	Status in which communication is not possible. In this status, MAC address learning is not performed. This is the status after link-up or of ports after topology stabilization and blocking.	20 seconds (variable) or until BPDU reception
Listening	Status in which communication is not possible. In this status, MAC address learning is not performed. This is the duration until the topology stabilizes before the corresponding port is learned.	15 seconds (variable)

Status	Status overview	Transition to the next status
Learning	Status in which communication is not possible. In this case, however, MAC address learning is performed. This is the duration for which MAC address learning is performed before the corresponding port transitions to `Forwarding`.	15 seconds (variable)
Forwarding	Status in which communication is possible. In this case, the topology is stable.	--

Legend: --: Not applicable

Table 22-4: Status transitions for Rapid PVST+ and Rapid STP (Single Spanning Tree)

Status	Status overview	Transition to the next status
Disable	Status in which a port cannot be used. This transitions to `Discarding` as soon as the port becomes available.	--
Discarding	Status in which communication is not possible. In this status, MAC address learning is not performed. This is the duration until the topology stabilizes before the corresponding port is learned.	Omitted or 15 seconds (variable)
Learning	Status in which communication is not possible. In this case, however, MAC address learning is performed. This is the duration for which MAC address learning is performed before the corresponding port transitions to `Forwarding`.	Omitted or 15 seconds (variable)
Forwarding	Status in which communication is possible. In this case, the topology is stable.	--

Legend: --: Not applicable

With Rapid PVST+ and Rapid STP, the `Discarding` and `Learning` statuses are skipped by BPDU reception from the partner switch. This enables high-speed topology changes.

When using a rapid Spanning Tree Protocol, set it according to the conditions described below. If these conditions are not satisfied, discarding and learning might not be skipped, and high-speed status transitions might not be performed.

- The entire topology is built using the same protocol (Rapid PVST+ or Rapid STP). For details about reciprocal connections for Rapid PVST+ and Rapid STP, see *22.3.2 PVST+ for access ports*.
- Point-to-Point connections are used between switches running for the Spanning Tree Protocol.
- PortFast is set on ports not connected to switches running for the Spanning Tree Protocol.

22.1.4 Configuration components for Spanning Tree topologies

Designing a Spanning Tree topology involves roles for bridges and ports, as well as parameters used to determine these roles. The following explains usage for these configuration components and topology designs.

(1) Bridge role

The table below describes bridge roles. Spanning Tree topology design starts with determining the root bridge.

Table 22-5: Bridge roles

Bridge role	Overview
Root bridge	The switch at the logical center of a built topology. There can only be one within a topology.
Designated bridge	A switch other than the root bridge for forwarding frames from the root bridge.

(2) Port role

The table below describes port roles. Ports on designated bridges have three types of roles. For root bridges, all ports are designated ports.

Table 22-6: Port roles

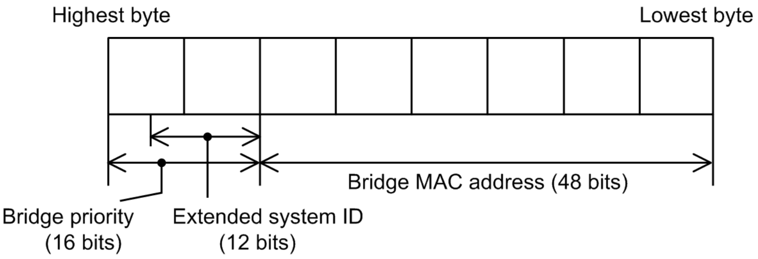
Port role	Overview
Root port	A port for a communication path from a designated bridge to the root bridge. This port allows communication.
Designated port	A port, other than the root port, for which communication is possible. It allows communication downstream from the root bridge to other ports in the topology.
Non-designated port	A port other than a root port or designated port, for which communication is not possible. It serves as an alternate path when a fault occurs.

(3) Bridge ID

Each switch in a topology is identified by a parameter called a bridge ID. The switch that has the lowest bridge ID has the highest priority, and is selected as the root bridge.

Bridge IDs consist of a bridge priority (16 bits) and the bridge MAC address (48 bits). The lowest 12 bits of a bridge priority is the extended system ID. For an extended system ID, 0 is set for Single Spanning Tree or Multiple Spanning Tree, and the VLAN ID is set for PVST+. The following figure shows a bridge ID.

Figure 22-2: Bridge ID



(4) Path cost

A value corresponding to the communication speed of each port on a switch is called the path cost. The total value of the port costs for all intermediate ports from a designated bridge to the root bridge is called the root path cost. If there are multiple paths to the root bridge, the root path cost is that of the shortest path.

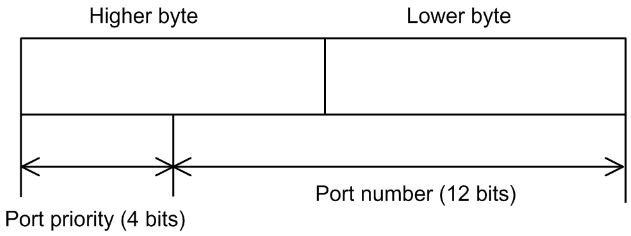
We recommend lowering the path cost to that of a fast port. The default value of the path cost corresponds to the speed of the port, but can also be changed in the configuration.

(5) Port ID

Each port in a switch is identified by a parameter called a port ID. Port IDs are used to select a communication path when two or more redundant connections exist between two switches, and the path cost cannot be changed for each port. Note that when redundant connections are used between two switches, we recommend using link aggregation. Use a Spanning Tree Protocol to enable redundant connections between switches that do not support link aggregation.

Port IDs consist of a port priority (4 bits) and a port number (12 bits). The following figure shows a port ID.

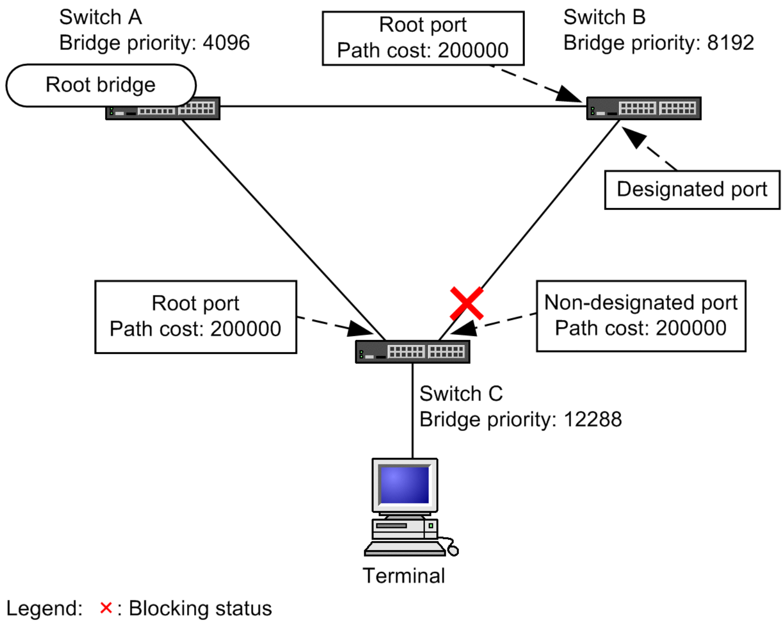
Figure 22-3: Port ID



22.1.5 Designing Spanning Tree topologies

The topology of a Spanning Tree Protocol is based on the bridge ID and path cost. The figure below shows the basic procedures for designing a topology. In the example configuration in the figure, two core switches are used for redundancy, placed to handle terminals as edge switches.

Figure 22-4: Designing Spanning Tree topologies



(1) Selecting the root bridge by bridge IDs

The switch with the lowest bridge ID is chosen as the root bridge. Normally, you set the bridge priority of the switch that you want to be the root bridge to the lowest value (highest priority). In the example in the figure, Switch A is the root bridge, and Switch B and Switch C are designated bridges.

Note that Switch B will become the alternate root bridge if a fault occurs on the root bridge. Switch C is set as the lowest priority.

For the design of a Spanning Tree topology, we recommend configurations that follow the example in the figure of setting the switch handling the network core as the root bridge and using alternate root bridges to make the core redundant.

(2) Designing communication paths

After a root bridge is determined, the communication paths from each designated bridge to the root bridge are determined.

(a) Selecting the root port based on path cost

For Switch B and Switch C, the path to the root bridge is determined by finding the lowest root path cost value. In the example in the figure, the path cost for all ports is 200000. Among the directly connected ports, the one with the lowest root path cost is chosen as the root port.

The root path cost of a path from a designated bridge to the root bridge is calculated by comparing the total path cost of the outgoing ports bound for the root bridge for each switch. For example, because the path cost of the path passing through Switch B for Switch C is 400000, it is not chosen for the root port.

The default cost for a path is the smallest value, which is based on the fastest port speed. In addition, the root port is determined by comparing root path costs. Therefore, you normally do not need to make changes to path costs to prioritize the use of paths with fast ports or the minimum of intermediate switches. To prioritize paths than have slow ports over paths than have fast ports, change the configuration to design paths for which communication is performed.

(b) Selecting designated ports and non-designated ports

Ports other than the root port are used for the connection between Switch B and Switch C. One or more of these ports are non-designated ports and are placed in `Blocking` status. This is how Spanning Tree Protocols use the `Blocking` status on a given side to prevent loops.

Designated ports and non-designated ports are chosen as follows:

- The port on the switch with the lowest root path cost between switches is the designated port, and ports on higher cost switches are non-designated ports.
- If root path costs are the same, the port on the switch that has the smaller bridge ID is the designated port, and ports on switches that have larger IDs are non-designated ports.

In the example in the figure, the root path costs are the same. According to the bridge priority, Switch B has the designated port and Switch C has the non-designated port, which is placed in `Blocking` status. To change the port of Switch B to `Blocking` status, set the path costs so that the root path cost of Switch B increases.

22.1.6 STP compatibility mode

(1) Overview

For a switch using Rapid PVST+, Rapid STP, or Multiple Spanning Tree, if the partner switch uses PVST+ or STP, the corresponding port runs in STP compatibility mode.

Under STP compatibility mode operation, high-speed transitions can no longer be performed on the corresponding port, requiring more time for communication to be restored.

If the partner switch is changed to a Rapid PVST+, Rapid STP, or Multiple Spanning Tree, restoration is performed from the STP compatibility mode, and high-speed transitions become possible again, but depending on the timing, the corresponding port and partner switch might continue to run in STP compatibility mode.

The STP compatibility mode recovery functionality performs forced restoration for ports running in STP compatibility mode, allowing them to perform normal high-speed transition.

(2) Restoration functionality

The `clear spanning-tree detected-protocol` operation command can be executed to perform forced restoration from STP compatibility mode. The link type of the corresponding port can be either point-to-point or shared.

(3) Automatic-restoration functionality

If the link type of the corresponding port is point-to-point, the STP compatibility mode recovery functionality runs automatically.

If the corresponding port is a non-designated port running in STP compatibility mode, an RST BPDU or MST BPDU can be sent from the corresponding port to disable STP compatibility mode.

If the link type of the corresponding port is shared, automatic-restoration mode does not run, because it cannot run correctly.

22.1.7 Notes common to Spanning Tree Protocols

(1) CPU overloading

If the CPU is overloaded, the BPDUs sent and received by the Switch are discarded, a timeout message might be output, the topology might change, and communication might be temporarily cut off.

(2) Specifying configuration commands that disable VLANs

When the `no spanning-tree disable` configuration command is used to enable the Spanning Tree functionality for the Switch, all VLANs temporarily go down.

22.2 Configuration of the Spanning Tree operating mode

The following explains settings for the Spanning Tree operating mode.

If the Switch starts without a configuration being set, it runs in the `pvst` operating mode.

22.2.1 List of configuration commands

The following table describes the configuration commands for the Spanning Tree operating mode.

Table 22-7: List of configuration commands

Command name	Description
spanning-tree disable	Stops the Spanning Tree functionality.
spanning-tree mode	Sets the operating mode for Spanning Tree functionality.
spanning-tree single mode	Selects STP and Rapid STP for Single Spanning Tree.
spanning-tree vlan mode	Selects PVST+ and Rapid PVST+ for each VLAN.

22.2.2 Configuring the operating mode

The operating mode of a switch can be set so that various Spanning Tree Protocols can be used. The table below describes the switch operating modes. If no operating mode is set, operation is performed in pvst mode.

Keep in mind that when `rapid-pvst` is specified for the operating mode, the Single Spanning Tree default is STP.

Table 22-8: Spanning Tree operation modes

Command name	Description
spanning-tree disable	Disables the Spanning Tree Protocol.
spanning-tree mode pvst	Allows Single Spanning Tree to be used with PVST+. PVST+ is used for operation by default. Single Spanning Tree does not run by default.
spanning-tree mode rapid-pvst	Allows Single Spanning Tree to be used with PVST+. Rapid PVST+ for a rapid Spanning Tree Protocol runs by default. Single Spanning Tree does not run by default.
spanning-tree mode mst	Runs Multiple Spanning Tree.

(1) Setting the pvst operation mode

Points to note

The example below shows how to set the switch operating mode to `pvst`. When a port VLAN is created, PVST+ is automatically run on the VLAN. Each VLAN can be changed to Rapid PVST+.

Single Spanning Tree does not run by default, but can run through settings. Operation uses STP by default, but can be changed to Rapid STP.

Command examples

1. `(config)# spanning-tree mode pvst`

   Sets the Spanning Tree operating mode to `pvst`. PVST+ is automatically run for port VLANs.

2. `(config)# spanning-tree vlan 10 mode rapid-pvst`

Changes the operating mode of VLAN 10 to Rapid PVST+. Other port VLANs are run using PVST+, and VLAN 10 runs using Rapid PVST+.

3. `(config)# spanning-tree single`

   Runs Single Spanning Tree. This is applied to VLANs for which PVST+ is not used. By default, STP is used for operation.

4. `(config)# spanning-tree single mode rapid-stp`

   Changes Single Spanning Tree to Rapid STP.

(2) Setting the rapid-pvst operating mode

Points to note

The example below shows how to set the switch operating mode to `rapid-pvst`. When a port VLAN is created, Rapid PVST+ is automatically run on the VLAN. Each VLAN can be changed to PVST+.

Single Spanning Tree does not run by default, but can run through settings. Keep in mind that when `rapid-pvst` is specified for the operating mode, the Single Spanning Tree default is STP.

Command examples

1. `(config)# spanning-tree mode rapid-pvst`

   Sets the Spanning Tree operating mode to `rapid-pvst`. Rapid PVST+ is automatically run for port VLANs.

2. `(config)# spanning-tree vlan 10 mode pvst`

   Changes the operating mode of VLAN 10 to PVST+. Other port VLANs are run using Rapid PVST+, and VLAN 10 runs using PVST+.

3. `(config)# spanning-tree single`

   Runs Single Spanning Tree. This is applied to VLANs for which PVST+ is not used. By default, STP is used for operation.

4. `(config)# spanning-tree single mode rapid-stp`

   Changes Single Spanning Tree to Rapid STP.

(3) Setting the mst operating mode

Points to note

When Multiple Spanning Tree is used, set the switch operating mode to `mst`. Multiple Spanning Tree is applied to all VLANs. When Multiple Spanning Tree is used, PVST+ and Single Spanning Tree cannot be used together.

Command examples

1. `(config)# spanning-tree mode mst`

Runs Multiple Spanning Tree.

(4) Stopping Spanning Tree Protocols

Points to note

If Spanning Tree Protocols are not used, `disable` can be set to stop all Spanning Tree Protocols on the Switch.

Command examples

1.
```
(config)# spanning-tree disable
```

Stops all Spanning Tree operation.

22.3 Description of PVST+

PVST+ builds a tree for each VLAN. These trees can be used for load balancing. In addition, access ports can be used to connect with switches running on Single Spanning Tree.

22.3.1 Using PVST+ to balance load

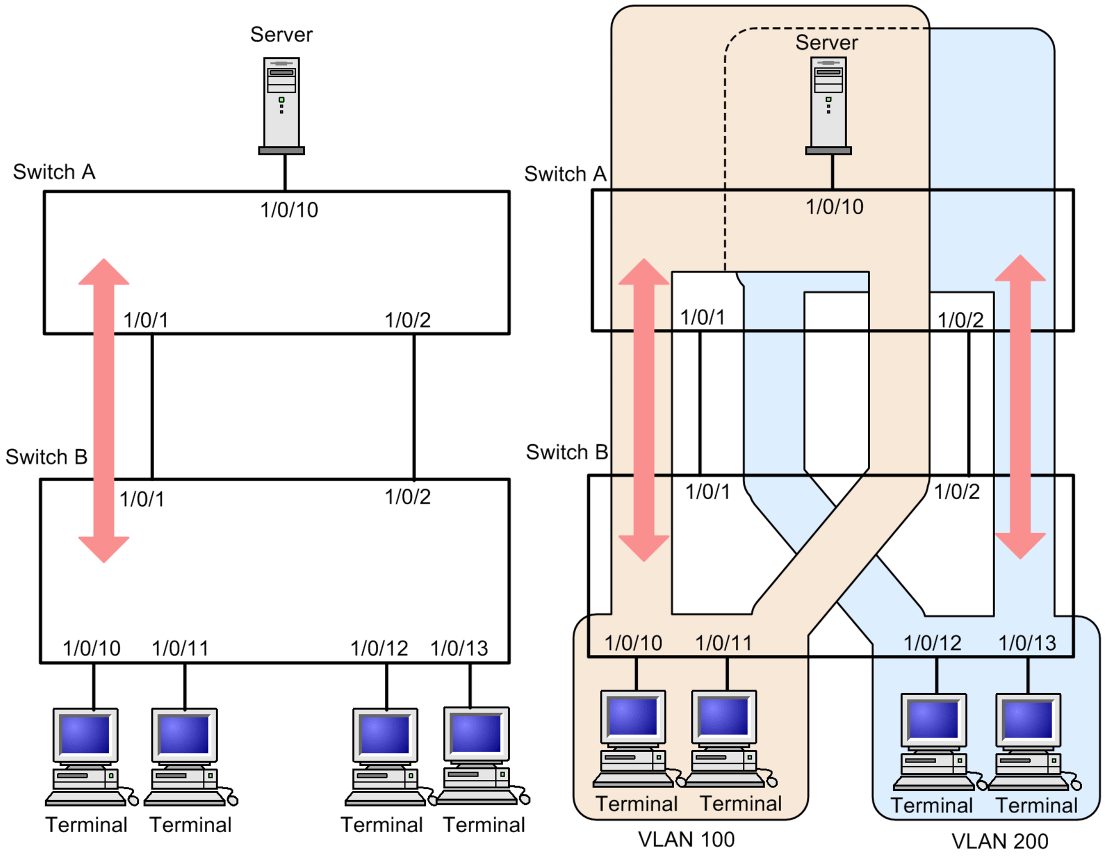
When Single Spanning Tree is used in a network that has redundant paths between switches, such as Switch A and Switch B in the figure below, access from each terminal to the server is concentrated on port 1 between Switches A and B. In this case, PVST+ can be used to set up multiple VLANs that have different topologies in order to create redundant paths, which would allow the load to be distributed. The figure below shows an example of load balancing by port priority.

In this example, the port priority for VLAN 100 is set higher for port 1/0/1 than port 1/0/2, whereas the port priority for VLAN 200 is set higher for port 1/0/2 than port 1/0/1, allowing access from each terminal to the server to be load-balanced for each VLAN.

Figure 22-5: Using PVST+ to balance load

(1) In Single Spanning Tree, because port 1/0/2 is not normally used as a redundant path, the load is concentrated on port 1/0/1.

(2) Separate topologies can be used for each VLAN with PVST+, to balance the load between Switches A and B.



22.3.2 PVST+ for access ports

(1) Description

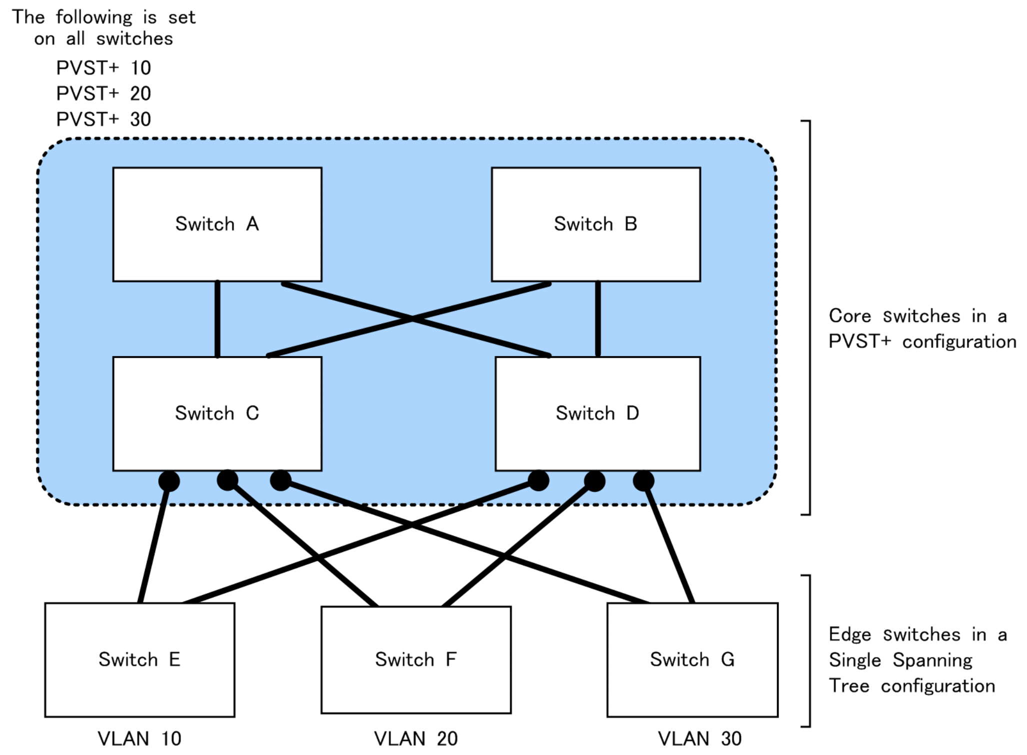
A network can be built using switches that use Single Spanning Tree and switches that support Single Spanning Tree functionality for one tree (abbreviated hereafter simply as Single Spanning Tree) and PVST+. Switches running on Single Spanning Tree are used as edge switches, and

Switches are used for core switches. This kind of network configuration has the following advantages:

- Problems that occur on an edge switch for not result in topology changes for other edge switches.
- Load balancing can be performed among core switches.

Single Spanning Tree is connected by access ports. The figure below shows a configuration example. In this example, Single Spanning Tree runs on the edge switches, and PVST+ runs on the core switches. The core switches treat ports connected to edge switches as access ports. A single VLAN is set up for each edge switch.

Figure 22-6: Connecting to Single Spanning Tree


The following is set on all switches
PVST+ 10
PVST+ 20
PVST+ 30
Switch A
Switch B
Switch C
Switch D
Core switches in a PVST+ configuration
Switch E
Switch F
Switch G
Edge switches in a Single Spanning Tree configuration
VLAN 10
VLAN 20
VLAN 30

When a fault occurs on switch E, because the core switches use PVST+, topology change notifications are not sent to switches F and G.

Legend: ●: Access port

(2) When PVST+ and Single Spanning Tree coexist on access ports

When PVST+ and Single Spanning Tree coexist, Single Spanning Tree stops (switched to `Disable` status) on the access port.

(3) Configuration-inconsistency detection functionality

For ports connected on the same VLAN, if an access port, protocol port, or MAC port is set for the Switch (using an untagged frame), and a trunk port is set for the partner switch (using a tagged frame), communication for this port will not be possible for the corresponding VLAN. Ports like these are detected as configuration mismatches. This mismatch is detected if the Switch has an access port, and the trunk port is set on the partner switch (using a tagged frame). In this case, the corresponding port stops (`Disable` status). If the trunk port setting (using a tagged frame) is deleted on the partner switch, the stopped status is automatically removed after *hello-time* x 3 seconds (six seconds by default).

22.3.3 Notes on PVST+ usage

(1) Notes on use with other functionality

For details, see *18.3 Compatibility between Layer 2 switch functionality and other functionality*.

(2) VLAN 1 (default VLAN) PVST+ and Single Spanning Tree

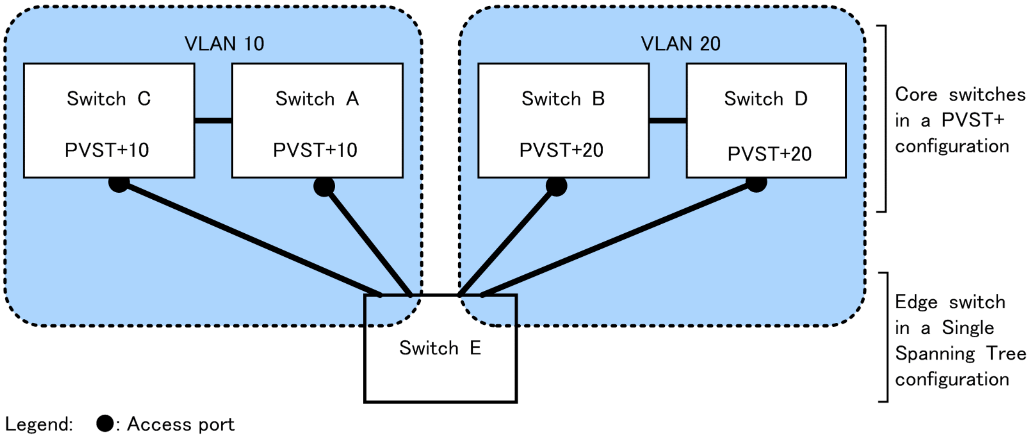
Single Spanning Tree and VLAN 1 PVST+ cannot run at the same time. When Single Spanning Tree runs, the VLAN 1 PVST+ stops.

(3) Prohibited configurations

Configure the Switch and switches running on Single Spanning Tree within one Spanning Tree. Configurations using more than one Spanning Tree will not result in a valid topology.

The figure below shows an example of a prohibited configuration. In this example, because the switch E Single Spanning Tree is connected to more than one PVST+ Spanning Tree, the topology is not valid.

Figure 22-7: Example prohibited configuration with Single Spanning Tree



Because switch E does not consist of a Single Spanning Tree, the topology is invalid.

22.4 PVST+ configuration

22.4.1 List of configuration commands

The following table describes the configuration commands for PVST+.

Table 22-9: List of configuration commands

Command name	Description
spanning-tree cost	Sets the default path cost value for each port.
spanning-tree pathcost method	Sets the default value for the margin of values used for path costs for a port.
spanning-tree port-priority	Sets the default value for the port priority for each port.
spanning-tree vlan	Sets PVST+ starting and stopping operation.
spanning-tree vlan cost	Sets the path cost value for a VLAN.
spanning-tree vlan forward-time	Sets the time required for port status transitions.
spanning-tree vlan hello-time	Sets the sending interval for BPDUs.
spanning-tree vlan max-age	Sets the maximum enabled time for sent BPDUs.
spanning-tree vlan pathcost method	Sets the margin of values used for path costs for a VLAN.
spanning-tree vlan port-priority	Sets the port priority for a VLAN.
spanning-tree vlan priority	Sets the bridge priority.
spanning-tree vlan transmission-limit	Sets the maximum number of BPDUs that can be sent per *hello-time* interval.

22.4.2 Configuring PVST+

Points to note

When the `pvst` or `rapid-pvst` operating mode is set, PVST+ automatically runs on port VLANs, but the mode can be changed and PVST+ can be set to start or stop per VLAN. The `no spanning-tree vlan` command is used to stop operation.

To prevent PVST+ operation for a newly created VLAN, use the `no spanning-tree vlan` command to set this before the VLAN is created.

Command examples

1.
```
(config)# no spanning-tree vlan 20
```
Stops VLAN 20 PVST+ operation.

2.
```
(config)# spanning-tree vlan 20
```
Runs the stopped VLAN 20 PVST+.

Notes

- PVST+ runs automatically when nothing is displayed for the configuration. The `no spanning-tree vlan` command can be used to stop it, and the configuration can be checked to make sure it has stopped.

- The maximum number of port VLANs on which PVST+ can run is 250. It will not run automatically on any subsequently created port VLANs.

22.4.3 Configuring PVST+ topologies

(1) Setting bridge priority

The bridge priority is a parameter for determining the root bridge. When a topology is designed, the highest priority is set for the switch to be used for the root bridge, and the second highest priority is set for the switch to be used next for the root bridge if a fault occurs on the root bridge.

Points to note

For bridge priorities, a lower value indicates a higher priority, and the switch with the lowest set value is the root bridge. Because the root bridge is decided by a bridge ID consisting of the bridge priority and switch MAC address, if this parameter is not set, the switch with the lowest MAC address becomes the root bridge.

Command examples

1.
```
(config)# spanning-tree vlan 10 priority 4096
```

Sets the bridge priority for the VLAN 10 PVST+ to 4096.

(2) Setting path costs

The path cost is a parameter for determining communication paths. When a Spanning Tree topology is designed, after the bridge priority is determined, the root port of each designated bridge (communication path from the designated bridge to the root bridge) is determined by using this parameter.

Points to note

Path cost values are set for each port of a designated bridge. Small values can be set to make root port selection more likely. If no value is set, different default values are used for each port speed, with faster ports more likely to be chosen for the root port.

Path costs are set to prioritize the use of slow ports over fast ports as paths. No settings are needed for topologies in which fast ports are prioritized.

Path cost values consist of two types, `short` (16-bit values) and `long` (32-bit values), either of which must be used over an entire topology. When using ports whose speed is 10 Gbit/s or more, we recommend using `long` (32-bit value) types. By default, `short` (16-bit value) types are used for operation. Automatic settings based on Ethernet interface speed differ depending on whether `short` (16-bit value) or `long` (32-bit value) types are set. The following table describes the default values for path costs.

Table 22-10: Default path cost value

Port speed	Default path cost value	
	short (16-bit value)	long (32-bit value)
10 Mbit/s	100	2000000
100 Mbit/s	19	200000
1 Gbit/s	4	20000
10 Gbit/s	2	2000
40 Gbit/s **[AX3800S]**	2	500

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree cost 100
(config-if)# exit
```
Sets the path cost of port 1/0/1 to 100.

2.
```
(config)# spanning-tree pathcost method long
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree vlan 10 cost 200000
```
Sets `long` (32-bit value) path costs to be used, and then changes port 1/0/1 for VLAN 10 to have a cost value of 200000. The path cost is 200000 on port 1/0/1 for only VLAN 10, with other VLANs running at 100.

Notes

When link aggregation is used, the default value for the path costs of a channel group is not the total of all ports in the channel group, but the speed of a single port. When multi speed mode is used for link aggregation, this is the speed of the slowest port.

(3) Setting port priority

The port priority is set to determine which port is used when a Spanning Tree Protocol is used to make connections between two switches redundant, and the path costs are the same value for both.

Normally, we recommend that you use link aggregation as functionality to make connections between two switches redundant, but use this functionality when a Spanning Tree Protocol is needed for redundancy because the partner connected switch does not support link aggregation.

Points to note

For port priorities, a lower value indicates a higher priority. When redundancy is used between two switches, the path whose switch is closer to the root bridge and whose port has a higher priority is used as the communication path. If this parameter is not set, the port with the lower port number is prioritized.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree port-priority 64
(config-if)# exit
```
Sets the port priority for port 1/0/1 to 64.

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree vlan 10 port-priority 144
```
Changes the port priority of port 1/0/1 for VLAN 10 to 144. For port 1/0/1, only VLAN 10 has a port priority of 144, with other VLANs running at 64.

22.4.4 Configuring PVST+ parameters

Each parameter must be set to satisfy the following relationship: 2 x (*forward-time* - 1) ≥ *max-age* ≥ 2 x (*hello-time* + 1). When a parameter is changed, parameters must be adjusted on all switches comprising the Spanning Tree Protocol.

(1) Setting BPDU sending intervals

A short BPDU sending interval makes topology changes easier to detect. A longer interval requires more time to detect a topology change, but can reduce BPDU traffic and the load on the Spanning Tree program for the Switch.

Points to note

When no value is set, BPDUs are sent at two-second intervals. Normally, this setting is not required.

Command examples

1. `(config)# spanning-tree vlan 10 hello-time 3`

   Sets the PVST+ BPDU sending interval to 3 seconds for VLAN 10.

Notes

A short BPDU sending interval makes topology changes easier to detect, but might increase load on the Spanning Tree program due to an increase in BPDU traffic. If setting this parameter shorter than the default value (2 seconds) causes timeout messages to be output and the topology to change frequently, change it back to the default value.

(2) Setting the maximum number of BPDUs to be sent

To prevent an increase in CPU load for a Spanning Tree Protocol, the maximum number of BPDUs to be sent per *hello-time* (BPDU sending interval) can be chosen. If topology changes frequently occur, a large quantity of BPDUs are sent to report and gather topology changes, possibly increasing BPDU traffic and CPU load. This can be controlled by limiting the maximum number of BPDUs to be sent.

Points to note

If no value is set, operation is performed with a maximum number of BPDUs per *hello-time* (BPDU sending interval) of 3. The configuration for this parameter only takes effect for Rapid PVST+, and is fixed at 3 for PVST+. Normally, this setting is not required.

Command examples

1. `(config)# spanning-tree vlan 10 transmission-limit 5`

   Sets the maximum number of BPDUs to be sent per *hello-time* to 5 for VLAN 10 Rapid PVST+.

(3) Setting maximum enabled times for BPDUs

You can set the maximum enabled time for BPDUs sent from the root bridge. The BPDU counter is incremented whenever a switch is passed, and BPDUs exceeding the maximum enabled time are disabled and ignored.

Points to note

The maximum enabled time can be increased to have BPDUs reach many switches. If no value is set, 20 is used for the maximum enabled time.

Command examples

1. `(config)# spanning-tree vlan 10 max-age 25`

   Sets the maximum enabled time for BPDUs to 25 seconds on the PVST+ for VLAN 10.

(4) Setting status transition times

For timer-based operation in PVST+ mode or Rapid PVST+ mode, the port status transitions at a fixed time interval. For the PVST+ mode, it transitions from `Blocking` to `Listening`, `Learning`, and then `Forwarding`, and for the Rapid PVST+ mode, it transitions from `Discarding` to `Learning` and then `Forwarding`. The time required for these status transitions can be set. A small value can be set to transition more quickly to the `Forwarding` status.

Points to note

If no value is set, 15 seconds is used for the status transition time. When changing this parameter to a shorter time, make sure that the relationship between the BPDU maximum enabled time (*max-age*) and sending interval (*hello-time*) satisfies the following: 2 x (*forward-time* - 1) ≥ *max-age* ≥ 2 x (*hello-time* + 1).

Command examples

1. `(config)# spanning-tree vlan 10 forward-time 10`

   Sets the status transition time to 10 for the VLAN 10 PVST+.

22.5 PVST+ operation

22.5.1 List of operation commands

The following table describes the operation commands for PVST+.

Table 22-11: List of operation commands

Command name	Description
show spanning-tree	Shows Spanning Tree information.
show spanning-tree statistics	Shows Spanning Tree statistics.
clear spanning-tree statistics	Clears Spanning Tree statistics.
clear spanning-tree detected-protocol	Forces recovery of STP compatible mode for Spanning Tree Protocols.
show spanning-tree port-count	Shows the numbers handled by Spanning Tree Protocols.
restart spanning-tree	Restarts the Spanning Tree program.
dump protocols spanning-tree	Outputs to a file detailed event trace information and control table information collected for Spanning Tree Protocols.

22.5.2 Checking PVST+ statuses

PVST+ information is displayed in the execution results of the `show spanning-tree` command. The PVST+ or Rapid PVST+ operation mode can be checked in `Mode`. To check that the topology has been built properly, make sure that the contents of `Root Bridge ID` are correct, along with `Status` and `Role` in `Port Information`.

Figure 22-8: Results of executing the show spanning-tree command

```
> show spanning-tree vlan 1
Date 20XX/09/04 11:39:43 UTC
VLAN 1              PVST+ Spanning Tree:Enabled  Mode:PVST+
  Bridge ID        Priority:32769       MAC Address:0012.e205.0900
    Bridge Status:Designated
  Root Bridge ID   Priority:32769       MAC Address:0012.e201.0900
    Root Cost:1000
    Root Port:0/1
  Port Information
    0/1        Up    Status:Forwarding  Role:Root
    0/2        Up    Status:Forwarding  Role:Designated
    0/3        Up    Status:Blocking    Role:Alternate
    0/4        Down  Status:Disabled    Role:-
    0/10       Up    Status:Forwarding  Role:Designated PortFast
    0/11       Up    Status:Forwarding  Role:Designated PortFast
    0/12       Up    Status:Forwarding  Role:Designated PortFast
>
```

22.6 Description of Single Spanning Tree

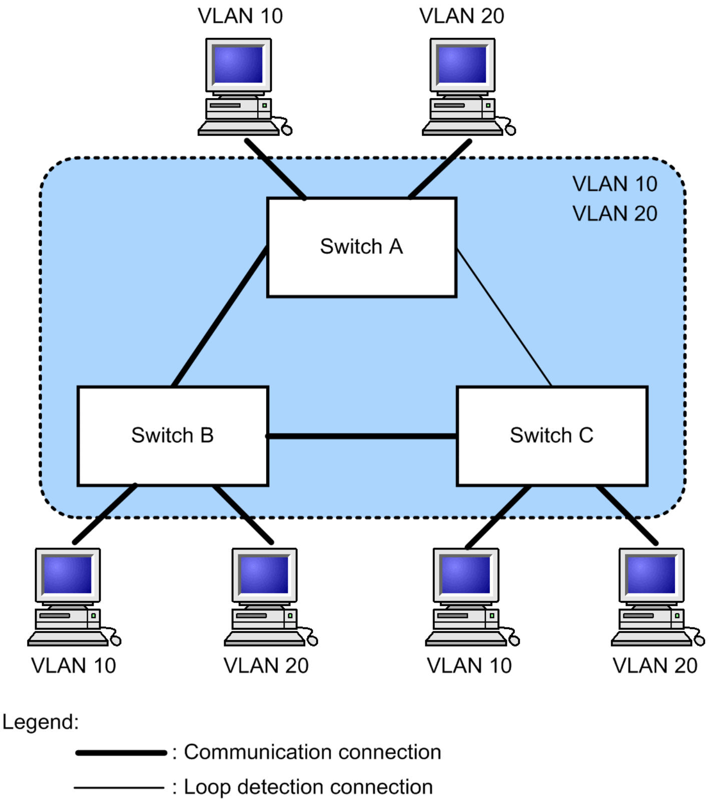
Single Spanning Tree creates topologies in which all switches are targets.

22.6.1 Overview

Single Spanning Tree and one Spanning Tree Protocol can be used to avoid loops on all VLANs, and can handle more VLANs than PVST+ controlling individual VLANs.

The figure below shows a network configuration based on Single Spanning Tree. In this figure, VLAN 10 and VLAN 20 are set for Switches A, B, and C, with PVST+ stopped on all VLANs to apply Single Spanning Tree. A single topology is used for all VLANs for communication.

Figure 22-9: Network configuration based on Single Spanning Tree



22.6.2 Usage with PVST+

A PVST+ cannot be used for protocol VLANs and MAC VLANs. Also, a PVST+ can run no more than 250 VLANs. Subsequent VLANs cannot be used. Single Spanning Tree can be used to apply a Spanning Tree Protocol to these VLANs even when a PVST+ is used.

Single Spanning Tree is applied to all VLANs for which a PVST+ is not running. The following table describes the VLANs subject to Single Spanning Tree when Single Spanning Tree is used with a PVST+.

Table 22-12: Single Spanning Tree target VLAN

Item	VLAN
PVST+ target VLAN	VLANs running on a PVST+. PVST+ runs as many as 250 port VLANs automatically.

Item	VLAN
Single Spanning Tree target VLAN	251st and subsequent port VLANs
	VLANs for which PVST+ stops (specified by the `no spanning-tree vlan` command)
	Default VLANs (port VLANs with a VLAN ID of 1)
	Protocol VLANs
	MAC VLANs

22.6.3 Notes on Single Spanning Tree usage

(1) Notes on use with other functionality

For details, see *18.3 Compatibility between Layer 2 switch functionality and other functionality*.

(2) VLAN 1 (default VLAN) PVST+ and Single Spanning Tree

Single Spanning Tree and VLAN 1 PVST+ cannot run at the same time. When Single Spanning Tree runs, the VLAN 1 PVST+ stops.

22.7 Configuration of Single Spanning Tree

22.7.1 List of configuration commands

The following table describes the configuration commands for Single Spanning Tree.

Table 22-13: List of configuration commands

Command name	Description
spanning-tree cost	Sets the default path cost value for each port.
spanning-tree pathcost method	Sets the default value for the margin of values used for path costs for a port.
spanning-tree port-priority	Sets the default value for the port priority for each port.
spanning-tree single	Starts or stops Single Spanning Tree.
spanning-tree single cost	Sets the path cost value for Single Spanning Tree.
spanning-tree single forward-time	Sets the time required for port status transitions.
spanning-tree single hello-time	Sets the sending interval for BPDUs.
spanning-tree single max-age	Sets the maximum enabled time for sent BPDUs.
spanning-tree single pathcost method	Sets the margin of values used for path costs for Single Spanning Tree.
spanning-tree single port-priority	Sets the port priority for Single Spanning Tree.
spanning-tree single priority	Sets the bridge priority.
spanning-tree single transmission-limit	Sets the maximum number of BPDUs that can be sent per *hello-time* interval.

22.7.2 Configuring Single Spanning Tree

Points to note

The example below shows how to start or stop Single Spanning Tree. Single Spanning Tree does not run simply by setting the `pvst` or `rapid-pvst` operation mode, but start operation according to settings.

VLAN 1 (default VLAN) and Single Spanning Tree cannot be used at the same time. When Single Spanning Tree is set, the VLAN 1 PVST+ stops.

Command examples

1.
```
(config)# spanning-tree single
```

   Runs Single Spanning Tree. This setting stops the VLAN 1 PVST+, making VLAN 1 a Single Spanning Tree target.

2.
```
(config)# no spanning-tree single
```

   Stops Single Spanning Tree. When a VLAN 1 PVST+ is not set to stop, and 250 PVST+ instances are not already running, VLAN 1 PVST+ operation starts automatically.

22.7.3 Configuring topologies for Single Spanning Tree

(1) Setting bridge priority

The bridge priority is a parameter for determining the root bridge. When a topology is designed, the highest priority is set for the switch to be used for the root bridge, and the second highest priority is set for the switch to be used next for the root bridge if a fault occurs on the root bridge.

Points to note

For bridge priorities, a lower value indicates a higher priority, and the switch with the lowest set value is the root bridge. Because the root bridge is decided by a bridge ID consisting of the bridge priority and switch MAC address, if this parameter is not set, the switch with the lowest MAC address becomes the root bridge.

Command examples

1.
```
(config)# spanning-tree single priority 4096
```
Sets the bridge priority for Single Spanning Tree to 4096.

(2) Setting path costs

The path cost is a parameter for determining communication paths. When a Spanning Tree topology is designed, after the bridge priority is determined, the root port of each designated bridge (communication path from the designated bridge to the root bridge) is determined by using this parameter.

Points to note

Path cost values are set for each port of a designated bridge. Small values can be set to make root port selection more likely. If no value is set, different default values are used for each port speed, with faster ports more likely to be chosen for the root port.

Path costs are set to prioritize the use of slow ports over fast ports as paths. No settings are needed for topologies in which fast ports are prioritized.

Path cost values consist of two types, `short` (16-bit values) and `long` (32-bit values), either of which must be used over an entire topology. When using ports whose speed is 10 Gbit/s or more, we recommend using `long` (32-bit value) types. By default, `short` (16-bit value) types are used for operation. Automatic settings based on Ethernet interface speed differ depending on whether `short` (16-bit value) or `long` (32-bit value) types are set. The following table describes the default values for path costs.

Table 22-14: Default path cost value

Port speed	Default path cost value	
	short (16-bit value)	long (32-bit value)
10 Mbit/s	100	2000000
100 Mbit/s	19	200000
1 Gbit/s	4	20000
10 Gbit/s	2	2000
40 Gbit/s **[AX3800S]**	2	500

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree cost 100
```

```
(config-if)# exit
```

Sets the path cost of port 1/0/1 to 100.

2.
```
(config)# spanning-tree pathcost method long
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree single cost 200000
```

Sets `long` (32-bit value) path costs to be used, and then changes the port 1/0/1 for Single Spanning Tree to have a cost value of 200000. The path cost is 200000 on port 1/0/1 for only Single Spanning Tree, with other PVST+ using the same port running at 100.

Notes

When link aggregation is used, the default value for the path costs of a channel group is not the total of all ports in the channel group, but the speed of a single port. When multi speed mode is used for link aggregation, this is the speed of the slowest port.

(3) Setting port priority

The port priority is set to determine which port is used when a Spanning Tree Protocol is used to make connections between two switches redundant, and the path costs are the same value for both.

Normally, we recommend that you use link aggregation as functionality to make connections between two switches redundant, but use this functionality when a Spanning Tree Protocol is needed for redundancy because the opposite connected switch does not support link aggregation.

Points to note

For port priorities, a lower value indicates a higher priority. When redundancy is used between two switches, the path whose switch is closer to the root bridge and whose port has a higher priority is used as the communication path. If this parameter is not set, the port with the lower port number is prioritized.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree port-priority 64
(config-if)# exit
```

Sets the port priority for port 1/0/1 to 64.

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree single port-priority 144
```

Changes the port priority of port 1/0/1 for Single Spanning Tree to 144. For port 1/0/1, only Single Spanning Tree has a port priority of 144, with PVST+ instances using the same port running at 64.

22.7.4 Configuring Single Spanning Tree parameters

Each parameter must be set to satisfy the following relationship: 2 x (*forward-time* - 1) ≥ *max-age* ≥ 2 x (*hello-time* + 1). When a parameter is changed, parameters must be adjusted across the entire topology.

(1) Setting BPDU sending intervals

A short BPDU sending interval makes topology changes easier to detect. A longer interval requires more time to detect a topology change, but can reduce BPDU traffic and the load on the Spanning Tree program for the Switch.

Points to note

When no value is set, BPDUs are sent at two-second intervals. Normally, this setting is not required.

Command examples

```
1. (config)# spanning-tree single hello-time 3
```

Sets the BPDU sending interval for Single Spanning Tree to 3 seconds.

Notes

A short BPDU sending interval makes topology changes easier to detect, but might increase load on the Spanning Tree program due to an increase in BPDU traffic. If setting this parameter shorter than the default value (2 seconds) causes timeout messages to be output and the topology to change frequently, change it back to the default value.

(2) Setting the maximum number of BPDUs to be sent

To prevent an increase in CPU load for a Spanning Tree Protocol, the maximum number of BPDUs to be sent per *hello-time* (BPDU sending interval) can be chosen. If topology changes frequently occur, a large quantity of BPDUs are sent to report and gather topology changes, possibly increasing BPDU traffic and CPU load. This can be controlled by limiting the maximum number of BPDUs to be sent.

Points to note

If no value is set, operation is performed with a maximum number of BPDUs per *hello-time* (BPDU sending interval) of 3. The configuration for this parameter only takes effect for Rapid STP, and is fixed at 3 for STP. Normally, this setting is not required.

Command examples

```
1. (config)# spanning-tree single transmission-limit 5
```

Sets the maximum number of BPDUs to be sent per *hello-time* to 5 for Single Spanning Tree.

(3) Setting maximum enabled times for BPDUs

You can set the maximum enabled time for BPDUs sent from the root bridge. The BPDU counter is incremented whenever a switch is passed, and BPDUs exceeding the maximum enabled time are disabled and ignored.

Points to note

The maximum enabled time can be increased to have BPDUs reach many switches. If no value is set, 20 is used for the maximum enabled time.

Command examples

```
1. (config)# spanning-tree single max-age 25
```

Sets the maximum enabled time for BPDUs to 25 on Single Spanning Tree.

(4) Setting status transition times

For timer-based operation in STP mode or Rapid STP mode, the port status transitions at a fixed time interval. For the STP mode, it transitions from `Blocking` to `Listening`, `Learning`, and then `Forwarding`, and for the Rapid STP mode, it transitions from `Discarding` to `Learning` and then `Forwarding`. The time required for these status transitions can be set. A small value can be set to transition more quickly to the `Forwarding` status.

Points to note

If no value is set, 15 seconds is used for the status transition time. When changing this parameter to a shorter time, make sure that the relationship between the BPDU maximum enabled time (*max-age*) and sending interval (*hello-time*) satisfies the following: 2 x (*forward-time* - 1) ≥ *max-age* ≥ 2 x (*hello-time* + 1).

Command examples

1. `(config)# spanning-tree single forward-time 10`

   Sets the status transition time to 10 for Single Spanning Tree.

22.8 Operation for Single Spanning Tree

22.8.1 List of operation commands

The following table describes the operation commands for Single Spanning Tree.

Table 22-15: List of operation commands

Command name	Description
show spanning-tree	Shows Spanning Tree information.
show spanning-tree statistics	Shows Spanning Tree statistics.
clear spanning-tree statistics	Clears Spanning Tree statistics.
clear spanning-tree detected-protocol	Forces recovery of STP compatible mode for Spanning Tree Protocols.
show spanning-tree port-count	Shows the numbers handled by Spanning Tree Protocols.
restart spanning-tree	Restarts the Spanning Tree program.
dump protocols spanning-tree	Outputs to a file detailed event trace information and control table information collected for Spanning Tree Protocols.

22.8.2 Checking the Single Spanning Tree status

Use the `show spanning-tree` command to check information about Single Spanning Tree. The STP or Rapid STP operation mode can be checked in `Mode`. To check that the topology has been built properly, make sure that the contents of `Root Bridge ID` are correct, along with `Status` and `Role` in `Port Information`.

Figure 22-10: Information about Single Spanning Tree

```
> show spanning-tree single
Date 20XX/09/04 11:42:06 UTC
Single Spanning Tree:Enabled  Mode:Rapid STP
  Bridge ID        Priority:32768       MAC Address:0012.e205.0900
    Bridge Status:Designated
  Root Bridge ID   Priority:32768       MAC Address:0012.e205.0900
    Root Cost:0
    Root Port:-
  Port Information
    0/1        Up    Status:Forwarding  Role:Root
    0/2        Up    Status:Forwarding  Role:Designated
    0/3        Up    Status:Blocking    Role:Alternate
    0/4        Down  Status:Disabled    Role:-
    0/10       Up    Status:Forwarding  Role:Designated PortFast
    0/11       Up    Status:Forwarding  Role:Designated PortFast
    0/12       Up    Status:Forwarding  Role:Designated PortFast
>
```

22.9 Description of Multiple Spanning Tree

22.9.1 Overview

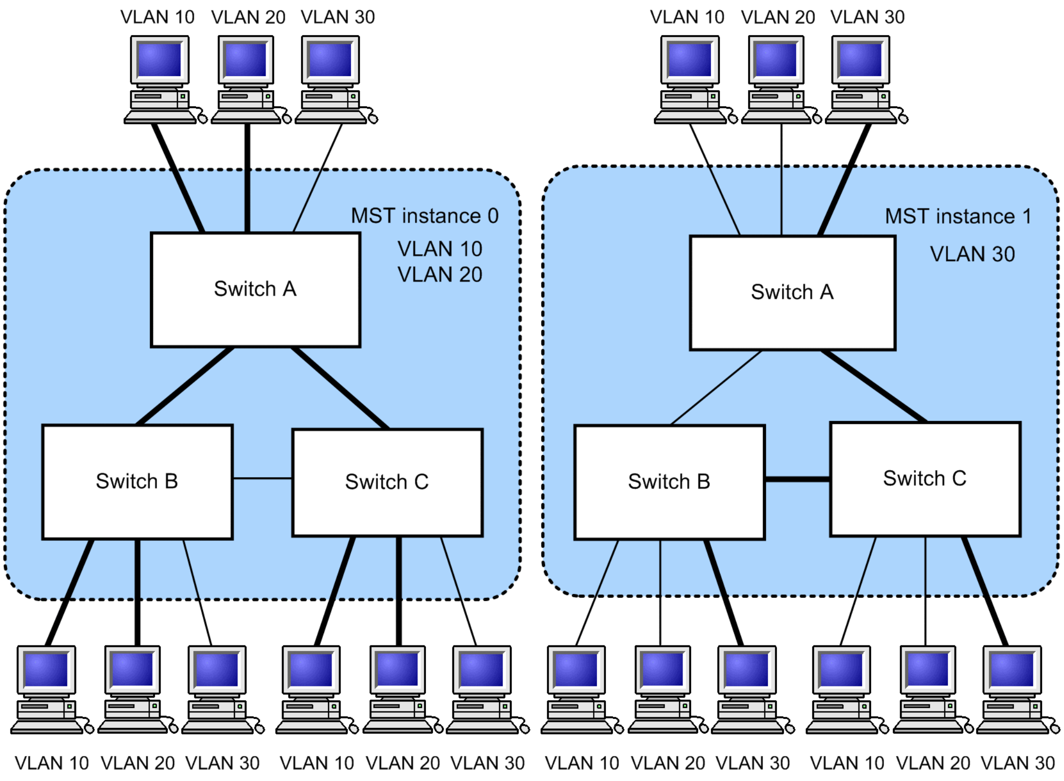
The following explains the features of Multiple Spanning Tree. MST instances can be used to perform load balancing. MST regions can be used to divide large network configurations into smaller configurations, to simplify network design. The following gives a functional overview of how Multiple Spanning Tree can be used to achieve these goals.

(1) MST instance

Multiple Spanning Tree allows Spanning Tree Protocols to be built for each group that aggregates multiple VLANs, called MST instances or MSTI, enabling load balancing for each MST instance. For load balancing using PVST+, a tree is needed for each VLAN, but with Multiple Spanning Tree, MST instances can be used to use only the trees needed through planned load balancing. Therefore, unlike PVST+, increases in CPU load and network load can be kept to a minimum for each increase in VLAN count. The switch allows as many as 16 MST instances to be set for the Switch.

The following figure shows an example MST instance setup.

Figure 22-11: Example MST instance setup



Two instances are defined on the network, with load balancing performed.
VLANs 10 and 20 are made to belong to instance 0, and VLAN 30 is made to belong to instance 1.

Legend:

━━ : Communication connection

── : Loop detection connections and non-communication connections

(2) MST regions

Multiple Spanning Tree allows multiple switches to be grouped and handled as an MST region. To belong in the same MST region, the region name, revision number, MST instance ID, and VLAN correspondence must be the same. These are set by configuration. Trees are built separately between MST regions and within MST regions, and the topology within an MST region can be built per MST instance.

The following explains Spanning Tree Protocols that run both between MST regions and within MST regions.

- CST

  The Common Spanning Tree (CST) controls connections between MST regions, and bridges using Single Spanning Tree. Because this topology performs calculations by physical port as with Single Spanning Tree, it cannot perform load balancing.

- IST

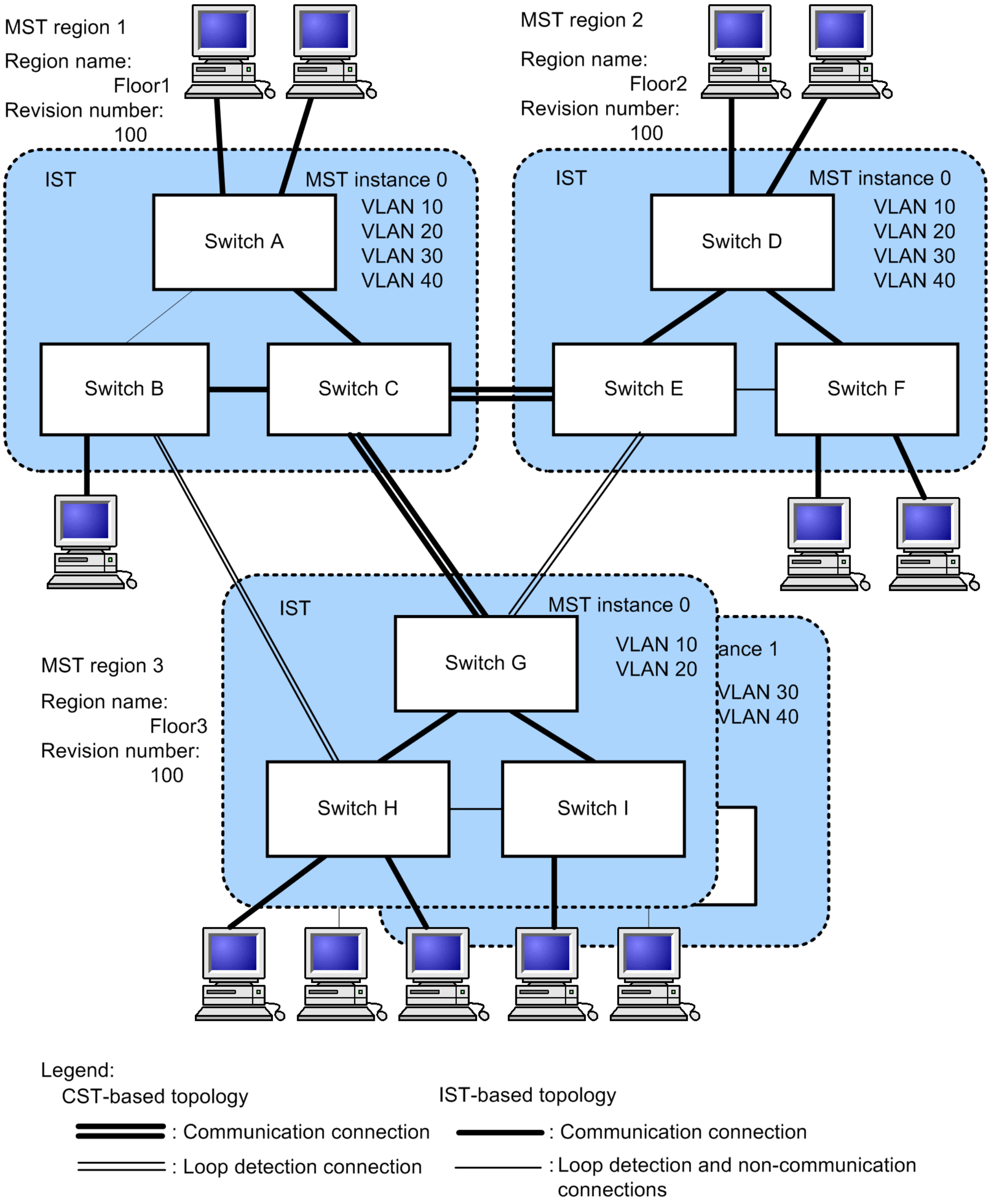
  The Internal Spanning Tree (IST) refers to a topology that runs by default within an MST region for connecting outside of the MST region, and for which an MST instance ID of 0 is assigned. The port connecting outside of the MST region is called the boundary port. Note that a unique MST instance is used to send and receive BPDUs within and between regions. The topology information for all MST instances is encapsulated in an MST BPDU for reporting.

- CIST

  The Common and Internal Spanning Tree (CIST) refers to a topology that combines ISTs and CSTs.

The following figure provides an overview of Multiple Spanning Tree.

Figure 22-12: Overview of Multiple Spanning Tree

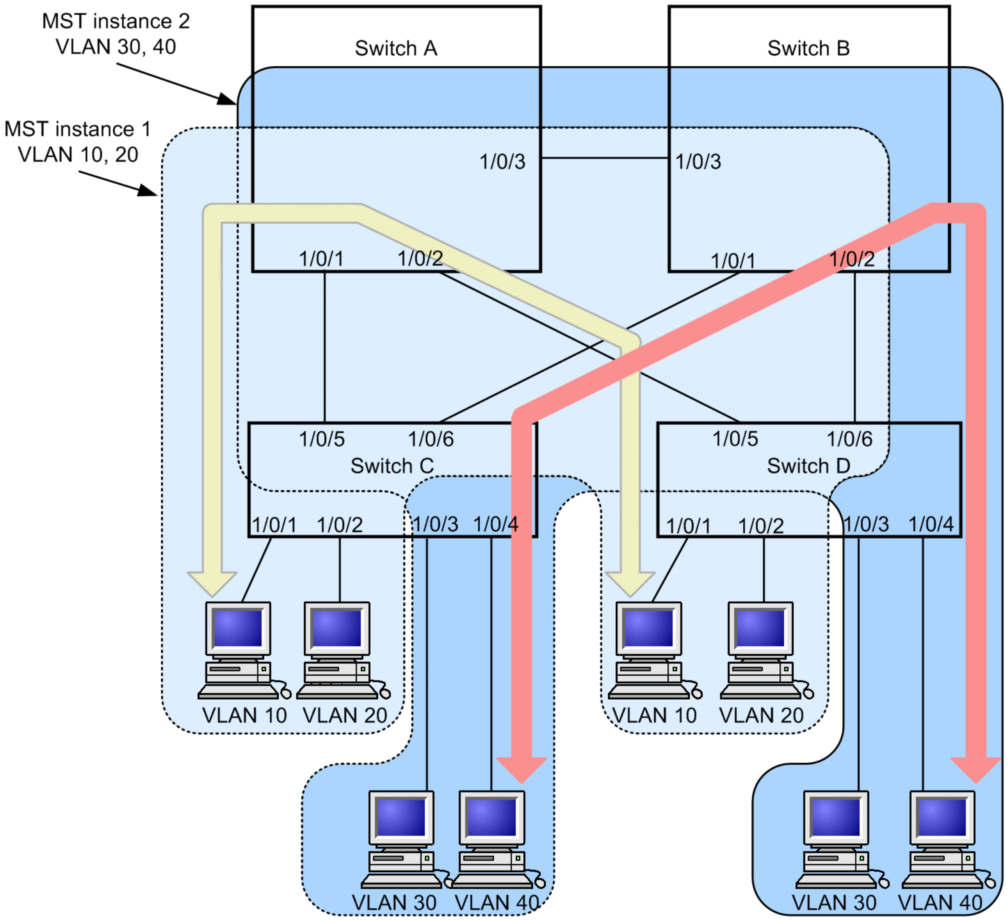


22.9.2 Designing networks for Multiple Spanning Tree

(1) Configuring load balancing for each MST instance

Multiple Spanning Tree allows load balancing to be performed for each MST instance. The figure below shows an example configuration for load balancing. In this example, VLANs 10 and 20 are set for MST instance 1, VLANs 30 and 40 are set for MST instance 2, for load balancing in two parts. As shown in this example, Multiple Spanning Tree can enable load balancing by managing four VLANs with just two trees.

Figure 22-13: Load balancing configuration for Multiple Spanning Tree



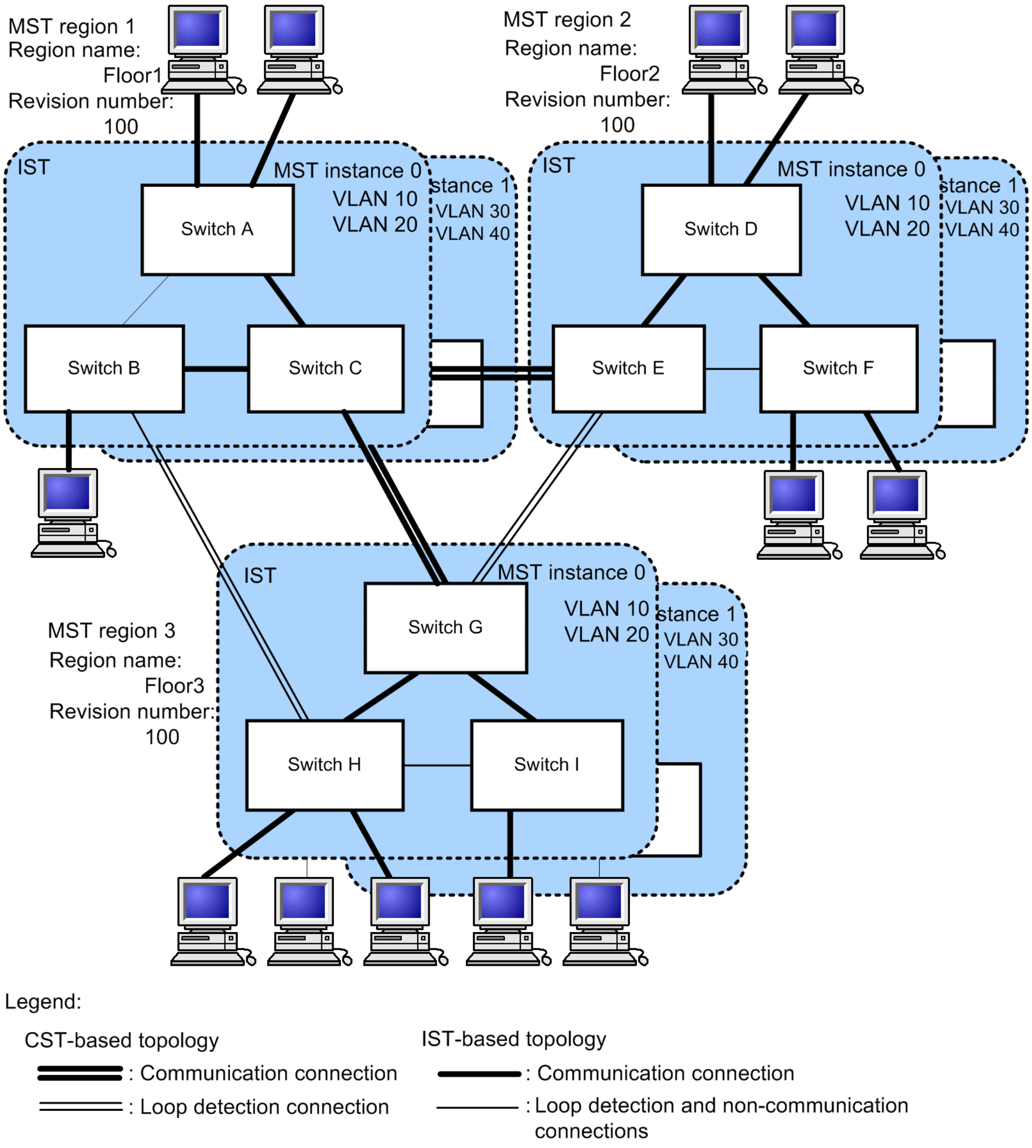
Load balancing is performed with the communication path for the VLAN 10 terminal connected to Switch C and Switch D, and the communication path for the VLAN 40 terminal connected to Switch C and Switch D.

(2) Designing networks based on MST regions

Network design becomes more complicated as network configurations grow larger, but MST regions can be used to divide them into smaller configurations to simplify network design, such as by implementing load balancing for each MST region.

The figure below shows an example network design based on MST regions. In this example, Switches A, B, and C are set for MST region 1, Switches D, E, and F are set for MST region 2, and Switches G, H, and I are set for MST region 3, dividing the network into three MST regions.

Figure 22-14: Network configuration by MST region



22.9.3 Compatibility with other Spanning Tree Protocols

(1) Compatibility with Single Spanning Tree

Multiple Spanning Tree can be used with STP or Rapid STP when run with Single Spanning Tree. Before a connection with one of these is established, connections with other MST regions are cut. High-speed status transitions are performed for connections with Rapid STP.

(2) Compatibility with PVST+

Multiple Spanning Tree is not compatible with PVST+. However, because the access port of switches for which PVST+ is running operate in the same way as Single Spanning Tree, the switches can connect to Multiple Spanning Tree.

22.9.4 Notes on Multiple Spanning Tree usage

(1) Notes on use with other functionality

For details, see *18.3 Compatibility between Layer 2 switch functionality and other functionality*.

(2) MST regions

The range of VLANs that can be handled by the Switch and other switches might differ. To handle such switches as the same MST region, make sure that the corresponding VLANs belong to MST instance 0.

(3) When time is required for topology convergence

When the events listed in the following table occur for CIST root bridges or MST instances, the topology might take a long time to settle, during which time communication might stop and MAC address tables might be cleared.

Table 22-16: Events occurring on root bridges

Event	Description	Type of root bridge type on which the event occurs	Affected topology
Configuration change	When the region name (1), revision number (2), or correspondence between instance number and VLAN (3) is changed by configuration, and the region is split or merged: (1) `name` command for the MST configuration mode (2) `revision` command for the MST configuration mode (3) `instance` command for the MST configuration mode	CIST root bridge	CIST
		Root bridge on MST instance 0 (IST)	CIST
		Root bridge on MST instance 1 and those subsequent	Corresponding MST instance
	When the bridge priority is reduced by the `spanning-tree mst root priority` command (a larger value is currently set)	CIST root bridge	CIST
		Root bridge on MST instance 1 and those subsequent	Corresponding MST instance
Additional Information	When the Switch stops	CIST root bridge	CIST
		Root bridge on MST instance 0 (IST)	CIST
		Root bridge on MST instance 1 and those subsequent	Corresponding MST instance
	When all ports are down for the Switch in a loop configuration, on the partner switch connected to the switch (and the Switch is no longer the root bridge in the corresponding loop configuration)	CIST root bridge	CIST
		Root bridge on MST instance 0 (IST)	CIST
		Root bridge on MST instance 1 and those subsequent	Corresponding MST instance

22.10 Configuration of Multiple Spanning Tree

22.10.1 List of configuration commands

The following table describes the configuration commands for Multiple Spanning Tree.

Table 22-17: List of configuration commands

Command name	Description
instance	Sets VLANs belonging to Multiple Spanning Tree MST instances.
name	Sets a string to identify a Multiple Spanning Tree region.
revision	Sets revision numbers to identify Multiple Spanning Tree regions.
spanning-tree cost	Sets the default path cost value for each port.
spanning-tree mode	Sets the operating mode for Spanning Tree functionality.
spanning-tree mst configuration	Sets the information required to form MST regions in Multiple Spanning Tree.
spanning-tree mst cost	Sets the path cost for each MST instance for Multiple Spanning Tree.
spanning-tree mst forward-time	Sets the time required for port status transitions.
spanning-tree mst hello-time	Sets the sending interval for BPDUs.
spanning-tree mst max-age	Sets the maximum enabled time for sent BPDUs.
spanning-tree mst max-hops	Sets the maximum number of hops within an MST region.
spanning-tree mst port-priority	Sets the port priority for each MST instance in Multiple Spanning Tree.
spanning-tree mst root priority	Sets the bridge priority for each MST instance.
spanning-tree mst transmission-limit	Sets the maximum number of BPDUs that can be sent per *hello-time* interval.
spanning-tree port-priority	Sets the default value for the port priority for each port.

22.10.2 Configuring Multiple Spanning Tree

(1) Configuring Multiple Spanning Tree

Points to note

When the Spanning Tree operating mode is set to Multiple Spanning Tree, PVST+ and Single Spanning Tree stop and then Multiple Spanning Tree operation starts.

Command examples

1. `(config)# spanning-tree mode mst`

   Enables Multiple Spanning Tree and starts CIST operation.

Notes

When the `no spanning-tree mode` command is used to delete operating mode settings for Multiple Spanning Tree, the default operating mode of `pvst` is used. In this case, PVST+ operation starts automatically on the port VLAN.

(2) Setting regions and instances

Points to note

MST regions require that all switches belonging to the same region have the same region name, revision number, and MST instance settings.

The instance number of an MST instance and the VLAN to which the instance belongs are set at the same time. To make the regions match, the Switch allows unset VLAN IDs to be set for the belonging instance. VLANs for which no belonging instance is specified automatically belong to the CIST (instance 0).

As many as 16 MST instances can be set, including the CIST (instance 0).

Command examples

1.
```
(config)# spanning-tree mst configuration
(config-mst)# name "REGION TOKYO"
(config-mst)# revision 1
```

Switches to the Multiple Spanning Tree configuration mode, and sets `name` (region name) and `revision` (revision number).

2.
```
(config-mst)# instance 10 vlans 100-150
(config-mst)# instance 20 vlans 200-250
(config-mst)# instance 30 vlans 300-350
```

Sets instances 10, 20, and 30, and sets the VLANs belonging to each instance. VLANs 100 to 150 are set for instance 10, VLANs 200 to 250 are set for instance 20, and VLANs 300 to 350 are set for instance 30. Other VLANs that are not specified belong to the CIST (instance 0).

22.10.3 Configuring topologies for Multiple Spanning Tree

(1) Setting bridge priority for each instance

The bridge priority is a parameter for determining the root bridge. When a topology is designed, the highest priority is set for the switch to be used for the root bridge, and the second highest priority is set for the switch to be used next for the root bridge in case a fault occurs on the root bridge.

Points to note

For bridge priorities, a lower value indicates a higher priority, and the switch with the lowest set value is the root bridge. Because the root bridge is decided by a bridge ID consisting of the bridge priority and switch MAC address, if this parameter is not set, the switch with the lowest MAC address becomes the root bridge.

The bridge priority for Multiple Spanning Tree is set for each instance. When values are changed for each instance, load balancing (building different topologies) can be performed per instance.

Command examples

1.
```
(config)# spanning-tree mst 0 root priority 4096
(config)# spanning-tree mst 20 root priority 61440
```

Sets the bridge priority of the CIST (instance 0) to 4096, and the bridge priority of instance 20 to 61440.

(2) Setting path costs for each instance

The path cost is a parameter for determining communication paths. When a Spanning Tree topology is designed, after the bridge priority is determined, the root port of each designated bridge (communication path from the designated bridge to the root bridge) is determined by using this parameter.

Points to note

Path cost values are set for each port of a designated bridge. Small values can be set to make root port selection more likely. If no value is set, different default values are used for each port speed, with faster ports more likely to be chosen for the root port.

Path costs are set to prioritize the use of slow ports over fast ports as paths. No settings are needed for topologies in which fast ports are prioritized.

The following table describes the default values for path costs.

Table 22-18: Default path cost value

Port speed	Default path cost value
10 Mbit/s	2000000
100 Mbit/s	200000
1 Gbit/s	20000
10 Gbit/s	2000
40 Gbit/s **[AX3800S]**	500

Command examples

1.
```
(config)# spanning-tree mst configuration
(config-mst)# instance 10 vlans 100-150
(config-mst)# instance 20 vlans 200-250
(config-mst)# instance 30 vlans 300-350
(config-mst)# exit
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree cost 2000
```

Sets MST instances 10, 20, and 30, and sets the path cost of port 1/0/1 to 2000. This means the path cost of port 1/0/1 is 2000 for the CIST (instance 0) and MST instances 10, 20, and 30.

2.
```
(config-if)# spanning-tree mst 20 cost 500
```

Changes the path cost of port 1/0/1 for MST instance 20 to 500. Instances other than instance 20 run at 2000.

Notes

When link aggregation is used, the default value for the path costs of a channel group is not the total of all ports in the channel group, but the speed of a single port. When multi speed mode is used for link aggregation, this is the speed of the slowest port.

(3) Setting port priority for each instance

The port priority is set to determine which port is used when a Spanning Tree Protocol is used to make connections between two switches redundant, and the path costs are the same value for both.

Normally, we recommend that you use link aggregation as functionality to make connections between two switches redundant, but use this functionality when a Spanning Tree Protocol is needed for redundancy because the partner connected switch does not support link aggregation.

Points to note

For port priorities, a lower value indicates a higher priority. When redundancy is used between two switches, the path whose switch is closer to the root bridge and whose port has a higher priority is used as the communication path. If this parameter is not set, the port with the lower port number is prioritized.

Command examples

1.

```
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree port-priority 64
(config-if)# exit
```

Sets the port priority for port 1/0/1 to 64.

2.

```
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree mst 20 port-priority 144
```

Sets the port priority of port 1/0/1 for instance 20 to 144. For port 1/0/1, only instance 20 has a port priority of 144, with other instances running at 64.

22.10.4 Configuring Multiple Spanning Tree parameters

Each parameter must be set to satisfy the following relationship: 2 x (*forward-time* - 1) ≥ *max-age* ≥ 2 x (*hello-time* + 1). When a parameter is changed, parameters must be adjusted across the entire topology.

(1) Setting BPDU sending intervals

A short BPDU sending interval makes topology changes easier to detect. A longer interval requires more time to detect a topology change, but can reduce BPDU traffic and the load on the Spanning Tree program for the Switch.

Points to note

When no value is set, BPDUs are sent at two-second intervals. Normally, this setting is not required.

Command examples

1.

```
(config)# spanning-tree mst hello-time 3
```

Sets the BPDU sending interval for Multiple Spanning Tree to 3 seconds.

Notes

A short BPDU sending interval makes topology changes easier to detect, but might increase load on the Spanning Tree program due to an increase in BPDU traffic. If setting this parameter shorter than the default value (2 seconds) causes timeout messages to be output and the topology to change frequently, change it back to the default value.

(2) Setting the maximum number of BPDUs to be sent

To prevent an increase in CPU load for a Spanning Tree Protocol, the maximum number of BPDUs to be sent per *hello-time* (BPDU sending interval) can be chosen. If topology changes frequently occur, a large quantity of BPDUs are sent to report and gather topology changes, possibly increasing BPDU traffic and CPU load. This can be controlled by limiting the maximum number of BPDUs to be sent.

Points to note

If no value is set, operation is performed with a maximum number of BPDUs per *hello-time* (BPDU sending interval) of 3. Normally, this setting is not required.

Command examples

1. `(config)# spanning-tree mst transmission-limit 5`

   Sets the maximum number of BPDUs to be sent per *hello-time* to 5 for Multiple Spanning Tree.

(3) Setting the maximum number of hops

You can set the maximum number of host for BPDUs sent from the root bridge. The BPDU counter is incremented whenever a switch is passed, and BPDUs exceeding the maximum number of hops are disabled and ignored.

For ports connected to Single Spanning Tree switches, the maximum enabled time (*max-age*) parameter is used instead of the maximum number of hops (*max-hops*). The counter for the number of hops is a valid parameter between Multiple Spanning Tree switches.

Points to note

The maximum number of hops can be increased to have BPDUs reach many switches. If no value is set, 20 is used for the maximum number of hops.

Command examples

1. `(config)# spanning-tree mst max-hops 10`

   Sets the maximum number of hops for BPDUs on Multiple Spanning Tree to 10.

(4) Setting maximum enabled times for BPDUs

For Multiple Spanning Tree, maximum enabled time (*max-age*) is a valid parameter only for ports connected to a Single Spanning Tree switch. It does not need to be set for configurations in which Multiple Spanning Tree runs for switches across the entire topology.

You can set the maximum enabled time for BPDUs sent from the root bridge. The BPDU counter is incremented whenever a switch is passed, and BPDUs exceeding the maximum enabled time are disabled and ignored.

Points to note

The maximum enabled time can be increased to have BPDUs reach many switches. If no value is set, 20 is used for the maximum enabled time.

Command examples

1. `(config)# spanning-tree mst max-age 25`

   Sets the maximum enabled time for Multiple Spanning Tree BPDUs to 25.

(5) Setting status transition times

For timer-based operation, the port status transitions at a fixed time interval from `Discarding` to `Learning`, and then `Forwarding`. The time required for these status transitions can be set. A small value can be set to transition more quickly to the `Forwarding` status.

Points to note

If no value is set, 15 seconds is used for the status transition time. When changing this parameter to a shorter time, make sure that the relationship between the BPDU maximum enabled time (*max-age*) and sending interval (*hello-time*) satisfies the following: 2 x (*forward-time* - 1) ≥ *max-age* ≥ 2 x (*hello-time* + 1).

Command examples

1. `(config)# spanning-tree mst forward-time 10`

   Sets the maximum enabled time for Multiple Spanning Tree BPDUs to 10.

22.11 Operation for Multiple Spanning Tree

22.11.1 List of operation commands

The following table describes the operation commands for Multiple Spanning Tree.

Table 22-19: List of operation commands

Command name	Description
show spanning-tree	Shows Spanning Tree information.
show spanning-tree statistics	Shows Spanning Tree statistics.
clear spanning-tree statistics	Clears Spanning Tree statistics.
clear spanning-tree detected-protocol	Forces recovery of STP compatible mode for Spanning Tree Protocols.
show spanning-tree port-count	Shows the numbers handled by Spanning Tree Protocols.
restart spanning-tree	Restarts the Spanning Tree program.
dump protocols spanning-tree	Outputs to a file detailed event trace information and control table information collected for Spanning Tree Protocols.

22.11.2 Checking the Multiple Spanning Tree status

Use the `show spanning-tree` command to check information about Multiple Spanning Tree. To check that the topology has been built properly, make sure that the following items are correct:

- The region settings (`Revision Level`, `Configuration Name`, and `VLAN Mapped` for `MST Instance`)
- The contents of `Regional Root`
- The `Status` and `Role` for `Port Information`

The following figure shows the result of executing the `show spanning-tree` command.

Figure 22-15: Results of executing the show spanning-tree command

```
> show spanning-tree mst
Date 20XX/09/04 11:41:03 UTC
Multiple Spanning Tree: Enabled
Revision Level: 65535  Configuration Name: MSTP001
CIST Information
  VLAN Mapped: 1-99,151-4095                                          ...1
  CIST Root       Priority: 32768       MAC      : 0012.e207.7200
  External Root Cost      : 2000        Root Port: 0/1
  Regional Root  Priority: 32768        MAC      : 0012.e207.7200
  Internal Root Cost      : 0
  Bridge ID       Priority: 32768       MAC      : 0012.e205.0900
  Regional Bridge Status : Designated
  Port Information
    0/1        Up   Status:Forwarding  Role:Root
    0/2        Up   Status:Discarding  Role:Backup
    0/3        Up   Status:Discarding  Role:Alternate
    0/4        Up   Status:Forwarding  Role:Designated
MST Instance 10
  VLAN Mapped: 100-150
  Regional Root  Priority: 32778        MAC      : 0012.e207.7200
  Internal Root Cost      : 2000        Root Port: 0/1
  Bridge ID       Priority: 32778       MAC      : 0012.e205.0900
  Regional Bridge Status : Designated
  Port Information
    0/1        Up   Status:Forwarding  Role:Root
    0/2        Up   Status:Discarding  Role:Backup
    0/3        Up   Status:Discarding  Role:Alternate
    0/4        Up   Status:Forwarding  Role:Designated
>
```

1. Displaying instance mapping VLANs (VLAN Mapped)

   The Switch supports VLAN IDs of 1 to 4094, but VLAN IDs used for region settings are 1 to 4095 according to the standard. 1 to 4095 are explicitly displayed to make it possible to check the instances to which the VLAN IDs supported by the standard, 1 to 4095, belong.

22.12 Description of common Spanning Tree functionality

22.12.1 PortFast

(1) Overview

PortFast is functionality for ports for which a terminal is connected and loops are known in advance not to occur. PortFast is not subject to Spanning Tree topology calculations, allowing communication immediately after link-up.

(2) BPDU reception when PortFast is applied

PortFast is set for ports for which no BPDUs are expected to be received, but when a BPDU is received on a port for which PortFast is set, a switch might exist ahead, meaning that a loop is possible. Therefore, PortFast functionality stops, and operation starts as a normal port subject to Spanning Tree operations including topology calculations and BPDU sending and reception.

After operation starts as a port subject to Spanning Tree operation, PortFast functionality is enabled again by links being brought up or down.

Use this in combination with the BPDU filter functionality to prevent PortFast functionality from stopping when a BPDU is received.

(3) BPDU transmission when PortFast is applied

Because Spanning Tree Protocols cannot run on ports for which PortFast is set, BPDUs are not sent.

However, to detect whether ports with PortFast set are mistakenly connected, BPDUs are sent for only 10 frames immediately after communication becomes possible due to PortFast functionality.

(4) BPDU guard

Functionality applied to PortFast includes the BPDU guard functionality. On ports for which the BPDU guard functionality is applied, when a BPDU is received, the port becomes inactive, instead of running as a Spanning Tree target port.

Ports put in the inactive status can be released using the `activate` command, to link up again with PortFast ports with the BPDU guard functionality applied, and resume communication.

22.12.2 BPDU filter

(1) Overview

On ports with the BPDU filter functionality applied, BPDU sending and reception stops. The BPDU filter functionality is applied to ports with PortFast set, for which a terminal is connected and loops are known not to occur.

(2) Notes on BPDU filters

When the BPDU filter functionality is set for ports other than those with PortFast applied, because BPDU sending and reception are stopped, communication is cut off until a timer-based port status transition is completed.

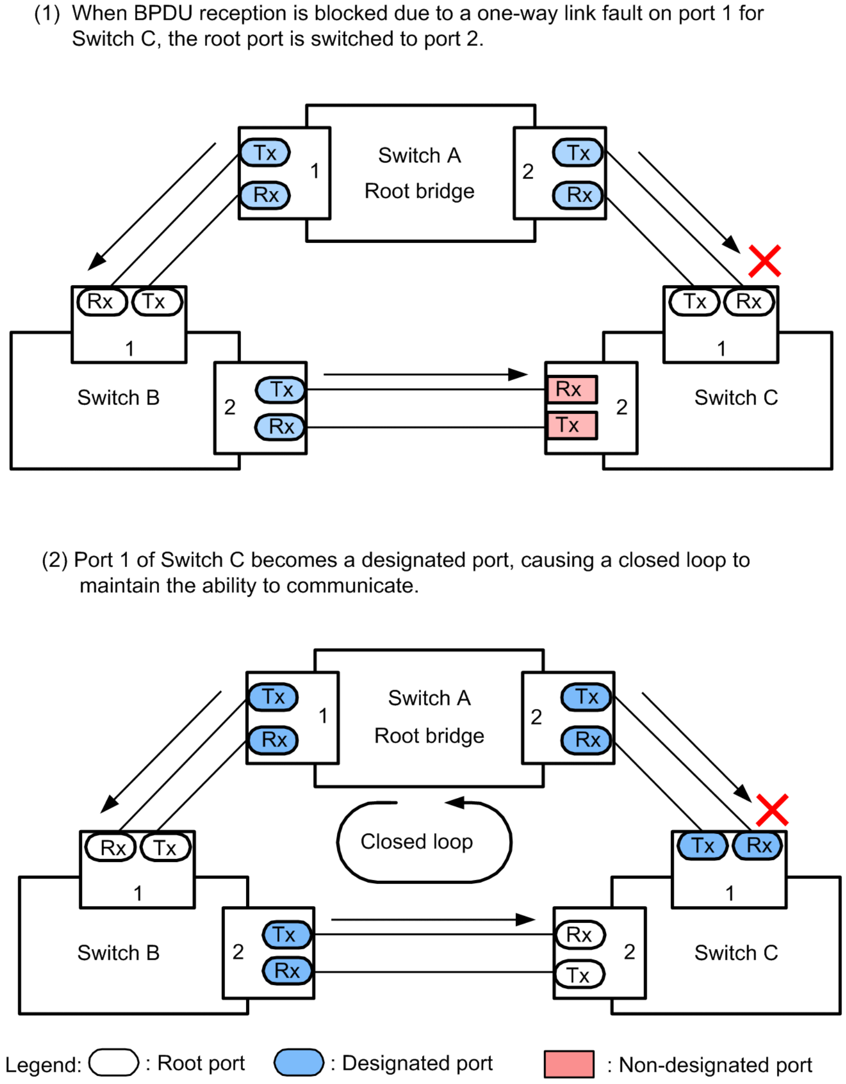
22.12.3 Loop guards

(1) Overview

When a unidirectional link fault occurs, such as when a one-way line is cut, and BPDU reception is cut off, a loop might have occurred. Loop guard functionality prevents these kinds of loops from occurring.

The following figure shows the problems that occur during unidirectional link faults.

Figure 22-16: Problems that occur during unidirectional link faults



(1) When BPDU reception is blocked due to a one-way link fault on port 1 for Switch C, the root port is switched to port 2.

(2) Port 1 of Switch C becomes a designated port, causing a closed loop to maintain the ability to communicate.

Legend: ○ : Root port ● : Designated port 🟥 : Non-designated port

Loop guard functionality transitions the status of a port for which BPDU reception has been cut off to a non-transferrable status until another BPDU is received. When BPDU reception starts, operation resumes as a normal Spanning Tree target port.

Loop guard functionality cannot be set for ports already set with PortFast functionality for specifying ports connected to terminals, or with root guard functionality.

(2) Notes on loop guards

Loop guards cannot be used for Multiple Spanning Tree.

After loop guard functionality is set, when the following events occur, the loop guard runs to block ports. Loop guards are not cleared until a BPDU is received.

- Starting the switch
- A port goes up (including due to link aggregation)
- The Spanning Tree program restarts
- The type of Spanning Tree Protocol changes (to STP or Rapid STP, PVST+ or Rapid PVST+)

Configure loop guard functionality not only on designated ports, but also on partner switches. When it is configured only on designated ports, even when the above events occur, the designated ports might not receive BPDUs. In cases like this, removing loop guards might take a long time. This is because removing a loop guard requires waiting for BPDU transmission after a BPDU reception timeout is detected on a port on the partner switch.

Also, even if loop guards are set for both ports, removing the loop guard on a designated port might take a long time if no BPDUs are received. Specifically, this happens when a bridge, port priority, or path cost is changes so that the opposing port becomes a designated port, in which case a BPDU timeout is detected on the opposing port, and loop guard operation is performed. If this port is a designated port, BPDUs might not be received, and removing loop guards might take a long time.

When loop guard functionality is set during operation, the loop guard will not run immediately, but instead will run when a BPDU reception timeout occurs.

When a switch that does not forward BPDUs exists between the Switch and a partner switch, and a port is linked up while loop guard functionality is set on both ports, loop guards will continue running on both ports. To perform recovery, BPDU forwarding functionality must be enabled on switches between both ports, and the ports must be linked up again.

22.12.4 Root guards

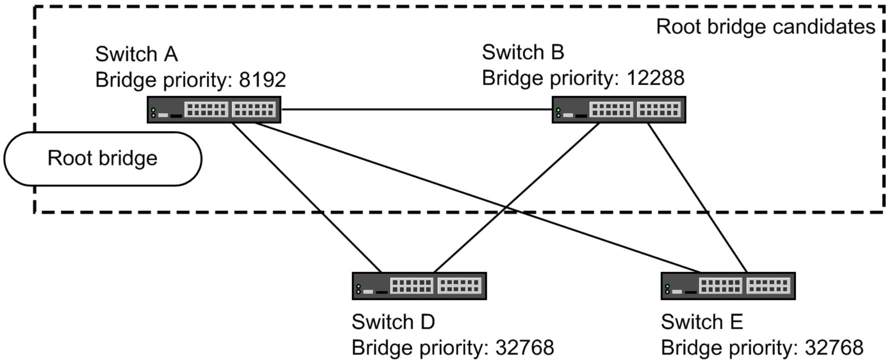
(1) Overview

Unintended topologies might occur if a switch is accidentally connected or a setting is changed somewhere where the network is not managed. When performance of the root bridge in an unintended topology is poor, a network fault might occur when traffic is congested. Root guard functionality avoids such network faults by identifying root bridge candidates for situations like this.

The figures below show problems that occur when switches are accidentally connected.

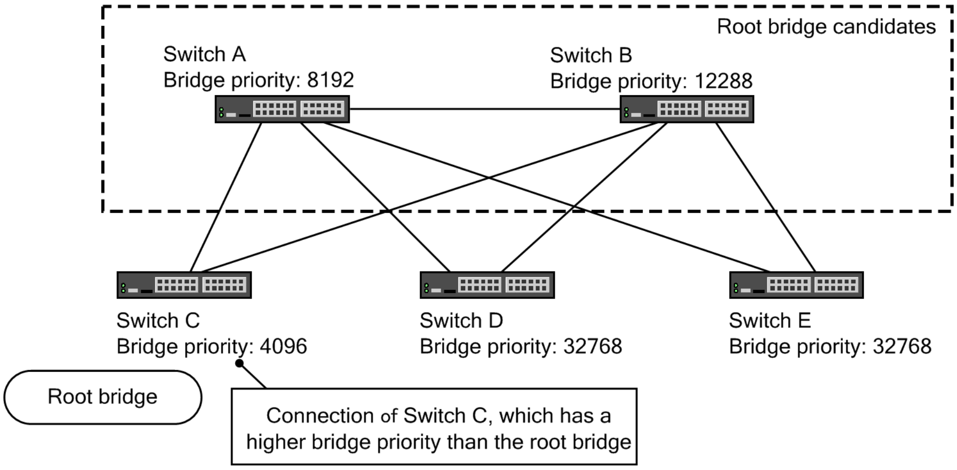
- Operation in which Switch A and Switch B run as root bridge candidates

Figure 22-17: Operation in which Switch A and Switch B run as root bridge candidates



- When Switch C, which has a higher bridge priority than Switch A or Switch B, is connected, it becomes the root bridge, and becomes congested with traffic

Figure 22-18: Operation in which Switch C, which has a higher bridge priority than Switch A or Switch B, is connected



Root guard functionality detects bridges with priorities higher than the current root bridge, and preserves the topology by discarding BPDUs. Loops can also be avoided by setting the corresponding port to be blocked. Root guard functionality cannot be used on ports for which loop guard functionality is set.

22.13 Configuration of the common Spanning Tree functionality

22.13.1 List of configuration commands

The following table describes the configuration commands for common Spanning Tree functionality.

Table 22-20: List of configuration commands

Command name	Description
spanning-tree bpdufilter	Sets BPDU filter functionality for each port.
spanning-tree bpduguard	Sets BPDU guard functionality for each port.
spanning-tree guard	Sets loop guard functionality and root guard functionality for each port.
spanning-tree link-type	Sets link types for ports.
spanning-tree loopguard default	Sets loop guard functionality to be used by default.
spanning-tree portfast	Sets PortFast functionality for each port.
spanning-tree portfast bpduguard default	Sets BPDU guard functionality to be used by default.
spanning-tree portfast default	Sets PortFast functionality to be used by default.

22.13.2 Configuring PortFast

(1) Setting PortFast

PortFast can be applied to allow immediate communication for ports known in advance not to have loops occur, such as ports connecting terminals.

Points to note

When the `spanning-tree portfast default` command is set, PortFast functionality is applied by default on access ports, protocol ports, and MAC ports. To apply this by default and disable it for each port, set the `spanning-tree portfast disable` command.

For trunk ports, this can be applied by specification for each port.

Command examples

1.
```
(config)# spanning-tree portfast default
```
Sets that PortFast functionality is to be applied by default for all access ports, protocol ports, and MAC ports.

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# switchport mode access
(config-if)# spanning-tree portfast disable
(config-if)# exit
```
Sets that PortFast functionality is not to be used on port 1/0/1 (access port).

3.
```
(config)# interface gigabitethernet 1/0/3
(config-if)# switchport mode trunk
```

```
(config-if)# spanning-tree portfast trunk
```

Specifies port 1/0/3 for the trunk port, so that PortFast functionality is applied. It is not applied by default to the trunk port. The trunk parameter needs to be specified to specify each port.

(2) Setting BPDU guards

BPDU guard functionality puts ports for which PortFast is applied in inactive status when they receive BPDUs. Normally, PortFast functionality is used to specify a port that is not a redundant path, assuming that no Spanning Tree switch exists in front of the port. This is set to avoid unintended topology changes caused by received BPDUs.

Points to note

In order to set BPDU guard functionality, PortFast functionality must be set at the same time. The `spanning-tree portfast bpduguard default` command can be used to apply BPDU guards by default for all ports to which PortFast functionality is applied. To disable BPDU guard functionality when it is applied by default, set the `spanning-tree bpduguard disable` command.

Command examples

1.
```
(config)# spanning-tree portfast default
(config)# spanning-tree portfast bpduguard default
```

Sets PortFast functionality for all access ports, protocol ports, and MAC ports. It also sets BPDU guard functionality for all ports to which PortFast functionality is applied.

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree bpduguard disable
(config-if)# exit
```

Sets BPDU guard functionality to not be used on port 1/0/1 (access port). Normal PortFast functionality is applied to port 1/0/1.

3.
```
(config)# interface gigabitethernet 1/0/2
(config-if)# switchport mode trunk
(config-if)# spanning-tree portfast trunk
```

Sets PortFast functionality for port 1/0/2 (trunk port). It also sets BPDU guard functionality. Because PortFast functionality is not applied by default to trunk ports, it is set for each port. If BPDU guard functionality is set by default, BPDU guards are applied automatically when PortFast functionality is set. If it is not set by default, it is set using the `spanning-tree bpduguard enable` command.

22.13.3 Configuring BPDU filters

The BPDU filter functionality discards any received BPDUs, and prevents BPDUs from being sent. Normally, ports that are not redundant path are assumed to be specified.

Points to note

The BPDU filter functionality can be set for each interface.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree bpdufilter enable
```
Sets the BPDU filter functionality for port 1/0/1.

22.13.4 Configuring loop guards

When a unidirectional link fault occurs, such as when a one-way line is cut, and BPDU reception is cut off, a loop might have occurred. Loop guard functionality prevents these kinds of loops from occurring.

Points to note

Loop guards run on ports for which PortFast functionality is not set.

When the `spanning-tree loopguard default` command is set, loop guards are applied to all ports other than those with PortFast set. When this is applied by default, the `spanning-tree guard none` command is set to disable loop guards.

Command examples

1.
```
(config)# spanning-tree loopguard default
```
Sets that loop guard functionality is to be applied for all ports other than those with PortFast set.

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree guard none
(config-if)# exit
```
Sets loop guards to be disabled on port 1/0/1 when loop guards are set to be applied by default.

3.
```
(config)# no spanning-tree loopguard default
(config)# interface gigabitethernet 1/0/2
(config-if)# spanning-tree guard loop
```
Deletes settings to apply loop guards by default, and applies loop guards by setting for each port, for port 1/0/2.

22.13.5 Configuring root guards

When a switch is accidentally connected to a network or a setting is changed, the root bridge might change, causing an unintended topology. Root guards can be set to prevent this kind of unintended topology change.

Points to note

Root guards are set for designated ports. They are applied to all locations connected to switches other than those that are root bridge candidates.

During root guard operation, if PVST+ is running, only ports for corresponding VLANs are set to be blocked. When Multiple Spanning Tree is running, only ports for corresponding instances are set to be blocked, but if the corresponding port is a boundary port, ports for all instances are set to be blocked.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree guard root
```
Sets root guard functionality for port 1/0/1.

22.13.6 Configuring link types

Link types represent the connection status of a port. The connections between switches must be point-to-point to perform high-speed status transitions for Rapid PVST+, Rapid STP for Single Spanning Tree, or Multiple Spanning Tree. For shared types, high-speed status transitions are not performed, and status transitions are performed by timer as with PVST+ and STP for Single Spanning Tree.

Points to note

A connection status can be set for each port. If it is not set, point-to-point is used when the port is a full duplex connection, and shared is used when it is a half duplex connection.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree link-type point-to-point
```
Runs port 1/0/1 as a point-to-point connection.

Notes

For configurations where the actual network connection type is not a 1-to-1 connection, do not use this command to specify point-to-point. In configurations other than 1-to-1 connections, at least two Spanning Tree switches neighbor a single port.

22.14 Operation for common Spanning Tree functionality

22.14.1 List of operation commands

The following table describes the operation command for common Spanning Tree functionality.

Table 22-21: List of operation commands

Command name	Description
show spanning-tree	Shows Spanning Tree information.

22.14.2 Checking the status of common Spanning Tree functionality

Use the `show spanning-tree detail` command to check information about Spanning Tree Protocols. The figure below shows an example for VLAN 10 PVST+.

The PortFast item can be checked to make sure that PortFast is set for ports 0/3, 0/4, and 0/5. PortFast is set for port 0/3, whereas BPDU guards are set for port 0/4 in addition to PortFast. This indicates that operation is running normally, without any unintended BPDU reception from any port. Port 0/5 sets the BPDU filter.

The Loop Guard item can be checked to make sure that a loop guard is set for port 0/2. The Root Guard item can be checked to make sure that a root guard is set for port 0/6. The Link Type item for each port can be used to check the link type. All ports run as point-to-point.

Figure 22-19: Spanning Tree information

```
> show spanning-tree vlan 10 detail
Date 20XX/10/21 18:13:59 UTC
VLAN 10             PVST+ Spanning Tree:Enabled  Mode:Rapid PVST+
  Bridge ID
    Priority:32778                  MAC Address:0012.e210.3004
    Bridge Status:Designated        Path Cost Method:Short
    Max Age:20                      Hello Time:2
    Forward Delay:15
  Root Bridge ID
    Priority:32778                  MAC Address:0012.e210.1004
    Root Cost:4
    Root Port:0/1
    Max Age:20                      Hello Time:2
    Forward Delay:15
  Port Information
  Port:0/1 Up
    Status:Forwarding               Role:Root
    Priority:128                    Cost:4
    Link Type:point-to-point        Compatible Mode:-
    Loop Guard:OFF                  PortFast:OFF
    BpduFilter:OFF                  Root Guard:OFF
    BPDU Parameters(20XX/10/21 18:13:59):
      Designated Root
        Priority:32778              MAC address:0012.e210.1004
      Designated Bridge
        Priority:32778              MAC address:0012.e210.1004
        Root Path Cost:0
      Port ID
        Priority:128                Number:1
      Message Age Time:0(3)/20
  Port:0/2 Up
    Status:Discarding               Role:Alternate
    Priority:128                    Cost:4
    Link Type:point-to-point        Compatible Mode:-
    Loop Guard:ON                   PortFast:OFF
    BpduFilter:OFF                  Root Guard:OFF
    BPDU Parameters(20XX/10/21 18:13:58):
```

```
    Designated Root
      Priority:32778              MAC address:0012.e210.1004
    Designated Bridge
      Priority:32778              MAC address:0012.e210.2004
      Root Path Cost:4
    Port ID
      Priority:128                Number:1
    Message Age Time:1(3)/20
Port:0/3 Up
  Status:Forwarding               Role:Designated
  Priority:128                    Cost:4
  Link Type:point-to-point        Compatible Mode:-
  Loop Guard:OFF                  PortFast:ON (BPDU not received)
  BpduFilter:OFF                  Root Guard:OFF
Port:0/4 Up
  Status:Forwarding               Role:Designated
  Priority:128                    Cost:4
  Link Type:point-to-point        Compatible Mode:-
  Loop Guard:OFF                  PortFast:BPDU Guard(BPDU not received)
  BpduFilter:OFF                  Root Guard:OFF
Port:0/5 Up
  Status:Forwarding               Role:Designated
  Priority:128                    Cost:4
  Link Type:point-to-point        Compatible Mode:-
  Loop Guard:OFF                  PortFast:ON(BPDU not received)
  BpduFilter:ON                   Root Guard:OFF
Port:0/6 Up
  Status:Forwarding               Role:Designated
  Priority:128                    Cost:4
  Link Type:point-to-point        Compatible Mode:-
  Loop Guard:OFF                  PortFast:OFF
  BpduFilter:OFF                  Root Guard:ON
```

Chapter

23. Description of the Ring Protocol

This chapter describes the Autonomous Extensible Ring Protocol.

The Autonomous Extensible Ring Protocol (abbreviated hereafter to Ring Protocol) is a Layer 2 network redundancy protocol for ring topologies.

23.1 Overview of the Ring Protocol

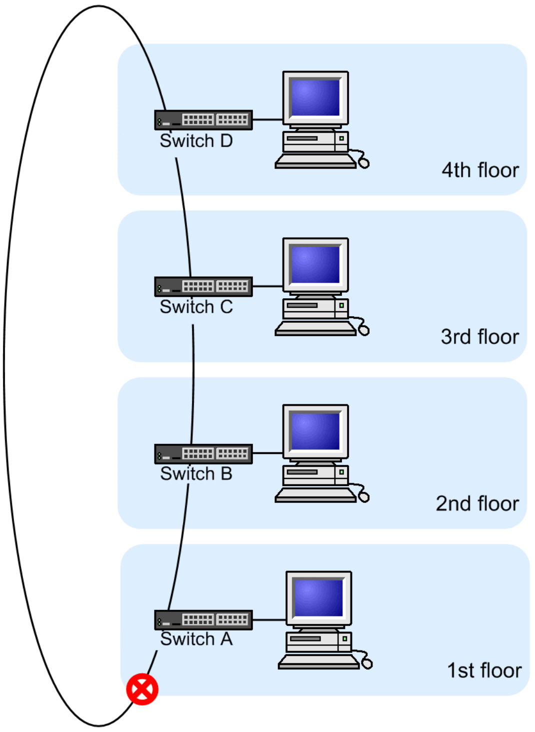
23.1.1 Overview

The Ring Protocol is a Layer 2 network redundancy protocol that detects faults in networks in which switches are connected in rings, and performs high-speed path switching accordingly.

Spanning Tree Protocols can be used as a Layer 2 network redundancy protocol, but suffer from shortcomings such as slow convergence for switching when faults occur. The Ring Protocol can be used to ensure that the path switching for when faults occur is performed at high speed. By using ring topology, the need for transmission paths and interfaces is reduced when compared to a mesh topology.

The following figure shows an example Ring Protocol application.

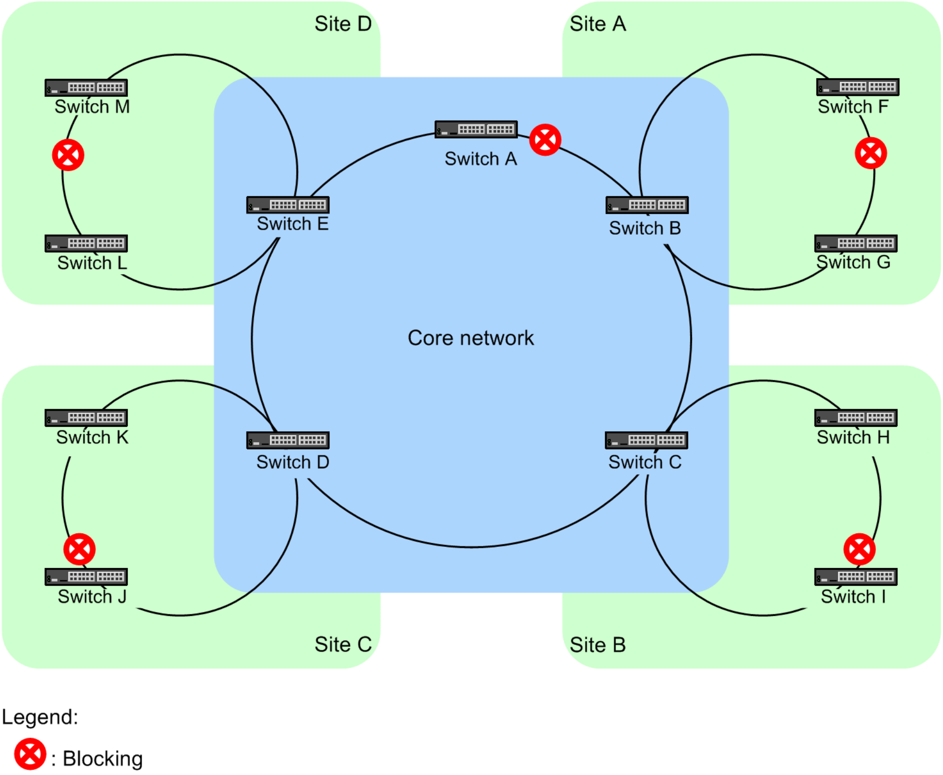
Figure 23-1: Example Ring Protocol application (part 1)



Legend:

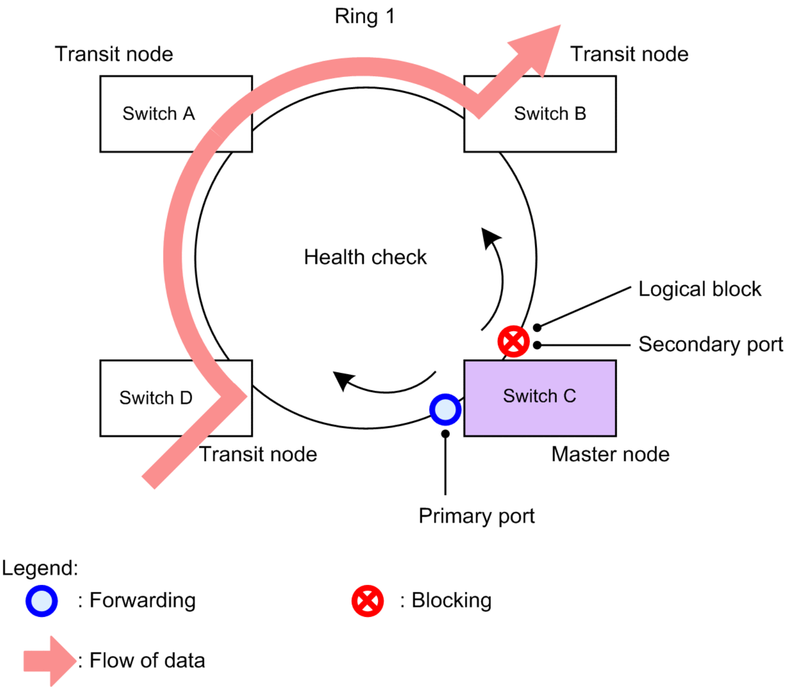
⊗ : Blocking

Figure 23-2: Example Ring Protocol application (part 2)



The following figure provides an overview of a ring network based on the Ring Protocol.

Figure 23-3: Overview of the Ring Protocol



Of the nodes constituting a ring, one is the master node and the others are transit nodes. The two ports connecting each node are called ring ports, and the ring ports of the master node include a primary port and a secondary port. The master node can divide a ring configuration by applying a logical block to the secondary port to prevent data frame loops. The master node regularly sends control frames (health check frames) to monitor the status within a ring, and determines whether a fault has occurred within the ring based on whether the sent health check frames have been received or not. Master nodes that detect a fault or fault restoration set or remove a logical block on the secondary port to perform path switching and restore communication.

23.1.2 Features

(1) Ethernet-based ring networks

The Ring Protocol is an Ethernet-based network redundancy protocol. Whereas conventional ring networks typically use dual-link fiber optics such as with FDDI, the Ring Protocol can be used to build ring networks using Ethernet.

(2) Simple operation method

Networks using the Ring Protocol have a simple configuration consisting of one master node and other transit nodes. Ring status monitoring (for faults and fault restoration) and path switching is primarily performed by the master node, and the other transit nodes perform path switching according to instructions from the master node.

(3) Control frames

The Ring Protocol uses its own control frames. These control frames are used for monitoring the ring status by the master node, and in instructions for path switching from the master node to transit nodes. Because control frame sending and reception is performed on a special VLAN, data frames and control frames are not sent within the same VLAN, unlike normal Spanning Tree Protocols. Also, because control frames are given processing priority, an increase in data traffic will not impact control frames.

(4) Load balancing method

Multiple VLANs used within a ring are aggregated logically by group, and data can be set to be balanced clockwise or counter-clockwise from the master node. This is useful for load balancing and dividing paths by VLAN.

23.1.3 Supported specifications

The following table describes the items and specifications supported by the Ring Protocol.

Table 23-1: Items and specifications supported by the Ring Protocol

Item		Description
Applicable layer	Layer 2	Y
	Layer 3	N
Ring configuration	Single ring	Y
	Multi-ring	Y (including multi-ring configurations with shared links)
Maximum number of ring IDs per switch		24 If the Ring Protocol is used together with a Spanning Tree Protocol or GSRP, or the multi-fault monitoring functionality is used, the number will be 8.
Ring ports (number of ports per ring ID)		2 (physical ports or link aggregations)
Number of VLANs	Number of control VLANs per ring ID	1 (default VLAN cannot be set)
	Maximum number of VLAN groups for data transfer per ring ID	2

Item		Description
	Maximum number of VLAN mappings per VLAN group for data transfer	128
	Maximum number of VLANs per VLAN mapping	1023
Health-check frame sending interval		200 to 60000 ms, in 1 ms increments
Fault monitoring time		500 to 300000 ms, in 1 ms increments
Load balancing method		Possible when two VLAN groups for data transfer are used
Multi-fault monitoring functionality	Number of multi-fault monitoring-enabled rings per switch	4
	Number of multi-fault monitoring VLANs per ring ID	1 (default VLAN cannot be set)
	Multi-fault monitoring frame sending interval	500 to 60000 ms, in 1 ms increments
	Multi-fault monitoring time	1000 to 300000 ms, in 1 ms increments

Legend: Y: Supported, N: Not supported

23.2 Basic Ring Protocol principles

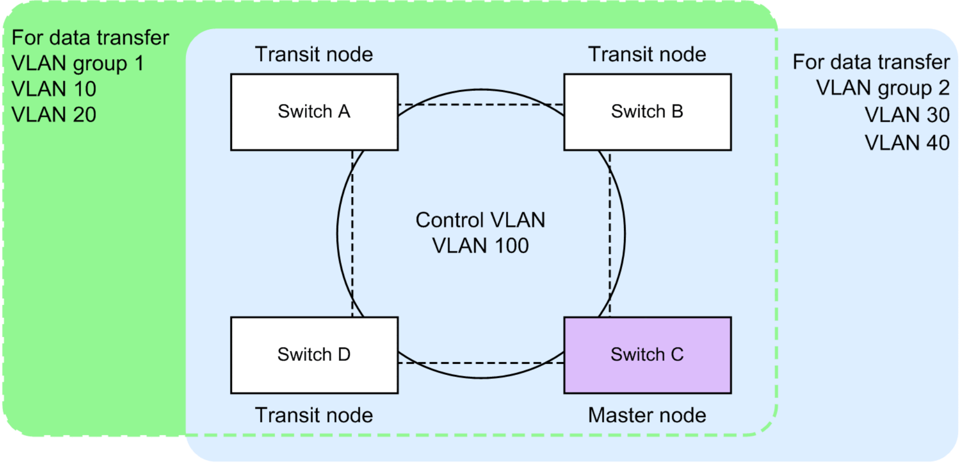
23.2.1 Network configuration

The following shows the basic network configuration for when the Ring Protocol is used.

(1) Single ring configuration

The following figure shows a single ring configuration.

Figure 23-4: Single ring configuration

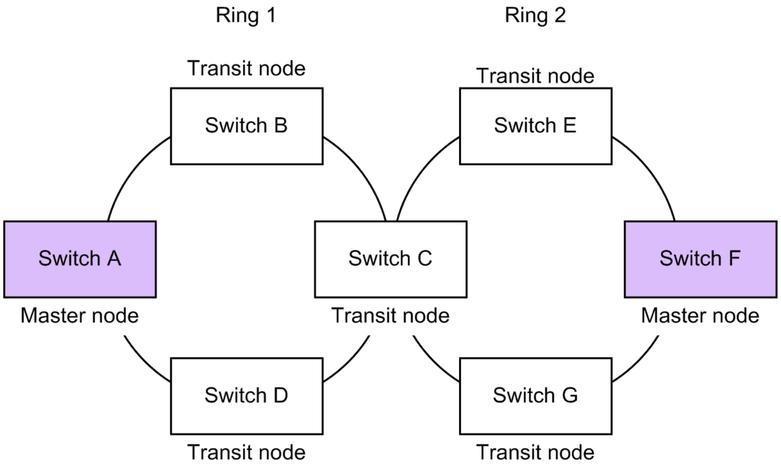


A single ring configuration consisting of one master node and multiple transit nodes is called a single ring configuration. The nodes in the ring are connected as ring ports by physical ports or link aggregations. Note that the same VLAN must be used as the control VLAN for all nodes in the ring, and a common VLAN must be used for data frame transfer. Control frames sent from the master node are circulated within the control VLAN. The VLANs used to send and receive data frames are aggregated into a single logical group called a VLAN group. VLAN groups can group multiple VLANs, and set a maximum of two groups for clockwise and counter-clockwise circulation in a single ring from the master node.

(2) Multi-ring configurations

Of the possible multi-ring configurations, the following figure shows one in which a single node is the contact point for the neighboring ring.

Figure 23-5: Multi-ring configurations

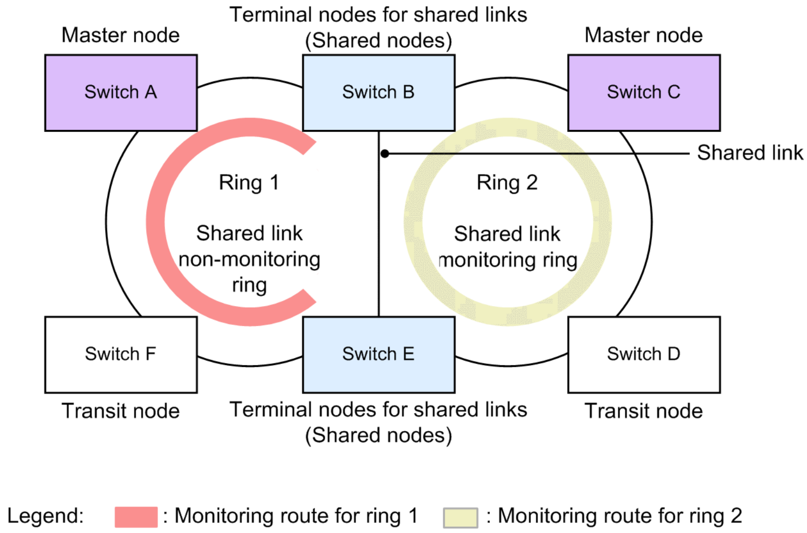


Each node in the ring runs as a single independent ring. Therefore, ring fault detection and recovery detection are performed independently by each ring.

(3) Multi-ring configurations with shared links

Of the possible multi-ring configurations, the following figure shows one in which multiple nodes are the contact points for the neighboring ring.

Figure 23-6: Multi-ring configurations with shared links



When multiple single rings are connected by multiple nodes, links are shared by multiple rings. These links are called shared links, and multi-ring configuration with these links is called a multi-ring configuration with shared links. On the other hand, when, as in (2), multiple single rings are connected by a single node, because no shared links exist, this is called a multi-ring configuration without shared links.

In a multi-ring configuration with shared links, when a common VLAN on a neighboring ring is used as a VLAN group for data transfer and a fault occurs for a shared link, the neighboring ring detects that a fault has occurred on each master node, and a loop spanning multiple rings (known as a super loop) occurs. Therefore, unlike a single ring configuration, this configuration requires that fault detection and switching operations be performed.

With the Ring Protocol, of the multiple rings for which shared links are a part of the ring, one ring is monitored for shared link faults and restoration (shared link monitoring ring), and the other rings are not monitored for shared link faults or restoration (shared link non-monitoring rings). Also, the nodes placed at both ends of a shared link are called terminal nodes (or shared nodes) in shared link non-monitoring rings. Here, because the monitored rings are unique within the master node for each ring, loops caused by faults between shared links can be prevented.

23.2.2 Control VLAN

In a network using the Ring Protocol, a special VLAN for sending and receiving control frames is used to restrict the range for sending control frames. These VLANs are called control VLANs, and the same VLAN is used for all nodes constituting a ring. Because control VLANs use a single common VLAN for each ring, in a multi-ring configuration, different VLANs need to be used in neighboring rings.

23.2.3 Fault monitoring methods

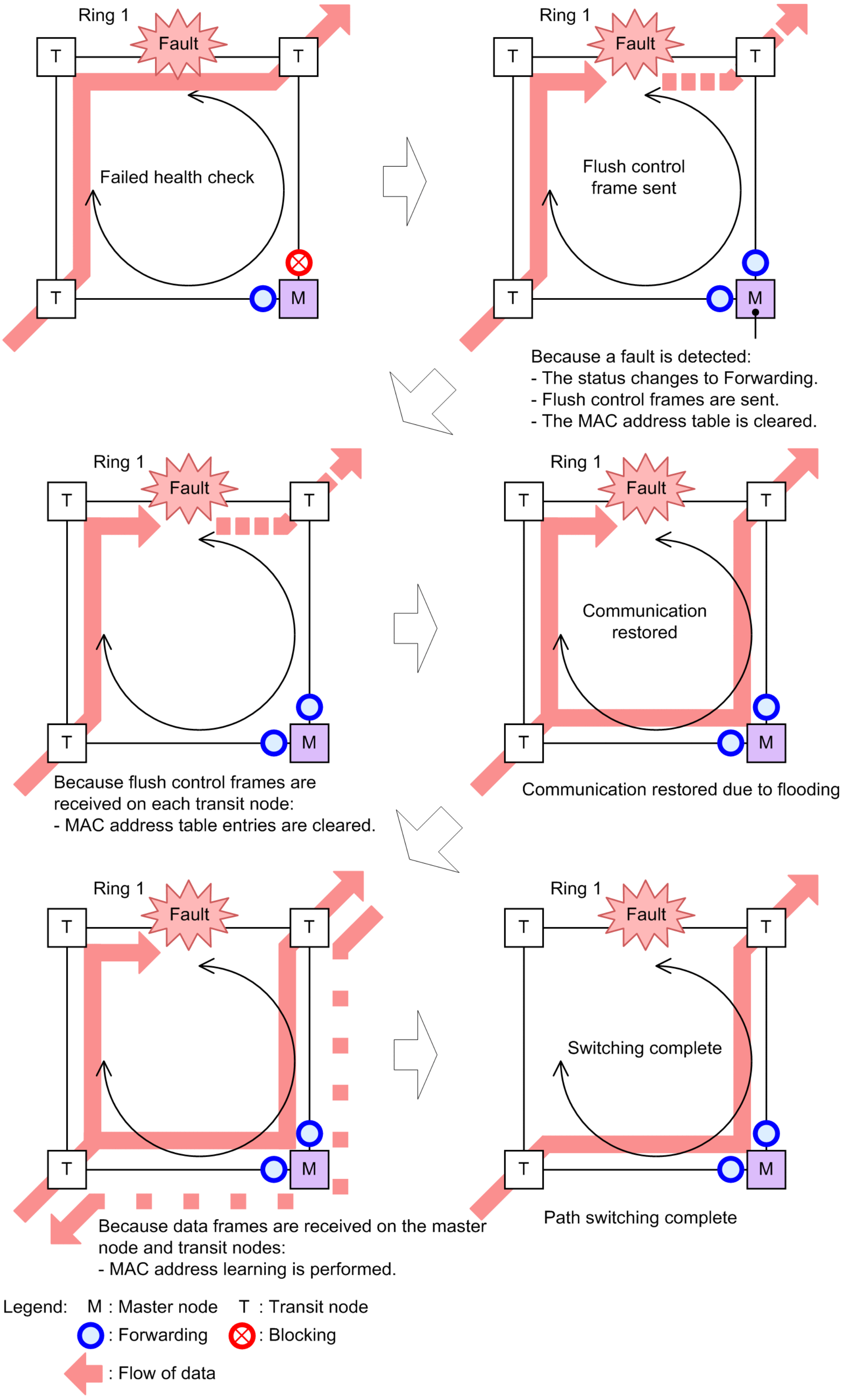
Ring faults are monitored under the Ring Protocol by having the master node regularly send control frames called health check frames, and then monitor whether or not these health check frames were received. When a health check frame does not arrive within a fixed time, the master node determines that a ring fault has occurred, and performs fault operations. Also, when a health check frame is received again during a ring fault, the master node determines recovery from the ring fault, and performs restoration operations.

23.2.4 Switching communication paths

In order to switch to an alternate path when a ring fault is detected, a master node changes the status of the secondary port from `Blocking` to `Forwarding`. Likewise, in order to perform path switch-back after recovery from the ring fault is detected, the master node changes the secondary port from `Forwarding` to `Blocking`. Therefore, in order to promptly restore communication, the MAC address table entries are cleared for all nodes in the ring. If MAC address table entries are not cleared, because data frames are sent according to the information before switching (or switch-back), data might not be received properly. Therefore, to restore communication, the MAC address table entries for all nodes in a ring are cleared.

The following figure shows the switching operations for both master nodes and transit nodes.

Figure 23-7: Overview of path switching for the Ring Protocol



Because a fault is detected:
- The status changes to Forwarding.
- Flush control frames are sent.
- The MAC address table is cleared.

Because flush control frames are received on each transit node:
- MAC address table entries are cleared.

Communication restored due to flooding

Because data frames are received on the master node and transit nodes:
- MAC address learning is performed.

Path switching complete

(1) Switching paths for master nodes

When a ring fault is detected on the master node, `Blocking` is removed for the secondary port, and the MAC address table entries are cleared for the ring port. Because of this, flooding occurs until MAC address learning is performed. MAC address learning is performed by sending and receiving frames over the secondary port, and switching is completed to a new path.

(2) Switching paths for transit nodes

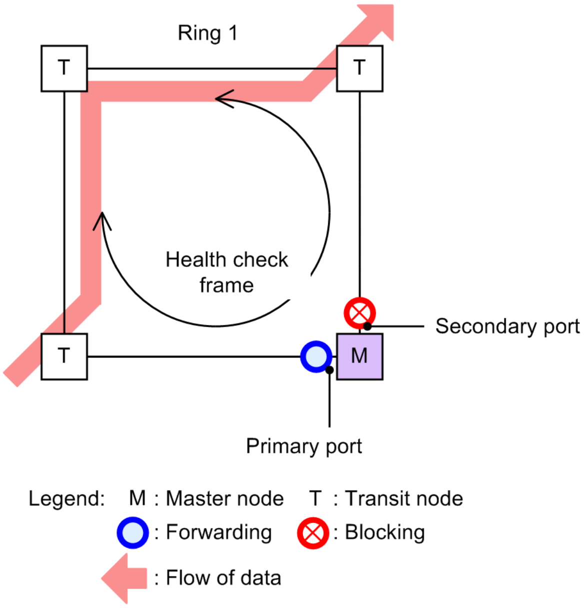
When a ring fault is detected on the master node, a control frame called a flush control frame is sent to other transit nodes in the ring of the same control VLAN, to request that MAC address table entries be cleared. When this flush control frame is received, MAC address table entries are cleared for the ring port. Because of this, flooding occurs until MAC address learning is performed. MAC address learning is performed by sending and receiving frames on the new path, and communication path switching is completed.

23.3 Overview of single ring operation

23.3.1 Normal ring operation

The following figure shows normal operation for a single ring.

Figure 23-8: Normal ring operation



(1) Master node operation

To prevent fault misdetection due to one-way link faults, health check frames are sent from two ring ports. Monitoring is performed to check that health check frames in both directions are received within the pre-determined time. Data frame transfer is performed on the primary port. Because the secondary port is logically blocked, data frame transfer and MAC address learning are not performed.

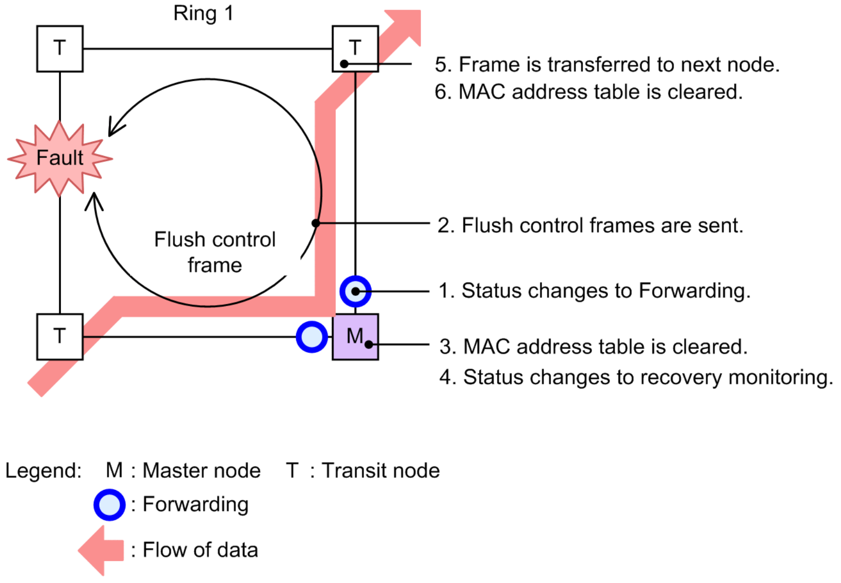
(2) Transit node operation

Health check frames sent by the master node are not monitored on transit nodes. When a health check frame is received, it is transferred to the next node in the ring. Data frame transfer is performed on both ring ports.

23.3.2 Operation when a fault is detected

The following figure shows operation when a ring fault has been detected for a single ring.

Figure 23-9: Operation during a ring fault


Ring 1
T
T
T
M
Fault
Flush control frame
5. Frame is transferred to next node.
6. MAC address table is cleared.
2. Flush control frames are sent.
1. Status changes to Forwarding.
3. MAC address table is cleared.
4. Status changes to recovery monitoring.
Legend: M : Master node T : Transit node
: Forwarding
: Flow of data

(1) Master node operation

A fault is determined to have occurred when health check frames in both directions are not received within the pre-determined time. Switching operation is performed as follows on the master node that detects the fault:

1. The VLAN status of the ring for data transfer is changed.

The ring VLAN status for the secondary port is changed from `Blocking` to `Forwarding`. The ring VLAN status when a fault is detected is changed as shown in the following table.

Table 23-2: VLAN status of rings for data transfer when a fault is detected

Ring port	Before (normal)	After (fault)
Primary port	Forwarding	Forwarding
Secondary port	Blocking	Forwarding

2. Flush control frames are sent.

Flush control frames are sent from the primary port and secondary port of the master node.

3. The MAC address table is cleared.

The MAC address table entries pertaining to the ring port are cleared. Clearing the MAC address table entries allows paths to be switched quickly.

4. The monitoring status is changed.

When a ring fault is detected, the master node changes from the fault monitoring status to the recovery monitoring status.

(2) Transit node operation

The following operation is performed on a transit node that receives a flush control frame sent from a master node detecting a fault:

5. Flush control frames are transferred.

Any received flush control frames are transferred to the next node.

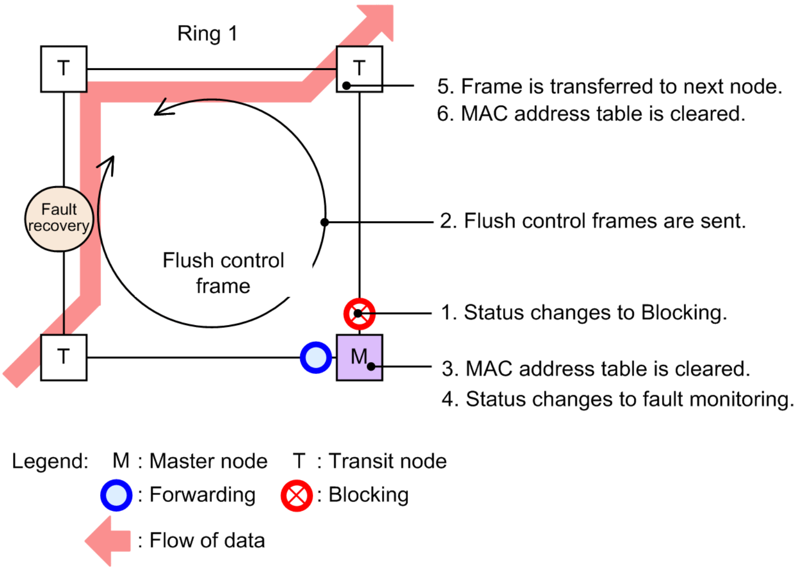
6. The MAC address table is cleared.

The MAC address table entries pertaining to the ring port are cleared. Clearing the MAC address table entries allows paths to be switched quickly.

23.3.3 Operation when recovery is detected

The following figure shows operation when recovery from a ring fault is detected for a single ring.

Figure 23-10: Operation during fault recovery


Ring 1
T
T
T
M
Fault recovery
Flush control frame
5. Frame is transferred to next node.
6. MAC address table is cleared.
2. Flush control frames are sent.
1. Status changes to Blocking.
3. MAC address table is cleared.
4. Status changes to fault monitoring.
Legend: M : Master node T : Transit node
○ : Forwarding ⊗ : Blocking
: Flow of data

(1) Master node operation

When a ring fault has been detected, and a health check frame sent by the current node is received, recovery from the ring fault is determined, and the following restoration operations are performed:

1. The VLAN status of the ring for data transfer is changed.

The ring VLAN status for the secondary port is changed from `Forwarding` to `Blocking`. The ring VLAN status when a recovery is detected is changed as shown in the following table.

Table 23-3: VLAN status of rings for data transfer when a recovery is detected

Ring port	Before (normal)	After (fault)
Primary port	Forwarding	Forwarding
Secondary port	Forwarding	Blocking

2. Flush control frames are sent.

Flush control frames are sent from the primary port and secondary port of the master node. Note that during recovery from the ring fault, any flush control frames transferred by each transit node return to the master node, and are discarded.

3. The MAC address table is cleared.

The MAC address table entries pertaining to the ring port are cleared.

Clearing the MAC address table entries allows paths to be switched quickly.

4. The monitoring status is changed.

When recovery from the ring fault is detected, the master node changes from the recovery monitoring status to the fault monitoring status.

(2) Transit node operation

The following operations are performed on a transit node that receives a flush control frame sent from a master node:

5. Flush control frames are transferred.

   Any received flush control frames are transferred to the next node.

6. The MAC address table is cleared.

   The MAC address table entries pertaining to the ring port are cleared.

   Clearing the MAC address table entries allows paths to be switched quickly.

To prevent loops on transit nodes for which a link fault has occurred and for which recovery has then been performed, the ring VLAN status of the ring port is changed to `Blocking`. This `Blocking` status is cleared when a flush control frame sent by the master node is received, or a timeout occurs on the transit node for the reception hold time for flush control frames (`forwarding-shift-time`) of the ring port. The reception hold time for flush control frames (`forwarding-shift-time`) is set when recovery from a link fault on a ring port has occurred.

23.3.4 Operation when path switch-back is suppressed and cleared

When the path switch-back suppression functionality is applied and a ring fault is detected on a master node, the master node status changes to recovery from restoration suppression, and the master node does not perform restoration operations immediately. To enable this functionality, the `preempt-delay` configuration command must be set.

The path switch-back suppression status is cleared when the following occur:

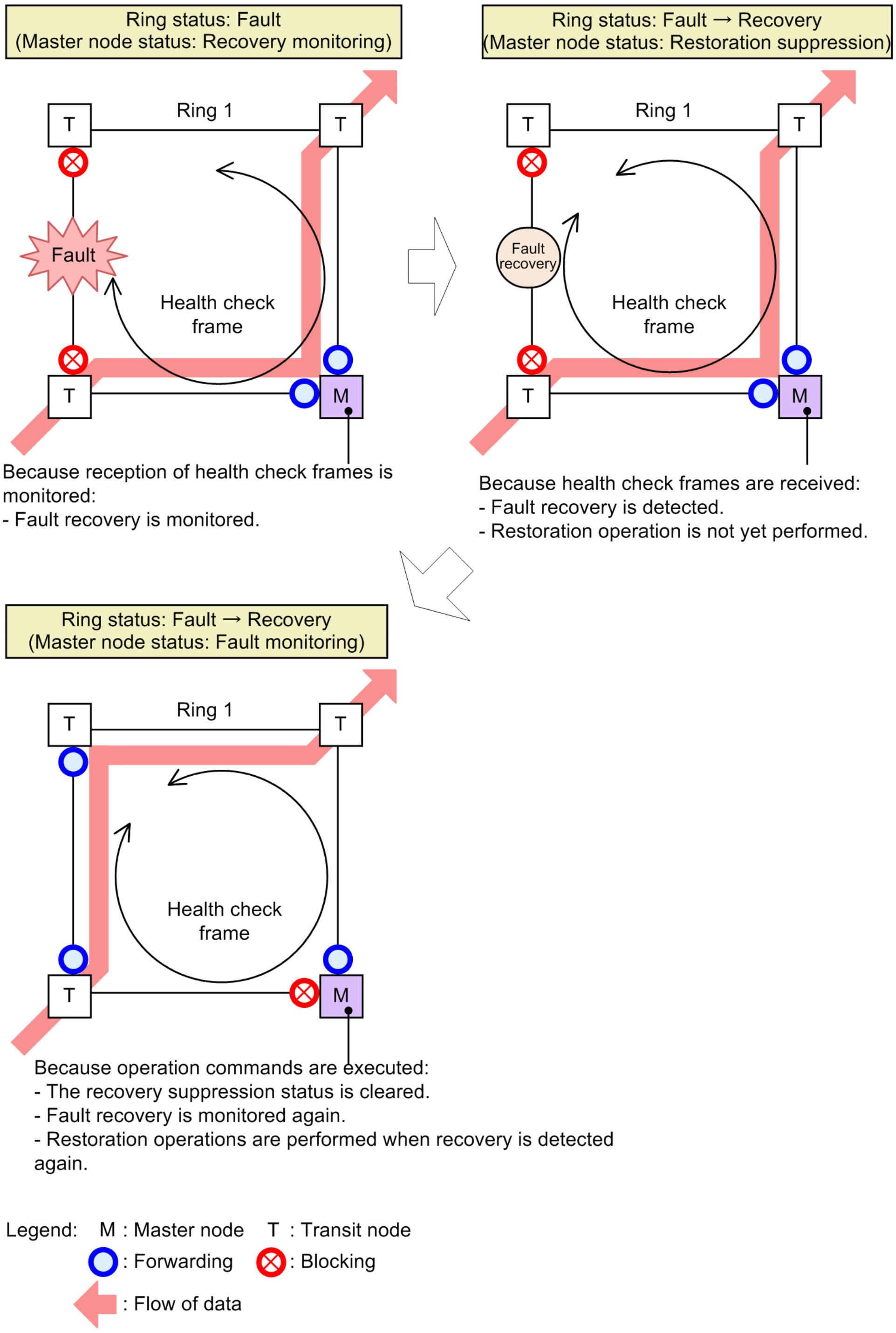
- Path switch-back suppression is cleared by executing the `clear axrp preempt-delay` operation command
- The path switch-back suppression time specified by the `preempt-delay` configuration command elapses
- The `preempt-delay` configuration command enabling path switch-back suppression functionality is deleted

When the restoration suppression status is cleared, the master node switches to the recovery monitoring status again. Then restoration operations are performed if recovery from the ring fault is detected again. When the restoration is completed, the master node switches to the fault monitoring status.

Even if a ring fault is detected in the path switch-back suppression status, the master node status remains recovery suppression. When the `clear axrp preempt-delay` operation command is executed to clear the path switch-back suppression status, the master node status changes to recovery monitoring again. Here, because ring fault recovery is not detected, restoration operations are not performed. Then, after recovery from all faults on the ring network, the master node detects fault recovery, and performs restoration operations instantly.

The figure below shows the operations performed when the `clear axrp preempt-delay` operation command is executed to clear path switch-back suppression. The same operation is performed when this status is cleared by other means.

Figure 23-11: Operation when operation commands are executed to clear path switch-back suppression



Ring status: Fault
(Master node status: Recovery monitoring)
Ring 1
T
T
T
M
Fault
Health check frame
Ring status: Fault → Recovery
(Master node status: Restoration suppression)
Ring 1
T
T
T
M
Fault recovery
Health check frame
Ring status: Fault → Recovery
(Master node status: Fault monitoring)
Ring 1
T
T
T
M
Health check frame
Legend: M : Master node T : Transit node
: Forwarding
: Blocking
: Flow of data

Because reception of health check frames is monitored:
- Fault recovery is monitored.

Because health check frames are received:
- Fault recovery is detected.
- Restoration operation is not yet performed.

Because operation commands are executed:
- The recovery suppression status is cleared.
- Fault recovery is monitored again.
- Restoration operations are performed when recovery is detected again.

The switch-back suppression status is also cleared for paths, and the master node status changes to fault monitoring status when the following events occur:

- A device starts up (including by execution of the `reload` and `ppupdate` operation commands).
- Reflecting to configuration file operation (executing the `copy` operation command)
- A Ring Protocol program is restarted (including by execution of the `restart axrp` operation command).

- A VLAN program is restarted (including by execution of the `restart vlan` operation command).

23.4 Overview of multi-ring operation

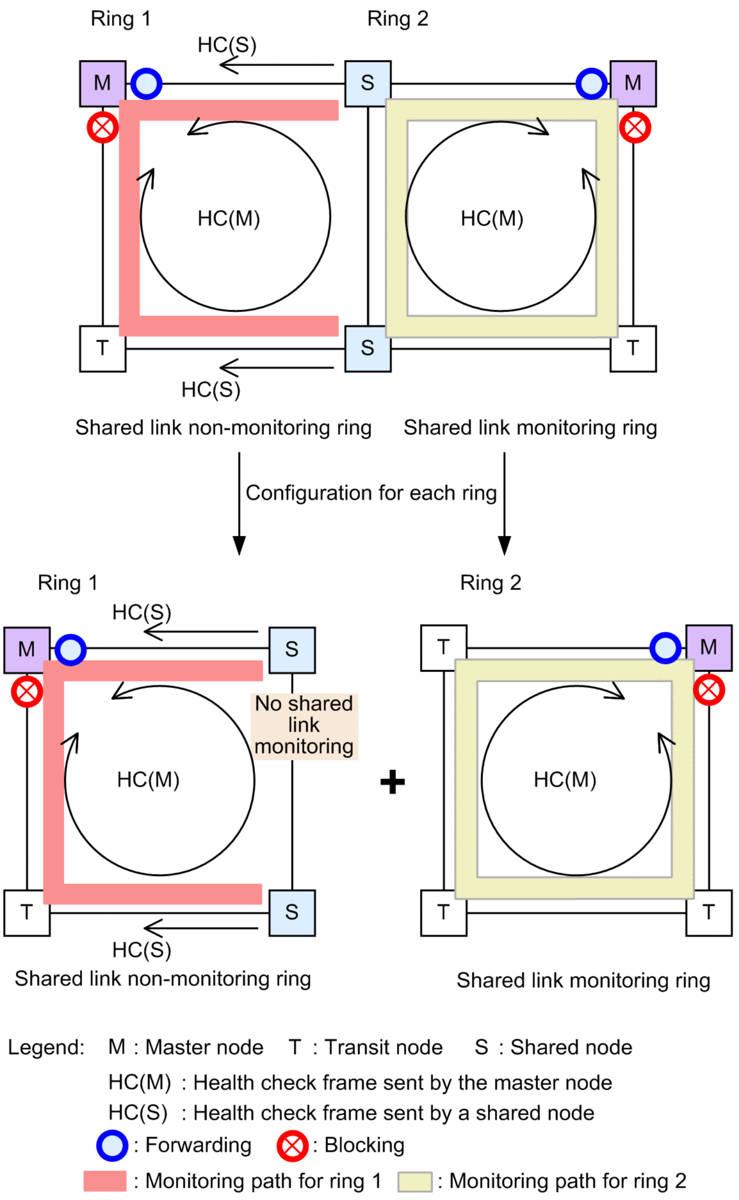
The following explains multi-ring configurations, focusing on those with shared links. For details about multi-ring configurations without shared links, because operation is the same as for single rings, see *23.3 Overview of single ring operation*.

From this section on, HC is used to refer to a health check frame, HC(M) is used to refer to a health check frame sent by the master node, and HC(S) is used to refer to a health check frame sent by a shared node.

23.4.1 Normal ring operation

The following figure shows normal operation for a multi-ring configuration with shared links.

Figure 23-12: Normal ring status

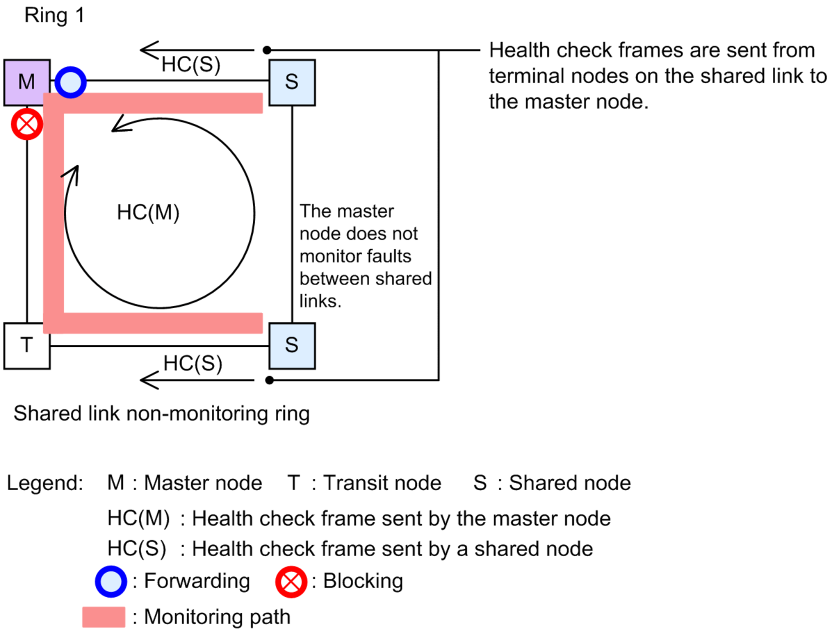

Ring 1
Ring 2
HC(S)
M
S
M
HC(M)
HC(M)
T
S
T
HC(S)
Shared link non-monitoring ring
Shared link monitoring ring
Configuration for each ring
Ring 1
Ring 2
HC(S)
M
S
T
M
No shared link monitoring
HC(M)
HC(M)
+
T
S
T
T
HC(S)
Shared link non-monitoring ring
Shared link monitoring ring
Legend: M : Master node T : Transit node S : Shared node
HC(M) : Health check frame sent by the master node
HC(S) : Health check frame sent by a shared node
○ : Forwarding ⊗ : Blocking
🟥 : Monitoring path for ring 1 🟨 : Monitoring path for ring 2

(1) Shared link non-monitoring rings

A shared link non-monitoring ring consists of one master node and multiple transit nodes.

However, to provide assistance because shared link faults are not monitored, health check frames are sent to the master node from the terminal nodes (shared nodes) of the shared link non-monitoring ring placed at both ends of the shared link. Of the two ring ports, these health check frames are sent from the ring port that is not a shared link. This means that when a fault occurs on a shared link, even though the master node of the shared link non-monitoring ring can no longer receive the health check frames it sent itself, fault detection can be prevented while health check frames can be received from the terminal nodes (shared nodes) of the shared link non-monitoring ring.

Figure 23-13: Normal operation for shared link non-monitoring rings


Ring 1
HC(S)
M
S
Health check frames are sent from terminal nodes on the shared link to the master node.
HC(M)
The master node does not monitor faults between shared links.
T
S
HC(S)
Shared link non-monitoring ring
Legend: M : Master node T : Transit node S : Shared node
HC(M) : Health check frame sent by the master node
HC(S) : Health check frame sent by a shared node
○ : Forwarding ⊗ : Blocking
▬ : Monitoring path

(a) Master node operation

To prevent fault misdetection due to one-way link faults, health check frames (HC(M)s) are sent from two ring ports. Monitoring is performed to check that HC(M)s in both directions are received within the pre-determined time. Aside from the HC(M)s sent from the master node, reception is also monitored for health check frames (HC(S)s) sent from the terminal nodes (shared nodes) of the shared link non-monitoring ring placed at both ends of a shared link. Data frame transfer is performed on the primary port. Because the secondary port is logically blocked, data frame transfer and MAC address learning are not performed.

(b) Transit node operation

Transit node operation is the same as for single rings. Transit nodes do not monitor HC(M)s and HC(S)s. When an HC(M) or HC(S) is received, it is transferred to the next node in the ring. Data frame transfer is performed on both ring ports.

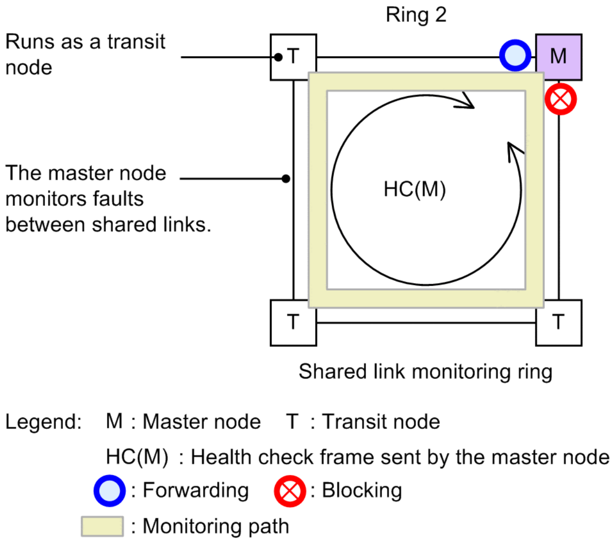
(c) Terminal node operation for shared link non-monitoring rings

Terminal nodes (shared nodes) for shared link non-monitoring rings send HC(S)s to the master node in shared link non-monitoring rings. Of the two ring ports, these HC(S)s are sent to the one that is not a shared link. The HC(M)s sent and data frames transferred by master nodes are the same as for transit nodes.

(2) Shared link monitoring rings

Like single rings, shared link monitoring rings consist of one master node and multiple transit nodes. The nodes placed at both ends of a shared link run the same as for a single ring, as master nodes or transit nodes.

Figure 23-14: Normal operation for shared link monitoring rings


Ring 2
Runs as a transit node
T
M
The master node monitors faults between shared links.
HC(M)
T
T
Shared link monitoring ring
Legend: M : Master node T : Transit node
HC(M) : Health check frame sent by the master node
: Forwarding
: Blocking
: Monitoring path

(a) Master node operation

To prevent fault misdetection due to one-way link faults, health check frames (HC(M)s) are sent from two ring ports. Monitoring is performed to check that HC(M)s in both directions are received within the pre-determined time. Data frame transfer is performed on the primary port. Because the secondary port is logically blocked, data frame transfer and MAC address learning are not performed.

(b) Transit node operation

Transit node operation is the same as for single rings. Transit nodes do not monitor the HC(M)s sent by the master node. When an HC(M) is received, it is transferred to the next node in the ring. Data frame transfer is performed on both ring ports.

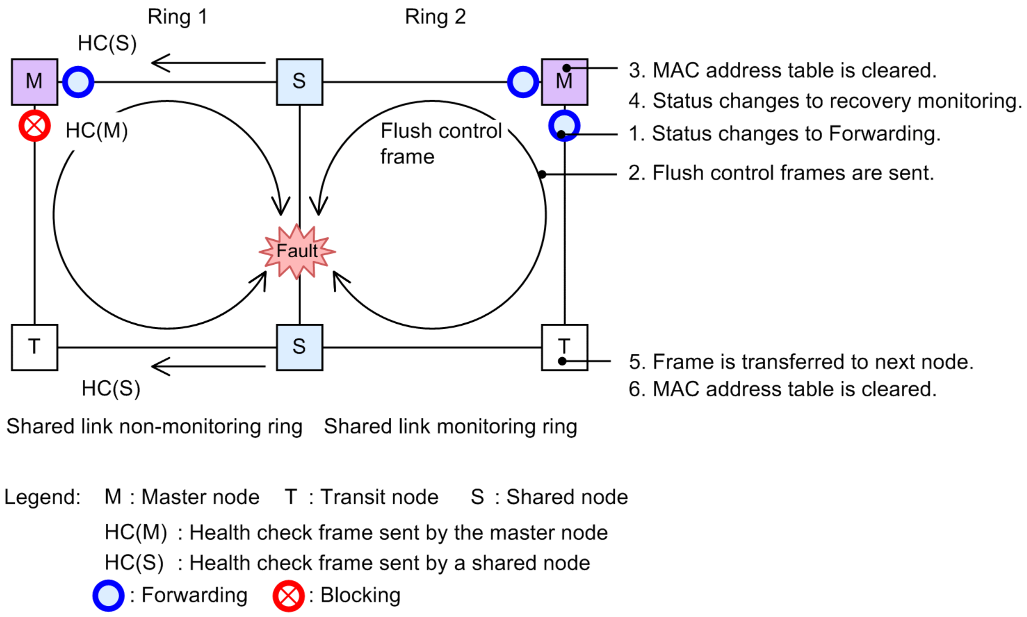
23.4.2 Operation for shared link faults and restoration

The following explains faults and restoration operations when a fault occurs between shared links for a multi-ring configuration with shared links.

(1) Operation when a fault is detected

The following figure shows operation for when a shared link fault is detected.

Figure 23-15: Operation during shared link faults


Ring 1
Ring 2
HC(S)
M
S
M
3. MAC address table is cleared.
4. Status changes to recovery monitoring.
HC(M)
Flush control frame
1. Status changes to Forwarding.
2. Flush control frames are sent.
Fault
T
S
T
5. Frame is transferred to next node.
6. MAC address table is cleared.
HC(S)
Shared link non-monitoring ring
Shared link monitoring ring
Legend: M : Master node T : Transit node S : Shared node
HC(M) : Health check frame sent by the master node
HC(S) : Health check frame sent by a shared node
○ : Forwarding ⊗ : Blocking

(a) Master node operation for shared link monitoring rings

When a fault occurs on a shared link, the master node can no longer receive HC(M)s from both directions, and a ring fault is detected. As with a single ring, the following fault operations are performed for the master node detecting the fault:

1. The VLAN status of the ring for data transfer is changed.
2. Flush control frames are sent.
3. The MAC address table is cleared.
4. The monitoring status is changed.

(b) Transit node operation for shared link monitoring rings

As with single rings, the following operations are performed when a flush control frame sent from the master node is received:

5. Flush control frames are transferred.
6. The MAC address table is cleared.

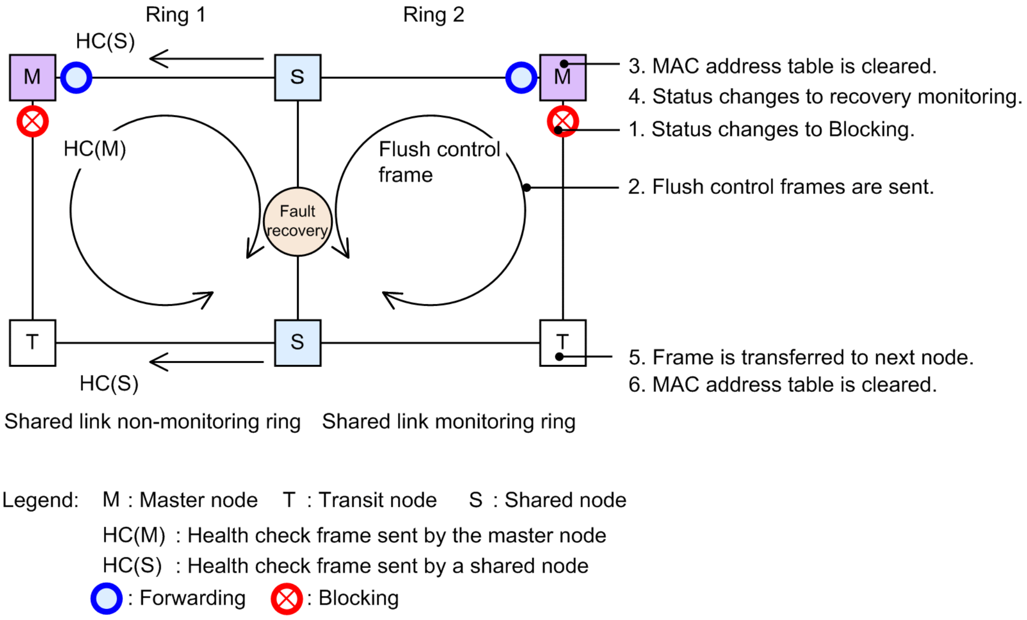
(c) Master node and transit node operation for shared link non-monitoring rings

Because the master node in a shared link non-monitoring ring does not detect ring faults for shared links, no fault operations are performed. Therefore, path switching does not occur for transit nodes.

(2) Operation when recovery is detected

The following figure shows operation when recovery from a fault is detected for a shared link.

Figure 23-16: Operation during shared link recovery


Ring 1
Ring 2
HC(S)
M
S
M
3. MAC address table is cleared.
4. Status changes to recovery monitoring.
1. Status changes to Blocking.
HC(M)
Flush control frame
2. Flush control frames are sent.
Fault recovery
T
S
T
5. Frame is transferred to next node.
6. MAC address table is cleared.
HC(S)
Shared link non-monitoring ring
Shared link monitoring ring
Legend: M : Master node T : Transit node S : Shared node
HC(M) : Health check frame sent by the master node
HC(S) : Health check frame sent by a shared node
: Forwarding
: Blocking

(a) Master node operation for shared link monitoring rings

When a ring fault has been detected, and the master node receives an HC(M) it sent itself, it determines that recovery from the ring fault has occurred. As with a single ring, the following restoration operations are performed:

1. The VLAN status of the ring for data transfer is changed.
2. Flush control frames are sent.
3. The MAC address table is cleared.
4. The monitoring status is changed.

(b) Transit node operation for shared link monitoring rings

As with single rings, the following operations are performed when a flush control frame sent from the master node is received:

5. Flush control frames are transferred.
6. The MAC address table is cleared.

(c) Master node and transit node operation for shared link non-monitoring rings

Because the master node in a shared link non-monitoring ring does not detect ring faults, no restoration is performed, including for transit nodes.

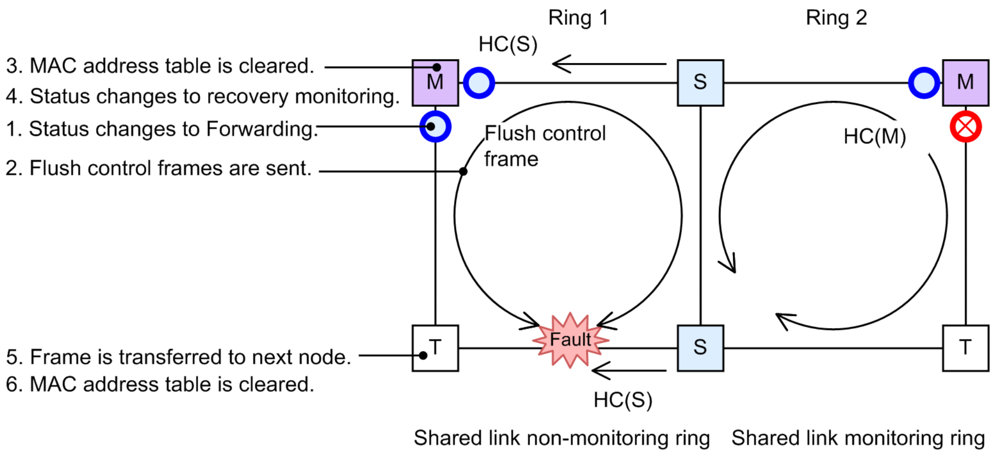
23.4.3 Operation for faults and restoration other than for shared links in a shared link non-monitoring ring

The following explains faults and restoration other than for shared links, for shared link non-monitoring rings.

(1) Operation when a fault is detected

The following figure shows operation when a fault is detected other than for shared links on shared link non-monitoring rings.

Figure 23-17: Operation during a ring fault other than for shared links on shared link non-monitoring rings


Ring 1
Ring 2
HC(S)
3. MAC address table is cleared.
4. Status changes to recovery monitoring.
1. Status changes to Forwarding.
2. Flush control frames are sent.
M
S
M
Flush control frame
HC(M)
5. Frame is transferred to next node.
6. MAC address table is cleared.
T
Fault
S
T
HC(S)
Shared link non-monitoring ring
Shared link monitoring ring

Legend: M : Master node T : Transit node S : Shared node
HC(M) : Health check frame sent by the master node
HC(S) : Health check frame sent by a shared node
○ : Forwarding ⊗ : Blocking

(a) Master node operation for shared link non-monitoring rings

The master node of a shared link non-monitoring ring detects a ring fault when it receives neither the two-way HC(M) sent by itself nor the HC(S) sent by a shared node. As with a single ring, the following operations are performed for the master node detecting the fault:

1. The VLAN status of the ring for data transfer is changed.
2. Flush control frames are sent.
3. The MAC address table is cleared.
4. The monitoring status is changed.

(b) Transit node and shared node operation for shared link non-monitoring rings

As with single rings, the following operations are performed when a flush control frame sent from the master node is received:

5. Flush control frames are transferred.
6. The MAC address table is cleared.

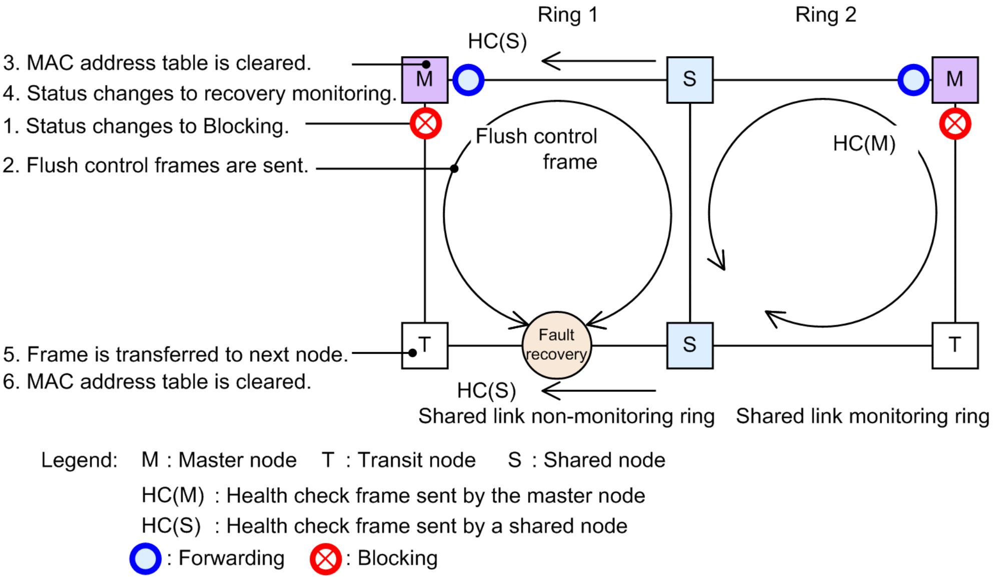
(c) Master node and transit node operation for shared link monitoring rings

Because no faults occur within a shared link monitoring ring, fault operation is not performed.

(2) Operation when recovery is detected

The following figure shows operation when a fault is restored other than for shared links in a shared link non-monitoring ring.

Figure 23-18: Operation for recovery from a ring fault other than for shared links in a shared link non-monitoring ring


Ring 1
Ring 2
HC(S)
3. MAC address table is cleared.
4. Status changes to recovery monitoring.
1. Status changes to Blocking.
2. Flush control frames are sent.
M
S
M
Flush control frame
HC(M)
5. Frame is transferred to next node.
6. MAC address table is cleared.
T
Fault recovery
S
T
HC(S)
Shared link non-monitoring ring
Shared link monitoring ring
Legend: M : Master node T : Transit node S : Shared node
HC(M) : Health check frame sent by the master node
HC(S) : Health check frame sent by a shared node
: Forwarding
: Blocking

(a) Master node operation for shared link non-monitoring rings

When a ring fault has been detected, and either the master node receives an HC(M) that it sent itself, or an HC(S) sent by shared nodes are received from both directions, recovery from the ring fault is determined. As with a single ring, the following restoration operations are performed:

1. The VLAN status of the ring for data transfer is changed.
2. Flush control frames are sent.
3. The MAC address table is cleared.
4. The monitoring status is changed.

(b) Transit node and shared node operation for shared link non-monitoring rings

As with single rings, the following operations are performed when a flush control frame sent from the master node is received:

5. Flush control frames are transferred.
6. The MAC address table is cleared.

(c) Master node and transit node operation for shared link monitoring rings

Because no faults occur within a shared link monitoring ring, restoration is not performed.

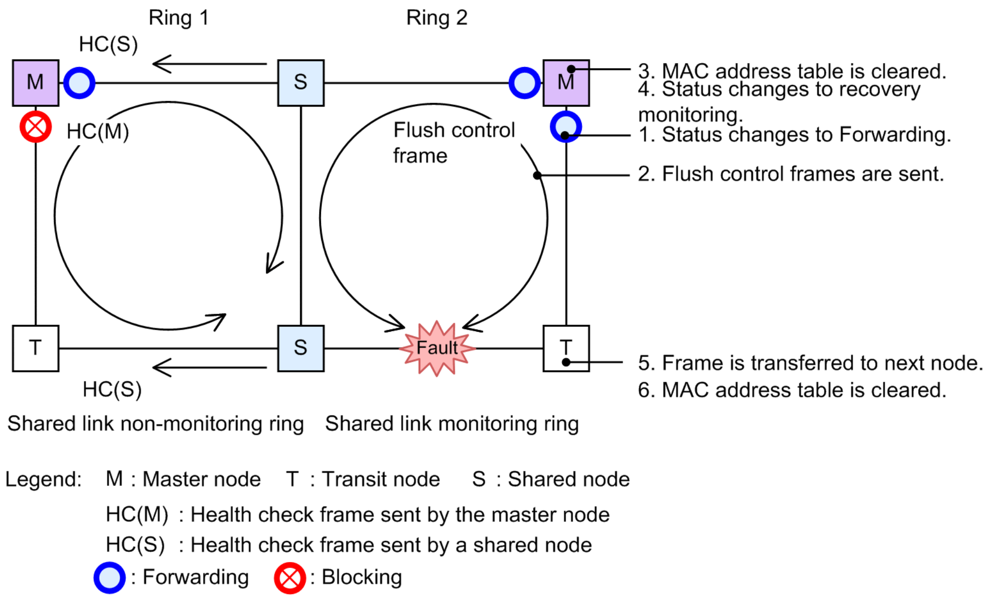
23.4.4 Faults and restoration other than for shared links in a shared link monitoring ring

The following explains faults and restoration other than for shared links in a shared link monitoring ring.

(1) Operation when a fault is detected

The following figure shows operation when a fault is detected other than for shared links in a shared link monitoring ring.

Figure 23-19: Operation during ring faults other than for shared links in a shared link monitoring ring


Ring 1
Ring 2
HC(S)
M
S
M
HC(M)
Flush control frame
3. MAC address table is cleared.
4. Status changes to recovery monitoring.
1. Status changes to Forwarding.
2. Flush control frames are sent.
T
S
Fault
T
5. Frame is transferred to next node.
6. MAC address table is cleared.
HC(S)
Shared link non-monitoring ring
Shared link monitoring ring
Legend: M : Master node T : Transit node S : Shared node
HC(M) : Health check frame sent by the master node
HC(S) : Health check frame sent by a shared node
○ : Forwarding
⊗ : Blocking

(a) Master node operation for shared link monitoring rings

When a fault is detected in a shared link monitoring ring, the master node can no longer receive HC(M)s from both directions, and detects a ring fault. As with a single ring, the following fault operations are performed for the master node detecting the fault:

1. The VLAN status of the ring for data transfer is changed.
2. Flush control frames are sent.
3. The MAC address table is cleared.
4. The monitoring status is changed.

(b) Transit node operation for shared link monitoring rings

As with single rings, the following operations are performed when a flush control frame sent from the master node is received:

5. Flush control frames are transferred.
6. The MAC address table is cleared.

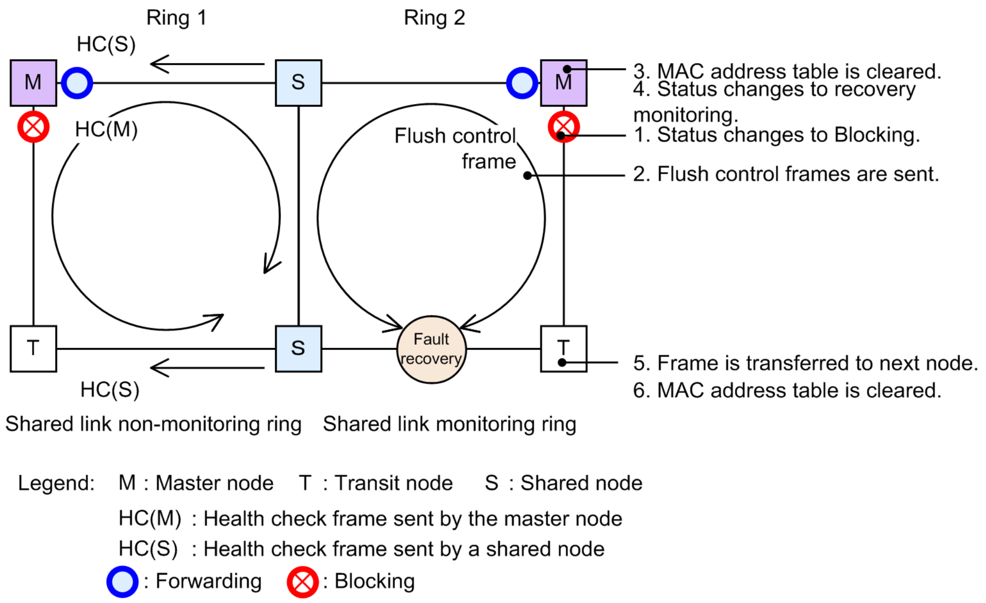
(c) Master node and transit node (shared node) operation for shared link non-monitoring rings

Because no faults occur within a shared link non-monitoring ring, fault operation is not performed.

(2) Operation when recovery is detected

The following figure shows operation for recovery from a fault other than for shared links in a shared link monitoring ring.

Figure 23-20: Operation for recovery from a ring fault other than for shared links in a shared link monitoring ring


Ring 1
Ring 2
HC(S)
M
S
M
HC(M)
Flush control frame
3. MAC address table is cleared.
4. Status changes to recovery monitoring.
1. Status changes to Blocking.
2. Flush control frames are sent.
T
S
Fault recovery
T
5. Frame is transferred to next node.
6. MAC address table is cleared.
HC(S)
Shared link non-monitoring ring
Shared link monitoring ring
Legend: M : Master node T : Transit node S : Shared node
HC(M) : Health check frame sent by the master node
HC(S) : Health check frame sent by a shared node
○ : Forwarding ⊗ : Blocking

(a) Master node operation for shared link monitoring rings

When a ring fault has been detected, and the master node receives an HC(M) it sent itself, it determines that recovery from the ring fault has occurred. As with a single ring, the following restoration operations are performed:

1. The VLAN status of the ring for data transfer is changed.
2. Flush control frames are sent.
3. The MAC address table is cleared.
4. The monitoring status is changed.

(b) Transit node operation for shared link monitoring rings

As with single rings, the following operations are performed when a flush control frame sent from the master node is received:

5. Flush control frames are transferred.
6. The MAC address table is cleared.

(c) Master node and transit node (shared node) operation for shared link non-monitoring rings

Because faults do not occur within a shared link non-monitoring ring, restoration is not performed.

23.4.5 Operation when path switch-back is suppressed and cleared

For details about path switch-back suppression and clearing for multi-ring configurations, because operation is the same as that for single rings, see *23.3 Overview of single ring operation*.

23.5 Multi-fault monitoring functionality for the Ring Protocol

23.5.1 Overview

The Multi-fault monitoring functionality monitors multi-faults for shared link monitoring rings on multi-ring configurations with shared links, and switches paths to shared link non-monitoring rings when a multi-fault is detected. Here, the shared link non-monitoring ring used for path switching is called a backup ring.

The targets of detection by the multi-fault monitoring functionality are shared link faults, other link faults within shared link monitoring rings, and device faults accompanying link faults.

The following shows an example of a fault on a shared link monitoring ring, as well as the combination of faults that can be detected by the multi-fault monitoring functionality.

Figure 23-21: Example of a fault on a shared link monitoring ring

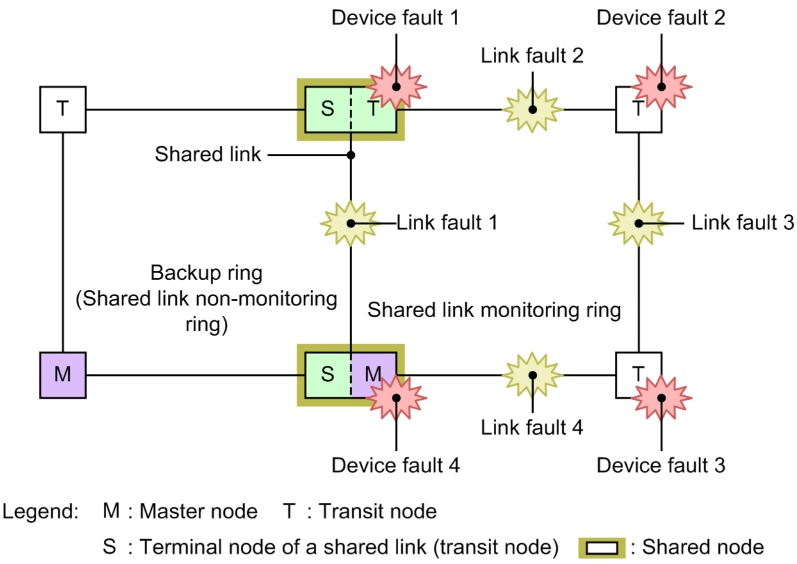

Device fault 1
Device fault 2
Link fault 2
T
S
T
T
Shared link
Link fault 1
Link fault 3
Backup ring
(Shared link non-monitoring ring)
Shared link monitoring ring
M
S
M
T
Link fault 4
Device fault 4
Device fault 3
Legend: M : Master node T : Transit node
S : Terminal node of a shared link (transit node)
: Shared node

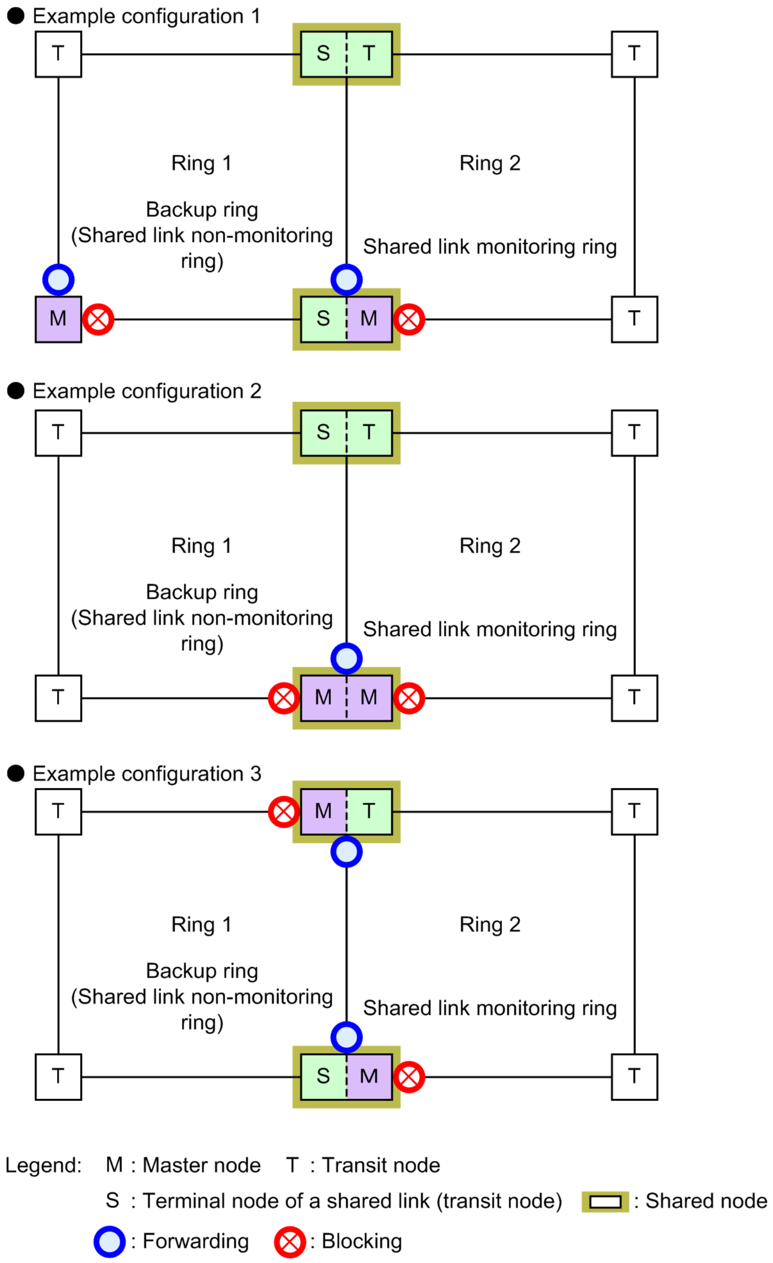
Table 23-4: Combinations of faults that can be detected by the multi-fault monitoring functionality

Failure type	Detectable combinations	
Link fault	Link fault 1 (shared link fault)	Link fault 2 (other link fault)
	Link fault 1 (shared link fault)	Link fault 3 (other link fault)
	Link fault 1 (shared link fault)	Link fault 4 (other link fault)
Device fault	Device fault 1 (shared node fault) only	
	Device fault 4 (shared node fault) only	
	Device fault 2 (transit node fault)	Link fault 1 (shared link fault)
	Device fault 3 (transit node fault)	Link fault 1 (shared link fault)

23.5.2 Basic configuration for the multi-fault monitoring functionality

The multi-ring configurations with shared links to which the multi-fault monitoring functionality can be applied are those in which the shared link non-monitoring rings used as the backup ring and the shared link monitoring ring are associated one-to-one. The shared node is set as the master node of the shared link monitoring ring. The following figure shows an example of a basic configuration for the multi-fault monitoring functionality.

Figure 23-22: Basic configuration example for the multi-fault monitoring functionality

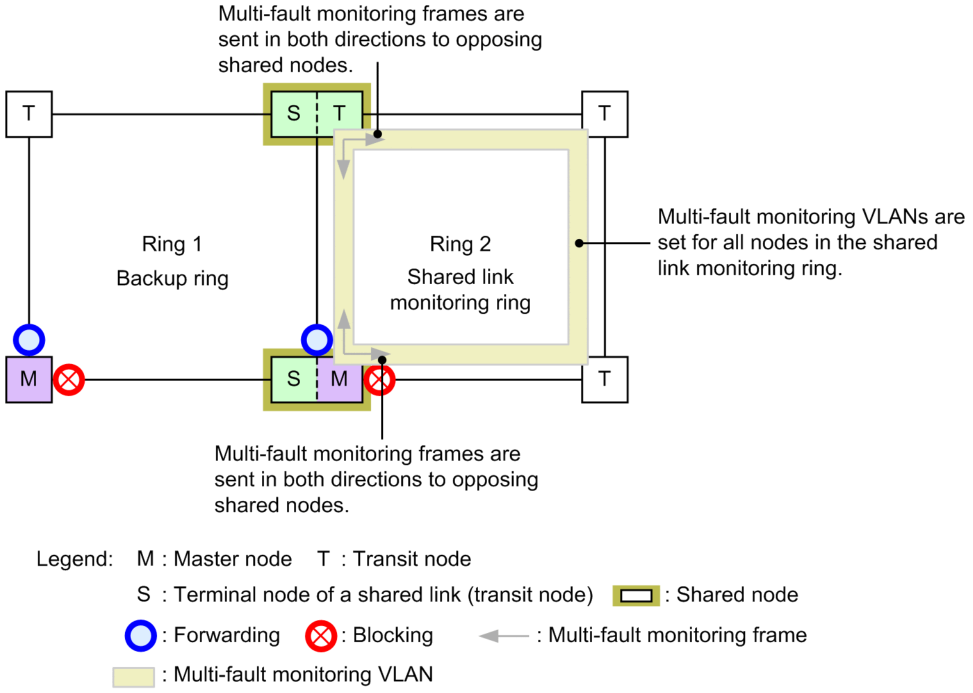

● Example configuration 1
T
S T
T
Ring 1
Ring 2
Backup ring
(Shared link non-monitoring ring)
Shared link monitoring ring
M
S M
T
● Example configuration 2
T
S T
T
Ring 1
Ring 2
Backup ring
(Shared link non-monitoring ring)
Shared link monitoring ring
T
M M
T
● Example configuration 3
T
M T
T
Ring 1
Ring 2
Backup ring
(Shared link non-monitoring ring)
Shared link monitoring ring
T
S M
T
Legend: M : Master node T : Transit node
S : Terminal node of a shared link (transit node)
: Shared node
: Forwarding
: Blocking

23.5.3 Overview of operation for multi-fault monitoring

Multi-faults are monitored on shared nodes placed at both ends of a shared link in a multi-ring configuration with shared links. Shared nodes send control frames for monitoring multi-faults in shared link monitoring rings (called multi-fault monitoring frames). Multi-fault monitoring frame reception is monitored on opposing shared nodes. Note that multi-fault monitoring frames are sent over a special VLAN (called a multi-fault monitoring VLAN).

The following figure gives an overview of multi-fault monitoring operation.

Figure 23-23: Overview of multi-fault monitoring operation


Multi-fault monitoring frames are sent in both directions to opposing shared nodes.
T
S
T
T
Ring 1
Backup ring
Ring 2
Shared link monitoring ring
Multi-fault monitoring VLANs are set for all nodes in the shared link monitoring ring.
M
S
M
T
Multi-fault monitoring frames are sent in both directions to opposing shared nodes.
Legend: M : Master node T : Transit node
S : Terminal node of a shared link (transit node)
: Shared node
: Forwarding
: Blocking
: Multi-fault monitoring frame
: Multi-fault monitoring VLAN

(1) Operation for each node in a shared link monitoring ring

For details about master node and transit node operation in a shared link monitoring ring, because operation is the same as that for multi-rings, see *(2) Shared link monitoring rings* in *23.4.1 Normal ring operation*.

For shared nodes, multi-faults for shared link monitoring rings are monitored. Shared nodes send multi-fault monitoring frames from both ring ports, and monitor whether multi-fault monitoring frames sent from both ring ports by opposing shared nodes are received within the pre-determined time.

(2) Operation for each node in a backup ring

For details about the operation for master nodes and transit nodes in a backup ring, because operation is the same as that for multi-rings, see *(1) Shared link non-monitoring rings* in *23.4.1 Normal ring operation*.

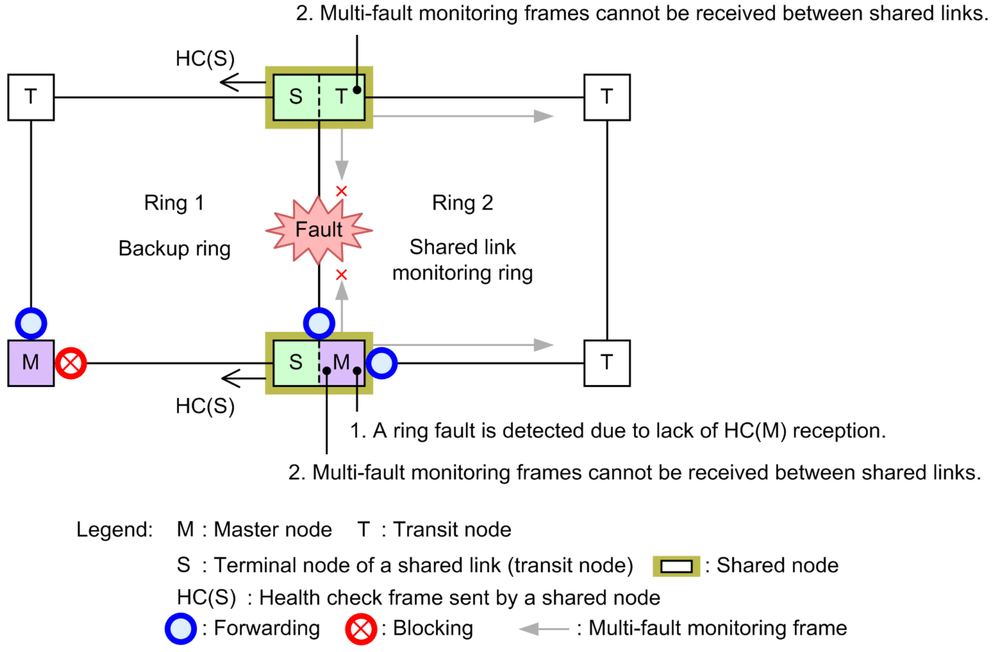
23.5.4 Operation when multi-faults occur

The following explains the operation when multi-faults occur due to shared link faults and other link faults in a shared link monitoring ring.

(1) Operation during shared link faults

The following figure shows the operation when a fault occurs for shared links in a shared link monitoring ring.

Figure 23-24: Operation during shared link faults


2. Multi-fault monitoring frames cannot be received between shared links.
HC(S)
T
S
T
T
Ring 1
Backup ring
Fault
Ring 2
Shared link monitoring ring
M
S
M
T
HC(S)
1. A ring fault is detected due to lack of HC(M) reception.
2. Multi-fault monitoring frames cannot be received between shared links.
Legend: M : Master node T : Transit node
S : Terminal node of a shared link (transit node) : Shared node
HC(S) : Health check frame sent by a shared node
: Forwarding : Blocking : Multi-fault monitoring frame

(a) Operation for each node in a shared link monitoring ring

1. A ring fault is detected by lack of HC(M) reception.

The master node can no longer receive HC(M)s from both directions, and detects a ring fault. For details about master node and transit node operation during ring fault detection, because operation is the same as multi-ring operation, see *(1) Operation when a fault is detected* in *23.4.2 Operation for shared link faults and restoration*.

2. Multi-fault monitoring frames cannot be received between shared links.

Shared nodes can no longer receive multi-fault monitoring frames between shared links, but because reception is still possible on the other ring port, multi-fault monitoring continues.

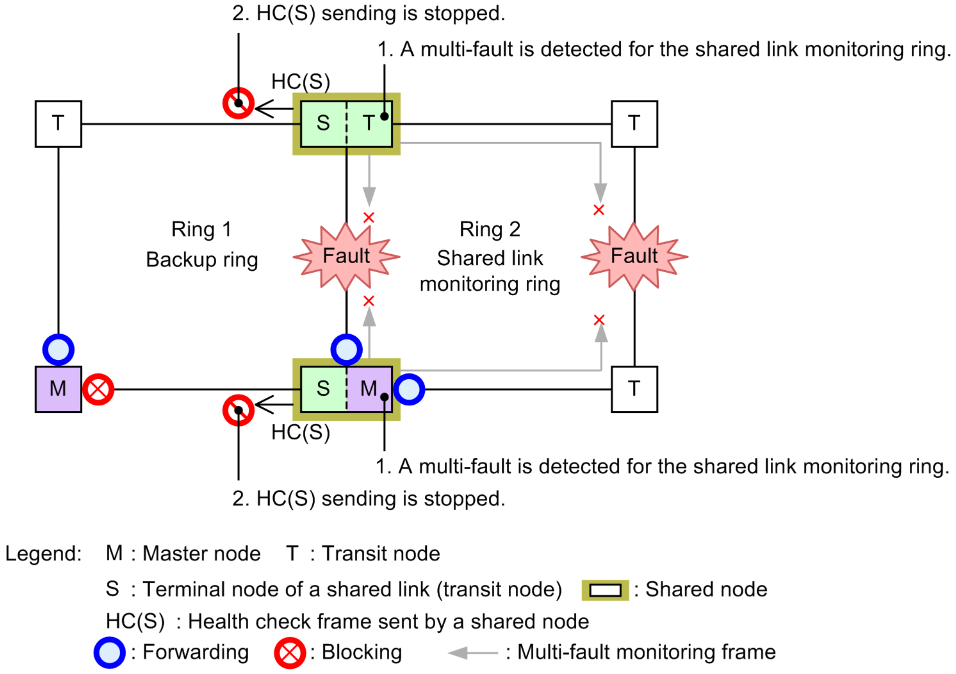
(b) Operation for each node in a backup ring

HC(M)s sent by the master node can no longer be received on a backup ring, but because HC(S)s sent by shared nodes can be received, no fault operation is performed.

(2) Operation when multi-faults occur

The following figure shows operation when multi-faults occur due to shared link faults or other link faults within a shared link monitoring ring.

Figure 23-25: Operation when multi-faults occur


2. HC(S) sending is stopped.
1. A multi-fault is detected for the shared link monitoring ring.
HC(S)
T
S
T
T
Ring 1
Backup ring
Fault
Ring 2
Shared link
monitoring ring
Fault
M
S
M
T
HC(S)
1. A multi-fault is detected for the shared link monitoring ring.
2. HC(S) sending is stopped.
Legend: M : Master node T : Transit node
S : Terminal node of a shared link (transit node) : Shared node
HC(S) : Health check frame sent by a shared node
: Forwarding : Blocking : Multi-fault monitoring frame

(a) Operation for each node in a shared link monitoring ring

1. A multi-fault is detected for the shared link monitoring ring.

Shared nodes can no longer receive multi-fault monitoring frames for both ring ports, and a multi-fault is detected.

(b) Operation for each node in a backup ring

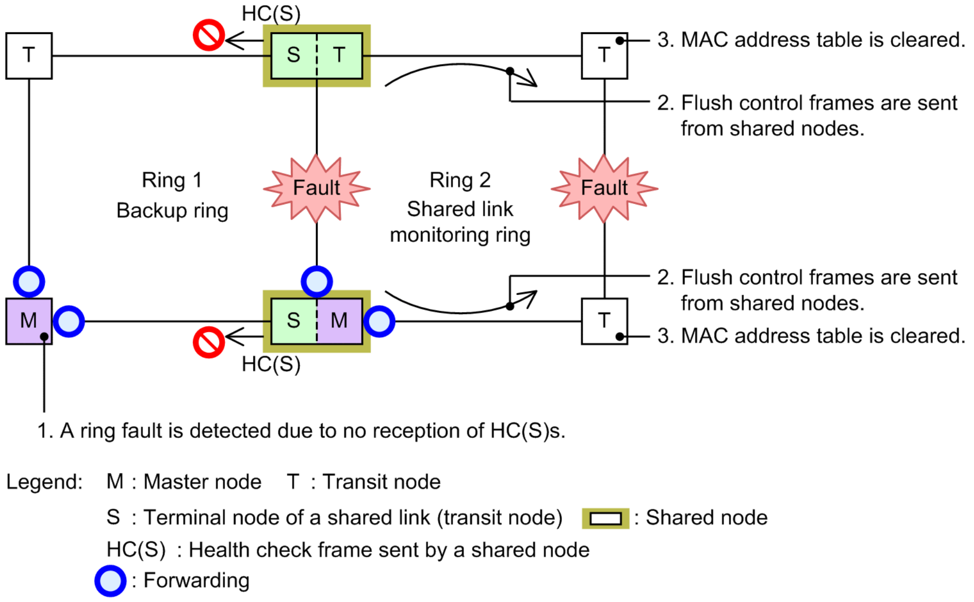
2. HC(S) sending is stopped.

The shared node detecting the multi-fault stops sending backup ring HC(S)s.

(3) Operation for switching to the backup ring

The following figure shows operation for switching to the backup ring due to multi-fault detection.

Figure 23-26: Operation for switching to the backup ring


HC(S)
T
S
T
T
3. MAC address table is cleared.
2. Flush control frames are sent from shared nodes.
Ring 1
Backup ring
Fault
Ring 2
Shared link monitoring ring
Fault
2. Flush control frames are sent from shared nodes.
M
S
M
T
3. MAC address table is cleared.
HC(S)
1. A ring fault is detected due to no reception of HC(S)s.
Legend: M : Master node T : Transit node
S : Terminal node of a shared link (transit node)
▭ : Shared node
HC(S) : Health check frame sent by a shared node
○ : Forwarding

(a) Operation for each node in a backup ring

1. A ring fault is detected due to no reception of HC(S)s.

The master node receives neither HC(M)s sent by itself from both directions nor HC(S)s sent by shared nodes, and detects a ring fault. For details about master node and transit node operation during ring fault detection, because operation is the same as multi-ring operation, see *(1) Operation when a fault is detected* in *23.4.3 Operation for faults and restoration other than for shared links in a shared link non-monitoring ring*.

(b) Operation for each node in a shared link monitoring ring

2. Flush control frames are sent from shared nodes.

When shared nodes receive a flush control frame from the master node of the backup ring, they send to the shared link monitoring ring only flush control frames that clear the MAC address table.

3. The MAC address table is cleared.

Transit nodes receive flush control frames sent from shared nodes, and clear the MAC address table.

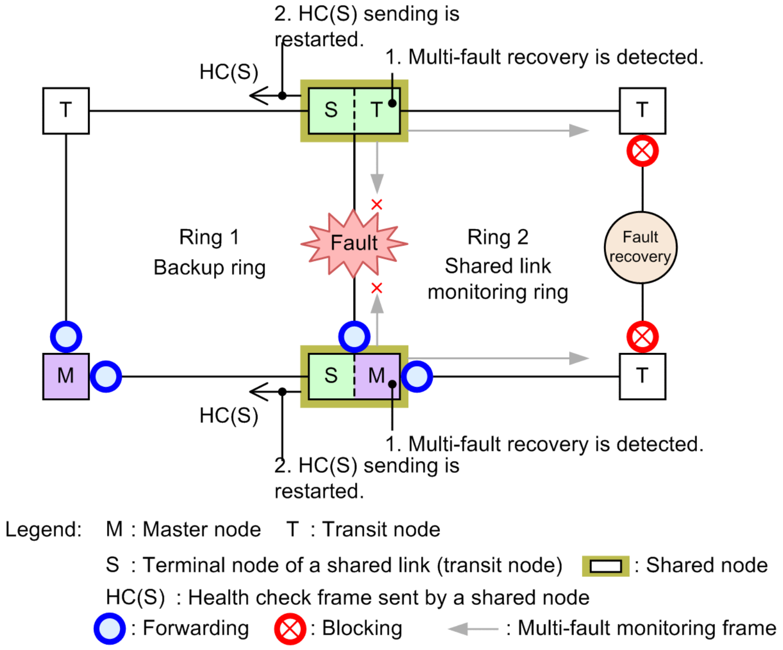
23.5.5 Operation during multi-fault recovery

The following explains the operation for recovery from a multi-fault on a shared link monitoring ring.

(1) Operation during partial recovery from a multi-fault

The following figure shows operation during partial recovery from a multi-fault in a shared link monitoring ring.

Figure 23-27: Operation during partial recovery from a multi-fault


2. HC(S) sending is restarted.
HC(S)
1. Multi-fault recovery is detected.
T
S
T
T
Ring 1
Backup ring
Fault
Ring 2
Shared link
monitoring ring
Fault recovery
M
S
M
T
HC(S)
1. Multi-fault recovery is detected.
2. HC(S) sending is restarted.
Legend:
M : Master node
T : Transit node
S : Terminal node of a shared link (transit node)
: Shared node
HC(S) : Health check frame sent by a shared node
: Forwarding
: Blocking
: Multi-fault monitoring frame

(a) Operation for each node in a shared link monitoring ring

1. Multi-fault recovery is detected.

A shared node receives a multi-fault monitoring frame sent from an opposing shared node, and detects multi-fault recovery.

(b) Operation for each node in a backup ring

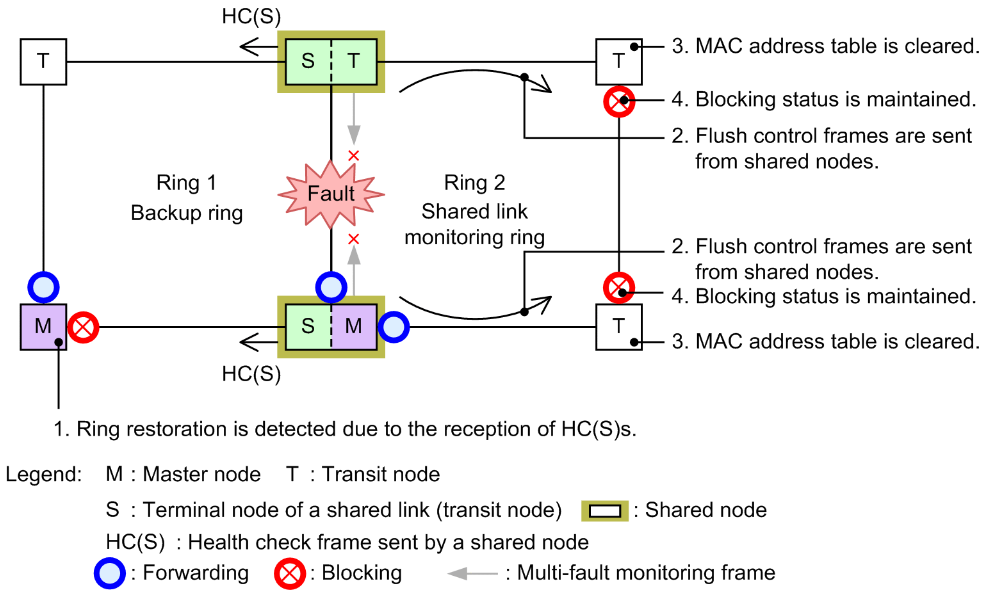
2. HC(S) sending is restarted.

The shared node that detected multi-fault recovery starts sending backup ring HC(S)s again.

(2) Switch-back operation from backup rings

The following figure shows switch-back operation from a backup ring.

Figure 23-28: Switch-back operation from backup rings


HC(S)
T
S
T
T
3. MAC address table is cleared.
4. Blocking status is maintained.
2. Flush control frames are sent from shared nodes.
Ring 1
Backup ring
Fault
Ring 2
Shared link
monitoring ring
2. Flush control frames are sent from shared nodes.
4. Blocking status is maintained.
3. MAC address table is cleared.
M
S
M
T
HC(S)
1. Ring restoration is detected due to the reception of HC(S)s.
Legend:
M : Master node
T : Transit node
S : Terminal node of a shared link (transit node)
: Shared node
HC(S) : Health check frame sent by a shared node
: Forwarding
: Blocking
: Multi-fault monitoring frame

(a) Operation for each node in a backup ring

1. Ring restoration is detected due to reception of HC(S)s.

When the master node receives HC(S)s sent by shared nodes from both directions, it determines that recovery from the ring fault has occurred, and performs restoration operations. For details about operation for the master node and transit nodes when recovery is detected, because operation is the same as for multi-rings, see *(2) Operation when recovery is detected* in *23.4.3 Operation for faults and restoration other than for shared links in a shared link non-monitoring ring*.

(b) Operation for each node in a shared link monitoring ring

2. Flush control frames are sent from shared nodes.

When shared nodes receive a flush control frame from the master node of the backup ring, they send to the shared link monitoring ring only flush control frames that clear the MAC address table.

3. The MAC address table is cleared.

Transit nodes receive flush control frames sent from shared nodes, and clear the MAC address table.

4. The Blocking status is maintained.

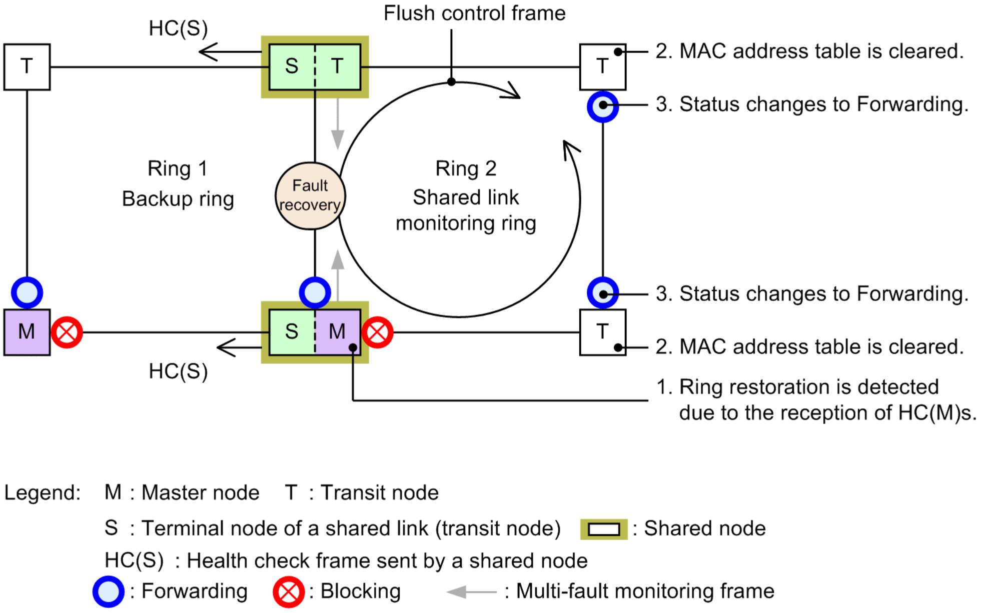
`Blocking` is maintained for the ring VLAN status of the ring ports after recovery from the link fault, because the master node has not detected ring restoration.

For details about when `Blocking` is cleared, see *(18) Communication during partial multi-fault recovery* in *23.7 Notes on Ring Protocol usage*.

(3) Operation during recovery from a shared link fault

The following figure shows operation during shared link fault restoration.

Figure 23-29: Operation during recovery from a shared link fault


HC(S)
Flush control frame
T
S
T
T
2. MAC address table is cleared.
3. Status changes to Forwarding.
Ring 1
Backup ring
Fault recovery
Ring 2
Shared link monitoring ring
3. Status changes to Forwarding.
M
S
M
T
2. MAC address table is cleared.
HC(S)
1. Ring restoration is detected due to the reception of HC(M)s.
Legend:
M : Master node
T : Transit node
S : Terminal node of a shared link (transit node)
: Shared node
HC(S) : Health check frame sent by a shared node
: Forwarding
: Blocking
: Multi-fault monitoring frame

(a) Operation for each node in a shared link monitoring ring

1. Ring restoration is detected due to HC(M) reception.

When the master node receives an HC(M) sent by itself, it determines that recovery from the ring fault has occurred, and performs restoration. For details about operation for the master node and transit nodes when recovery is detected, because operation is the same as for multi-rings, see *(2) Operation when recovery is detected* in *23.4.2 Operation for shared link faults and restoration*.

2. The MAC address table is cleared.

   Transit nodes receive flush control frames sent from the master node, and clear the MAC address table.

3. The status is changes to Forwarding.

   When transit nodes receive flush control frames sent from the master node, they change the ring VLAN status of the ring port after recovery from the link fault to `Forwarding`.

23.6 Ring Protocol network design

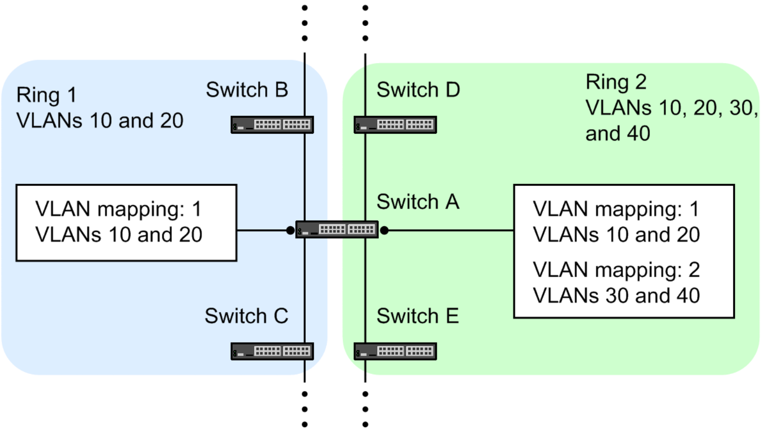
23.6.1 Using VLAN mappings

(1) VLAN mappings and VLANs for data transfer

When multiple ring IDs are set for a single device, such as in a multi-ring configuration, the same VLAN needs to be set multiple times for each ring ID. In such cases, the list of VLANs used as data transfer VLANs (called VLAN mapping) can be set in advance to simplify data transfer VLAN settings in a multi-ring configuration, and prevent loops due to mistakes in configuration settings.

VLAN mappings assign VLANs used for data transfer to VLAN mapping IDs. These VLAN mapping IDs are set for VLAN groups, and are managed as data transfer VLANs.

Figure 23-30: Example VLAN mapping assignment for each ring



(2) VLAN mappings for use with PVST+

When the Ring Protocol is used with PVST+, the VLANs used for PVST+ are also set in the VLAN mapping. In such cases, make sure that only one VLAN is assigned to the VLAN mapping. Set data transfer VLANs other than the VLANs used for PVST+ using a separate VLAN mapping, and set them in a VLAN group with the VLAN mapping used for PVST+.

23.6.2 Using forwarding-delay-time for control VLANs

When the Ring Protocol runs from the initial status, such as for device startup and program restart (using the `restart axrp` operation command) for a transit node, data transfer VLANs are logically blocked. Transit nodes remove this logical block when they receive a flush control sent from the master node. However, when the fault monitoring time (`health-check holdtime`) for the master node is long, such as during program restart, status changes for the ring network might not be recognized. In this case, because the logical block is not released until the reception hold time for flush control frames (`forwarding-shift-time`) times out, the data VLAN for the transit node cannot communicate. Because operation is performed as follows when a forwarding transition time (`forwarding-delay-time`) is set for the control VLAN, this kind of case can be avoided.

1. The transit node performs an immediate logical block of the control VLAN during device startup or after program restart.
2. Because the control VLAN for the transit node has been logically blocked, a fault is detected on the master node (even though a fault was already detected previously upon device startup). Therefore, communication is switched to an alternate path.
3. The transit node removes `Blocking` for the control VLAN, due to a timeout of the forwarding transition time (`forwarding-delay-time`) for the control VLAN.

4. The master node receives a health check frame, detects recovery, and sends a flush control frame.
5. The transit node receives this flush control frame, and removes the logical block on the data transfer VLAN. With this, communication on the data transfer VLAN is restarted, and restoration of the normal communication path is performed on the entire ring network.

(1) Relationship between the forwarding transition time (forwarding-delay-time) and fault monitoring time (health-check holdtime) for control VLANs

For the forwarding transition time (`forwarding-delay-time`) of a control VLAN, set a value greater than that of the fault monitoring time (`health-check holdtime`). For the forwarding transition time of a control VLAN (`forwarding-delay-time`), we recommend setting a value around twice that of the fault monitoring time (`health-check holdtime`). If a value less than that of the fault monitoring time (`health-check holdtime`) is set, faults cannot be detected on the master node. Therefore, switching cannot be performed to alternate paths, causing communication to be cut for an extended time.

23.6.3 Automatic primary port determination

The primary port of the master node is automatically determined according to information for the two ring ports set by the user. As shown in the table below, the port with the higher priority is used as the primary port. Also, the priority can be reversed for each VLAN group to allocate paths without any particular awareness by the user.

Table 23-5: Primary port selection method (VLAN group #1)

Ring port #1	Ring port #2	Prioritized port
Physical ports	Physical ports	The port with the smaller port number runs as the primary port.
Physical ports	Channel group	The physical port runs as the primary port.
Channel group	Physical ports	The physical port runs as the primary port.
Channel group	Channel group	The port with the smaller channel group number runs as the primary port.

Table 23-6: Primary port selection method (VLAN group #2)

Ring port #1	Ring port #2	Prioritized port
Physical ports	Physical ports	The port with the larger port number runs as the primary port.
Physical ports	Channel group	The channel group runs as the primary port.
Channel group	Physical ports	The channel group runs as the primary port.
Channel group	Channel group	The port with the larger channel group number runs as the primary port.

Note that in addition to the above determination method, the `axrp-primary-port` configuration command can be used by users to set the primary port for each VLAN group.

23.6.4 Configurations with mixed node types within the same device

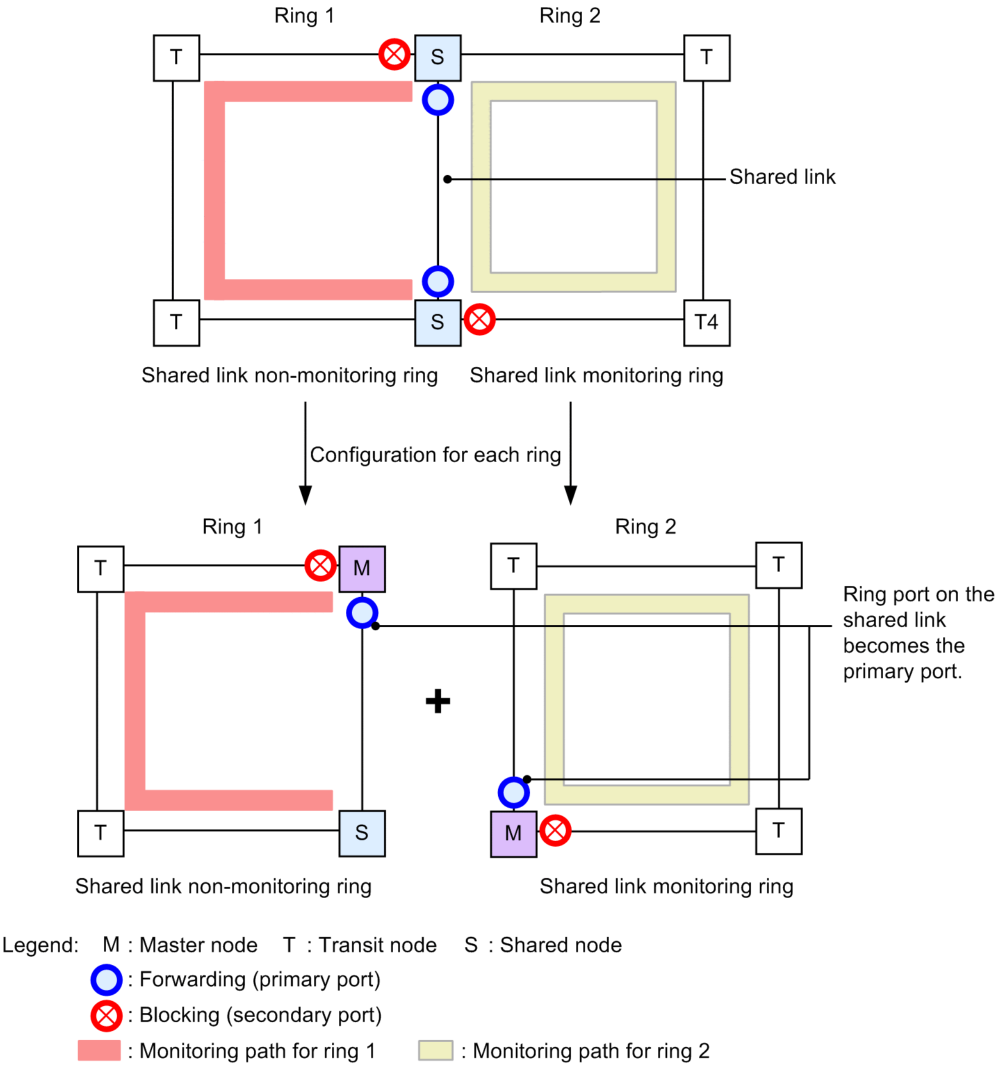
(1) Mixed settings for node types

If the Switch belongs to two different rings, it can run as the master node on one ring, and as a transit node on the other ring.

23.6.5 Configurations with mixed node types for shared nodes

In a multi-ring configuration with shared links, nodes place at both ends of a shared link can run as master nodes. In this case, the primary port of the master node is always the ring port of the shared link, regardless of the data transfer VLAN group. Therefore, this configuration does not allow load balancing based on setting two data transfer VLAN groups.

Figure 23-31: Port status when a shared node is used as the master node


Ring 1
Ring 2
T
S
T
Shared link
T
S
T4
Shared link non-monitoring ring
Shared link monitoring ring
Configuration for each ring
Ring 1
Ring 2
T
M
T
T
Ring port on the shared link becomes the primary port.
+
T
S
M
T
Shared link non-monitoring ring
Shared link monitoring ring
Legend: M : Master node T : Transit node S : Shared node
: Forwarding (primary port)
: Blocking (secondary port)
: Monitoring path for ring 1
: Monitoring path for ring 2

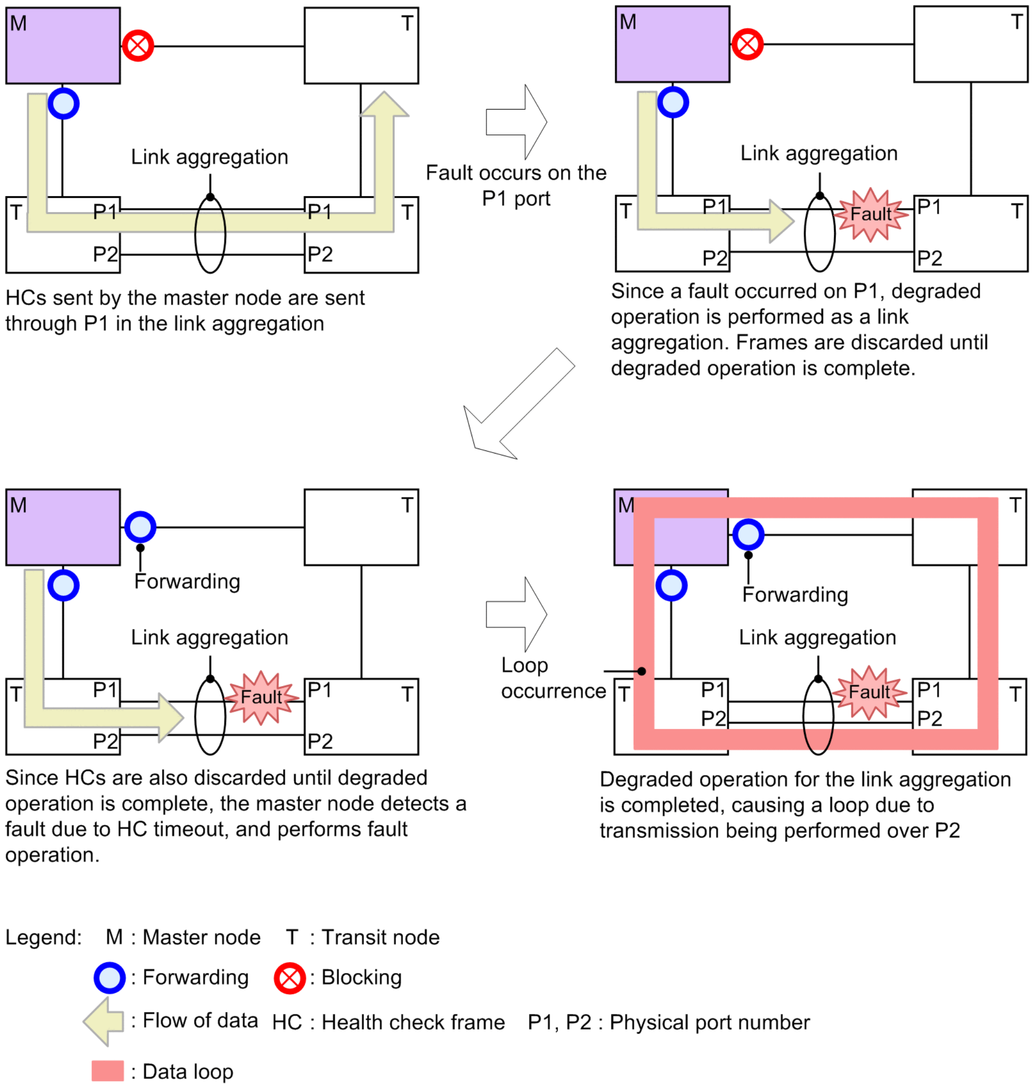
23.6.6 Setting fault monitoring times when link aggregation is used

When ring ports are configured using link aggregation, and a fault occurs for a port within the link aggregation transferring health check frames, control frames are discarded until link aggregation switching or degraded operation is completed. Therefore, when the fault monitoring time (`health-check holdtime`) of the master node is shorter than the time for completing link aggregation switching or degraded operation, the master node inadvertently detects a ring fault, and performs path switching. As a result, a loop might occur.

When ring ports are configured using link aggregation, the fault monitoring time for the master node needs to be set greater than the time for completing switching or degraded operation for the link aggregation.

Note that when LACP-based link aggregation is used, because the initial value of the LACPDU sending interval is `long` (30 seconds), when operation is performed without changing the initial value, a loop might occur. When using LACP-based link aggregation, either change the fault monitoring time for the master node, or set the LACPDU sending interval to `short` (1 second).

Figure 23-32: Fault detection when link aggregation is used



HCs sent by the master node are sent through P1 in the link aggregation

Since a fault occurred on P1, degraded operation is performed as a link aggregation. Frames are discarded until degraded operation is complete.

Since HCs are also discarded until degraded operation is complete, the master node detects a fault due to HC timeout, and performs fault operation.

Degraded operation for the link aggregation is completed, causing a loop due to transmission being performed over P2

23.6.7 Usage with IEEE 802.3ah/UDLD functionality

This protocol does not perform fault detection and switching operations for one-way link faults. To perform switching operations when a one-way link fault occurs, use IEEE 802.3ah/UDLD functionality. IEEE 802.3ah/UDLD functionality settings are performed for ring ports connected between nodes within a ring. When IEEE 802.3ah/UDLD functionality detects a one-way link fault, it blocks the corresponding port. This means that when the master node monitoring the corresponding ring detects a ring fault, it performs switching operations.

23.6.8 Usage with link-down detection timers and link-up detection timers

When the link status of ports used in a ring port (physical ports or physical ports belonging to a link aggregation) is unstable, the master node might continuously detect ring faults and ring fault recovery, causing unstable ring network statuses, loops, and extended communication cut-offs. To avoid such situations, a link-down detection timer and link-up detection timer can be used for ports used in a ring port. For details about settings for link-down detection timers and link-up detection timers, see *16.2.6 Configuring the link-down detection timer* and *16.2.7 Configuring the link-up detection timer*.

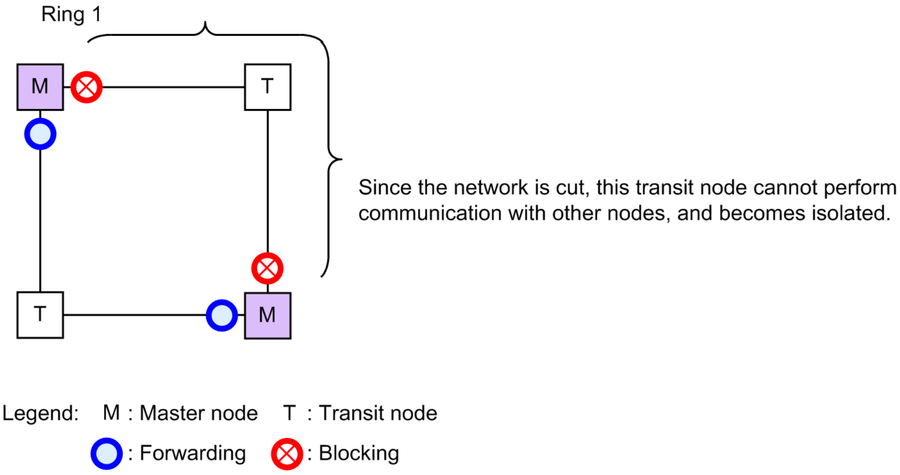
23.6.9 Prohibited Ring Protocol configurations

The following describes prohibited configurations for networks using the Ring Protocol.

(1) Setting multiple master nodes in the same ring

Do not set multiple master nodes within the same ring. When the same ring contains multiple master nodes, because the secondary port is logically blocked, the network is cut, preventing proper communication.

Figure 23-33: Setting multiple master nodes in the same ring

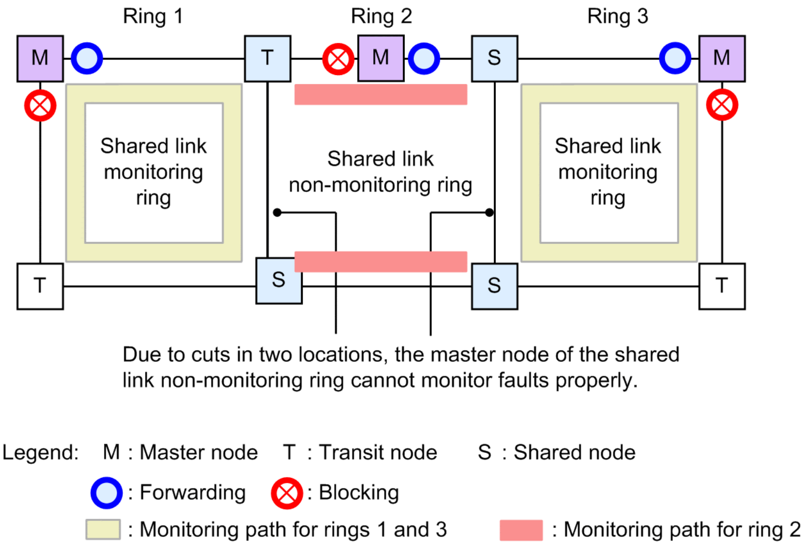


Since the network is cut, this transit node cannot perform communication with other nodes, and becomes isolated.

(2) Configuration with multiple shared link monitoring rings

In a multi-ring configuration with shared links, make sure that there is only one shared link monitoring ring within the network. If the network contains multiple shared link monitoring rings, fault monitoring within the shared link non-monitoring ring gets cut, preventing proper fault monitoring.

Figure 23-34: Configuration with multiple shared link monitoring rings

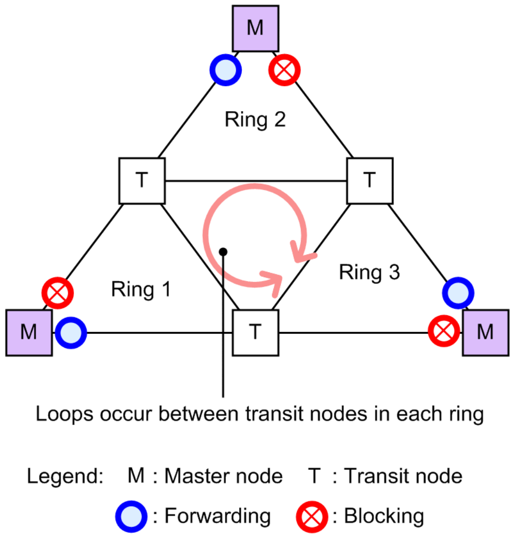

Ring 1
Ring 2
Ring 3
M
T
M
S
M
Shared link monitoring ring
Shared link non-monitoring ring
Shared link monitoring ring
T
S
S
T
Legend: M : Master node T : Transit node S : Shared node
: Forwarding
: Blocking
: Monitoring path for rings 1 and 3
: Monitoring path for ring 2

Due to cuts in two locations, the master node of the shared link non-monitoring ring cannot monitor faults properly.

(3) Example of a looped multi-ring configuration

For multi-ring configurations such as that in the following figure, loops form between transit nodes.

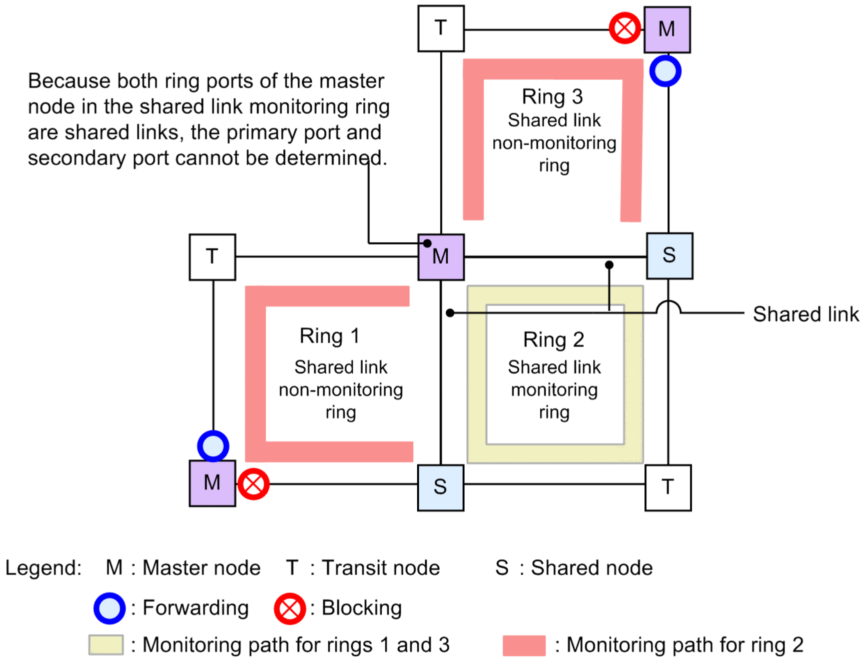
Figure 23-35: Looped multi-ring configuration


M
Ring 2
T
T
Ring 1
Ring 3
M
T
M
Loops occur between transit nodes in each ring
Legend: M : Master node T : Transit node
: Forwarding : Blocking

(4) Configuration in which the master node's primary port cannot be determined

Do not set a node located at one of the two terminal nodes of a shared link non-monitoring ring as the master node (shown in the figure below). In such configuration, the two ring ports of the master node will be shared links, and the primary port cannot be correctly determined.

Figure 23-36: Configuration in which the master node's primary port cannot be determined


T
M
Because both ring ports of the master node in the shared link monitoring ring are shared links, the primary port and secondary port cannot be determined.
Ring 3
Shared link non-monitoring ring
T
M
S
Shared link
Ring 1
Shared link non-monitoring ring
Ring 2
Shared link monitoring ring
M
S
T
Legend: M : Master node T : Transit node S : Shared node
: Forwarding : Blocking
: Monitoring path for rings 1 and 3
: Monitoring path for ring 2

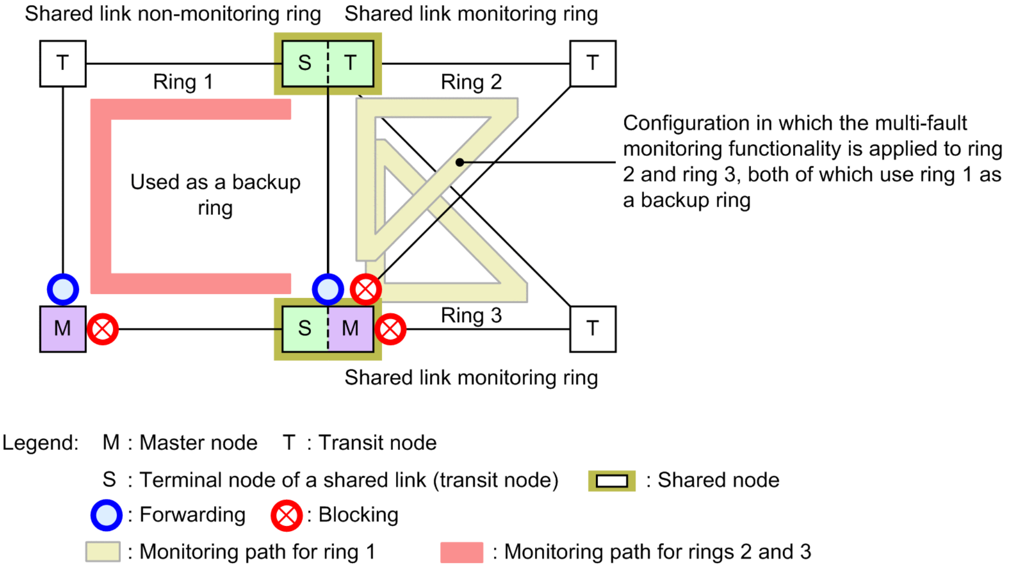
23.6.10 Prohibited configurations for the multi-fault monitoring functionality

The prohibited configurations when the multi-fault monitoring functionality is used are as follows.

(1) Configuration in which multiple shared link monitoring rings use the same backup ring

Shared link monitoring rings and shared link non-monitoring rings used as backup rings during multi-fault detection must be configured with a one-to-one association. When multiple shared link monitoring rings use the same shared link non-monitoring ring as a backup ring, and a multi-fault is detected on one of the shared link monitoring rings, another shared link monitoring ring turns into a loop configuration spanning the backup ring.

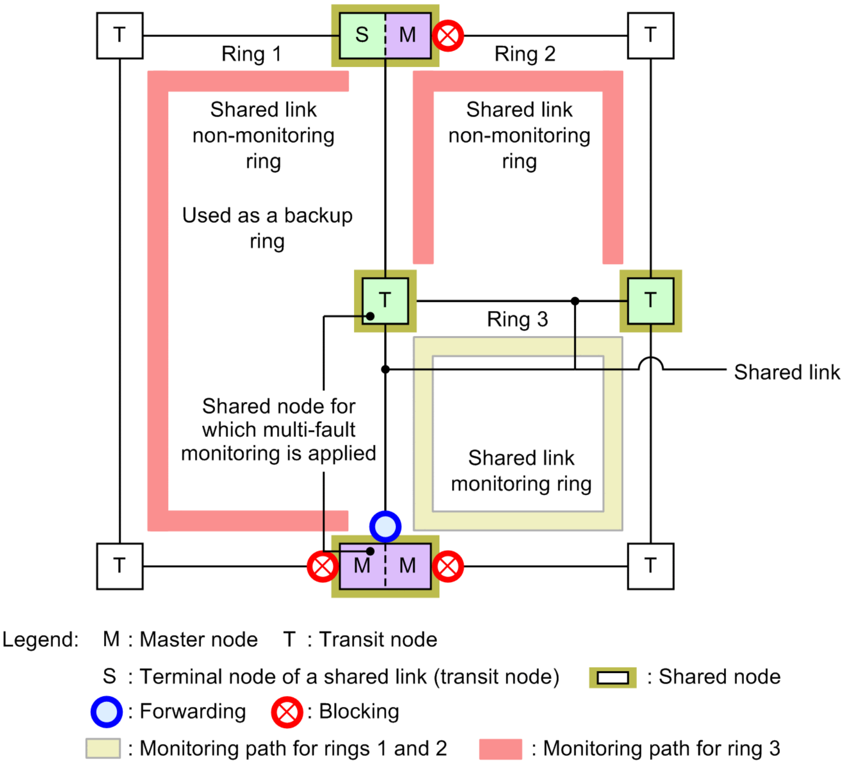
Figure 23-37: Configuration in which multiple shared link monitoring rings use the same backup ring


Shared link non-monitoring ring
Shared link monitoring ring
T
S
T
T
Ring 1
Ring 2
Used as a backup ring
Configuration in which the multi-fault monitoring functionality is applied to ring 2 and ring 3, both of which use ring 1 as a backup ring
M
S
M
Ring 3
T
Shared link monitoring ring
Legend: M : Master node T : Transit node
S : Terminal node of a shared link (transit node)
: Shared node
: Forwarding
: Blocking
: Monitoring path for ring 1
: Monitoring path for rings 2 and 3

(2) Configuration in which multi-faults are monitored on shared nodes within shared links

Shared nodes monitoring multi-faults need to be placed at both ends of shared links. Therefore, monitoring cannot be performed properly for configurations like that shown in the figure below, in which shared nodes within a shared link monitor multi-faults. Also, switching cannot be performed properly to the backup ring when a multi-fault occurs.

Figure 23-38: Configuration in which multi-faults are monitored on shared nodes within shared links

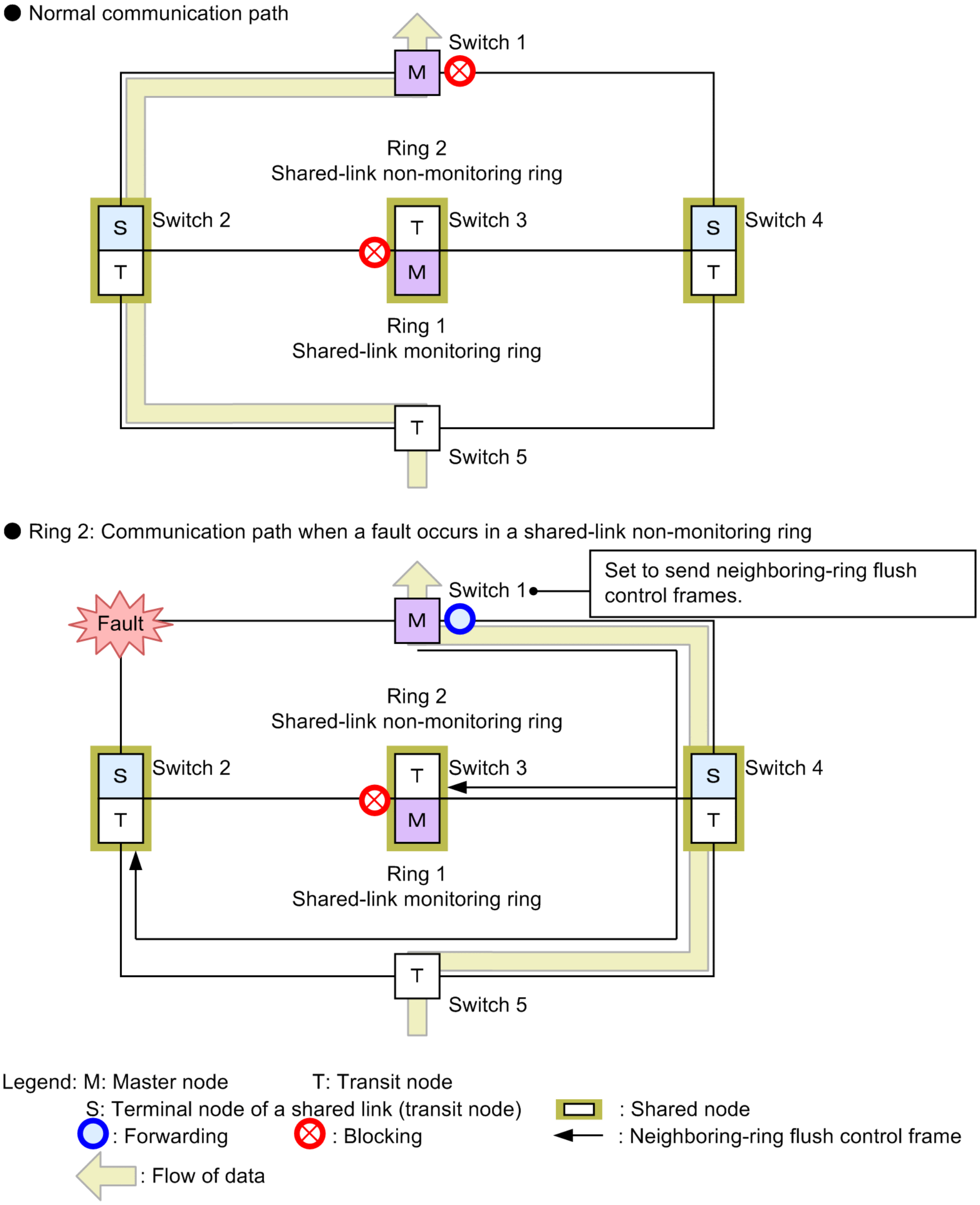

T
S
M
T
Ring 1
Ring 2
Shared link non-monitoring ring
Shared link non-monitoring ring
Used as a backup ring
T
T
Ring 3
Shared link
Shared node for which multi-fault monitoring is applied
Shared link monitoring ring
T
M
M
T
Legend: M : Master node T : Transit node
S : Terminal node of a shared link (transit node)
: Shared node
: Forwarding
: Blocking
: Monitoring path for rings 1 and 2
: Monitoring path for ring 3

23.6.11 Configurations in which both ring ports of a master node are shared links

In a multi-ring configuration shown in the figure below, both ring ports of the master node (switch 3 of ring 1) are shared links. In such a configuration, set the master node of a shared link non-monitoring ring (switch 1 of ring 2) to send flush control frames for neighboring rings using the `flush-request-transmit vlan` configuration command.

If a ring fault occurs in a shared link non-monitoring ring with this configuration, the master nodes can switch to a new communication path by sending flush control frames for neighboring rings to neighboring devices in the ring. The same applies to the case where a shared link non-monitoring ring is recovered from a fault.

Figure 23-39: Example configuration in which both ring ports of a master node are shared links


● Normal communication path
Switch 1
M
Ring 2
Shared-link non-monitoring ring
S
T
Switch 2
T
M
Switch 3
S
T
Switch 4
Ring 1
Shared-link monitoring ring
T
Switch 5
● Ring 2: Communication path when a fault occurs in a shared-link non-monitoring ring
Fault
Switch 1
Set to send neighboring-ring flush control frames.
M
Ring 2
Shared-link non-monitoring ring
Switch 2
Switch 3
Switch 4
Ring 1
Shared-link monitoring ring
Switch 5
Legend: M: Master node
T: Transit node
S: Terminal node of a shared link (transit node)
: Shared node
: Forwarding
: Blocking
: Neighboring-ring flush control frame
: Flow of data

If you do not configure the settings to send flush control frames for neighboring rings in this configuration and a ring fault occurs in a shared link non-monitoring ring, the path is switched in the shared link non-monitoring ring but is not switched in neighboring shared link monitoring rings. As a result, old MAC address learning data is left on devices in the shared link monitoring rings and it may take some time to switch the communication path. The same applies to the case where a shared link non-monitoring ring is recovered from a fault.

23.7 Notes on Ring Protocol usage

(1) Configuration changes during operation

Take care not to create a loop configuration when changing Ring Protocol configurations by performing the following operations:

- Stopping the Ring Protocol functionality (`disable` command)
- Changing the operating mode (`mode` command) and changing attributes (`ring-attribute` parameter)
- Changing control VLANs (`control-vlan` command) and changing VLAN IDs used by control VLANs (`vlan` command, `switchport trunk` command, and `state` command)
- Changing data transfer VLANs (`axrp vlan-mapping` command and `vlan-group` command)
- Changing primary ports (`axrp-primary-port` command)
- Adding the terminal node of a shared link non-monitoring ring to a device on which the master node of a shared link monitoring ring is running (adding a ring with the `rift-ring-edge` parameter specified in the operating mode attributes)

We recommend changing such configurations as follows:

1. Use the `shutdown` command or other means to take down the ring port of the device whose configuration is to be changed, or the secondary port of the master node.
2. Stop the Ring Protocol functionality for the device whose configuration is to be changed (`disable` command).
3. Change the configuration.
4. Clear the stop on the Ring Protocol functionality (`no disable` command).
5. Bring previously downed ring ports back up (such as by clearing the `shutdown` command).

(2) Notes on use with other functionality

For details, see *18.3 Compatibility between Layer 2 switch functionality and other functionality*.

(3) VLANs used for control VLANs

Ring Protocol control frames are tagged frames. Therefore, set VLANs used for control VLANs in `allowed vlan` (native VLANs cannot be used) for trunk ports.

(4) Ring VLAN status for transit nodes

For transit nodes, when a fault occurs for a device or ring port, and recovery succeeds, the ring VLAN status of the ring port is set to `Blocking` to prevent loops from occurring. One of the ways in which this `Blocking` status is cleared is when the reception hold time (`forwarding-shift-time`) for flush control frames times out. When the reception hold time for flush control frames (`forwarding-shift-time`) is shorter than the health check sending interval of the master node (`health-check interval`), a loop might occur. This can happen if the transit node ring port changes to the `Forwarding` status before the master node detects recovery from the ring fault and changes the secondary port to the `Blocking` status. Therefore, set the reception hold time for flush control frames (`forwarding-shift-time`) to a value greater than the health check sending interval (`health-check interval`).

(5) VLAN configurations in multi-rings with shared links

For shared links used in common among multiple rings, the same VLAN needs to be used for each ring. Port Forwarding/Blocking control for VLANs between shared links is performed by shared link monitoring rings. Therefore, when different VLANs are used for shared link monitoring/non-monitoring rings, VLANs used for the shared link non-monitoring rings remain in `Blocking` status, and are no longer able to communicate.

(6) Building networks when the Ring Protocol is used

Networks using the Ring Protocol have looped configurations. Therefore, build such networks as follows to avoid loops.

1. Beforehand, use `shutdown` or another command to take the ring port (physical port or channel group) of the ring configuration node down.
2. Set the Ring Protocol configuration, or copy (`copy` command) the configuration file including the Ring Protocol settings, to enable the Ring Protocol.
3. Bring the ring port back up (such as by clearing the `shutdown` command) when the Ring Protocol is set for all devices in the network.

(7) Health-check frame sending interval and fault monitoring times

Set the fault monitoring time (`health-check holdtime`) to a value greater than the sending interval (`health-check interval`). If the time is set to a value less than the sending interval, a reception timeout will occur and a fault will be mistakenly detected. Also, when setting the fault monitoring time and sending interval, make sure to take the network configuration and operation environment into account. We recommend setting a fault monitoring time of around three times the sending interval. Setting this to a value less than three times might cause faults to be mistakenly detected when delays occur due to network load and device CPU load.

(8) Interoperability

The Ring Protocol is functionality specific to the Switch. It cannot be used interoperably with third-party switches.

(9) Devices constituting rings

- In a network using the Ring Protocol, if a third-party switch, relay, or other device that does not support the Ring Protocol is placed between Switches, MAC address table entries are not cleared immediately. This situation occurs because the flush control frames sent by the master node for the Switches cannot be interpreted. As a result, because data frames are transferred according to the information before communication path switching (or switch-back), the data might not be delivered properly.
- When configuring a ring network with an AX6700S, AX6600S, or AX6300S series switch as the master node, and the Switch as the transit node, set the sending interval for master node health check frames to a value greater than or equal to the minimum value that can be specified for the Switch. When a value less than the minimum value for the health-check frame sending interval of the Switch is set, the CPU usage for the Switch might increase, preventing normal ring operation.

(10) When master node faults occur

When the master node cannot communicate because of a device fault or other reason, ring network fault monitoring is not performed. Therefore, communication continues as is between transit nodes other than the master node, without being switched to an alternate path. Also, when the master node has recovered from a device fault, it sends a flush control frame to the transit nodes in the ring. Therefore, communication might stop temporarily.

(11) When multi-faults occur within a network

When multiple faults occur between different nodes in the same ring (a multi-fault), because the master node was already performing fault detection for the first fault, the second and subsequent faults are not detected. Also, because health check frames sent by the master node cannot be received until recovery from the last fault in a multi-fault restoration detection situation occurs, recovery cannot be detected. As a result, communication might be temporarily impossible for multi-faults when a partial fault is restored (when a fault remains for the ring).

Note that when the multi-fault monitoring functionality is applied, multi-faults might be able to be detected, depending on the combination of faults. For details about the multi-fault monitoring functionality, see *23.5 Multi-fault monitoring functionality for the Ring Protocol*.

(12) Path switching when faults occur due to downed VLANs

When a downed link or other fault occurs on the primary port of the master node, VLANs set in the data transfer VLAN group might go down temporarily. In cases like this, it might take some time to restore communication by path switching.

Note that the VLAN Debounce functionality can sometimes be used to avoid downed VLANs. For details about the VLAN Debounce functionality, see *21.9 Description of the VLAN Debounce functionality*.

(13) Sending counts for flush control frames

Adjust the number of times that flush control frames are sent by the master node, based on configurations including the VLAN count and VLAN mapping count applying to the ring network.

If 64 or more VLAN mappings are used for a single ring port, set a sending count to 4 times or more. If the count is less than 4 times, the MAC address table entries cannot be cleared, and it might take some time to perform path switching.

(14) Specifying configuration commands that disable VLANs

If no configuration commands pertaining to the Ring Protocol have been set, when the first configuration command pertaining to the Ring Protocol (one of the following commands) is set, all VLANs will go down temporarily. Therefore, when a ring network that uses the Ring Protocol is built, we recommend setting the following configuration commands ahead of time.

- axrp
- axrp vlan-mapping
- axrp-ring-port
- axrp-primary-port
- axrp virtual-link

Note that for VLAN mapping (the `axrp vlan-mapping` command), the VLANs associated with the VLAN mapping will go down temporarily, even for new settings. The VLAN mappings already set and the other VLANs to which they are associated are not affected.

(15) Sending and receiving flush control frames when the master node device restarts

When the master node device restarts, and the transit node detects link-up for the ring port connected to the master node later than the master node does, the transit node might not be able to receive the flush control frames sent by the master node during initial operation. Here, the status of the ring port for the transit node unable to receive flush control frames will be `Blocking`. The corresponding ring port changes to the `Forwarding` status and communication is restored after the reception hold time for flush control frames (`forwarding-shift-time`) elapses.

When flush control frames cannot be received on neighboring transit nodes, and the sending count for flush control frames from the master node is controlled, reception might be possible. Also, to shorten the time to cut communication due to flush control frames not yet received, shorten the reception hold time for flush control frames sent by the transit node (initial value: 10 seconds).

This also applies to the following:

- Restarting VLAN programs (executing the `restart vlan` operation command)
- Reflecting to configuration file operation (executing the `copy` operation command)

(16) Setting the reception hold time for flush control frames when the path switch-back suppression functionality is applied

When using the path switch-back suppression functionality, either specify `infinity` for the reception hold time (`forwarding-shift-time`) for flush control frames for the transit node, or specify a value greater than the path switch-back suppression time (`preempt-delay`). If the reception hold time for flush control frames for the transit node times out during path switch-back suppression, and logical block on the corresponding ring port is cleared, because the master node clears the logical block on the secondary port, a loop might occur.

(17) Timing for starting monitoring for the multi-fault monitoring functionality

After the multi-fault monitoring functionality is applied to a shared node, multi-fault monitoring is started when the first multi-fault monitoring frame sent from the opposing shared node is received. As such, when the multi-fault monitoring functionality is set and a fault occurs for a ring network, multi-fault monitoring cannot be started. Set the multi-fault monitoring functionality when the status of the ring network is normal.

(18) Communication during partial multi-fault recovery

Because the master node does not detect ring restoration during partial multi-fault recovery, the transit node ring port is logically blocked until the reception hold time (`forwarding-shift-time`) for flush control frames elapses. To clear the logical block status, either shorten the reception hold time for flush control frames (initial value: 10 seconds), or recover remaining link faults to have the master node detect ring restoration. Also, when setting the reception hold time for flush control frames, set a value greater than the sending interval for multi-fault monitoring frames (using the `multi-fault-detection interval` configuration command). When a small value is set, loops might occur temporarily.

(19) Using the multi-fault monitoring functionality and path switch-back suppression functionality together

When the path switch-back suppression functionality is set for a shared link non-monitoring ring and recovery for a multi-fault succeeds, because the `Forwarding` status is maintained until the restoration suppression status is cleared for the secondary port, this might result in a loop configuration. When using the multi-fault monitoring functionality and path switch-back suppression functionality together, perform any of the following operations:

- Set the path switch-back suppression functionality only for the shared link monitoring ring
- Set the switch-back suppression time for the shared link monitoring ring sufficiently longer than the switch-back suppression time for the shared link non-monitoring ring
- When setting the switch-back suppression time for the shared link monitoring ring and shared link non-monitoring ring to `infinity`, first clear the restoration suppression status for the shared link non-monitoring ring and then clear the restoration suppression status for the shared link monitoring ring

(20) How to shut down link aggregation specified as the ring port

When nodes in a ring network are connected via link aggregation (static mode or LACP mode), make sure to shut down all physical ports belonging to the channel group by using the `shutdown` command before shutting down the channel group of the link aggregation by using the `shutdown` command.

If you bring up the channel group using the `no shutdown` command, make sure to shut down all physical ports belonging to the channel group by using the `shutdown` command.

Chapter

24. Settings and Operation for Ring Protocol

This chapter explains example settings for the Ring Protocol.

24.1 Configuration

To use the Ring Protocol functionality, `axrp`, `axrp vlan-mapping`, `mode`, `control-vlan`, `vlan-group`, and `axrp-ring-port` need to be set. Set the appropriate configuration for all nodes.

24.1.1 List of configuration commands

The following table describes the configuration commands for the Ring Protocol.

Table 24-1: List of configuration commands

Command name	Description
axrp	Sets the ring ID.
axrp vlan-mapping	Sets the VLAN mapping and VLANs participating in the mapping.
axrp-primary-port	Sets the primary port.
axrp-ring-port	Sets the ring port.
control-vlan	Sets the VLAN to be used as a control VLAN.
disable	Disables the Ring Protocol functionality.
flush-request-count	Sets the number of times flush control frames are sent.
flush-request-transmit vlan	Sets a VLAN that sends flush control frames for neighboring rings to devices in the neighboring ring.
forwarding-shift-time	Sets the reception hold time for flush control frames.
health-check holdtime	Sets the hold time for health check frames.
health-check interval	Sets the sending interval for health check frames.
mode	Sets the operating mode for a ring.
multi-fault-detection holdtime	Sets the reception hold time for multi-fault monitoring frames.
multi-fault-detection interval	Sets the sending interval for multi-fault monitoring frames.
multi-fault-detection mode	Sets the monitoring mode for multi-fault monitoring.
multi-fault-detection vlan	Sets the VLAN used as the multi-fault monitoring VLAN.
name	Sets the name for identifying a ring.
preempt-delay	Enables the path switch-back suppression functionality and sets the suppression time.
vlan-group	Sets the VLAN group for which to run the Ring Protocol functionality, and the VLAN mapping ID.

24.1.2 Flow of Ring Protocol settings

Normal operation of the Ring Protocol functionality requires settings that match the configuration. The flow of these settings is as follows.

(1) Stopping Spanning Tree Protocols

When the Ring Protocol is used, we recommend that you stop Spanning Tree Protocols in advance. However, note that when the Ring Protocol and a Spanning Tree Protocol are used together with the Switch, there is no need to stop the Spanning Tree Protocol. For details about stopping Spanning Tree Protocols, see *22. Spanning Tree Protocols*.

(2) Performing settings common to the Ring Protocol

Perform ring configuration settings and common settings that do not depend on the placement of the Switch within a ring.

- Ring ID
- Control VLAN
- VLAN mapping
- VLAN group

(3) Setting the mode and port

Perform ring configuration settings and settings related to the placement of the Switch within a ring. If the combination of settings contains a conflict, the Ring Protocol functionality will not operate properly.

- Mode
- Ring port

(4) Setting various parameters

The Ring Protocol functionality runs using the initial values if the following configurations are not set. To change these values, set them using commands.

- Disabling functionality
- Health-check frame sending interval
- Reception hold time for health check frames
- Reception hold time for flush control frames
- Number of times a flush control frame was sent
- Primary port
- Enabling the path switch-back suppression functionality and suppression time

24.1.3 Configuring ring IDs

Points to note

Set a ring ID. The same ring ID needs to be set for all devices belonging to the same ring.

Command examples

1.
```
(config)# axrp 1
```
Sets the ring ID to 1.

24.1.4 Configuring control VLANs

(1) Setting control VLANs

Points to note

Specify the VLAN to be used as the control VLAN. VLANs used for data transfer cannot be used. Note that VLAN IDs with the same value as VLAN IDs used in different rings cannot be used.

Command examples

1.
```
(config)# axrp 1
```
Switches to axrp configuration mode for ring ID 1.

2.
```
(config-axrp)# control-vlan 2
```
Specifies VLAN 2 as the control VLAN.

(2) Setting the forwarding transition time for control VLANs

Points to note

Set the forwarding transition time for the control VLAN of a transit node for when the Ring Protocol is in the initial status. This setting is ignored if performed for other nodes. Set the forwarding transition time for the control VLAN of a transit node (value set for the `forwarding-delay-time` parameter) to a value greater than that set for the hold time for health check frames on the master node (value set by the `health-check holdtime` command).

Command examples

1.
```
(config)# axrp 1
(config-axrp)# control-vlan 2 forwarding-delay-time 10
```
Sets the forwarding transition time for the control VLAN to 10 seconds.

24.1.5 Configuring VLAN mappings

(1) Setting new VLANs

Points to note

Bind a VLAN used for data transfer to a VLAN mapping. A single VLAN mapping can be used on multiple rings as a common definition. As many as 128 VLAN mappings can be set. Multiple VLANs can be set for a VLAN mapping by using lists.

The VLAN for data transfer used within a ring network must be the same for all nodes. However, because only VLANs for VLAN mappings specified for VLAN groups need to match, there is no need to match the VLAN mapping IDs for all nodes in a ring network.

Command examples

1.
```
(config)# axrp vlan-mapping 1 vlan 5-7
```
Sets VLAN IDs 5, 6, and 7 for VLAN mapping ID 1.

(2) Adding VLANs

Points to note

VLAN IDs can be added to VLAN mappings already set. When the ring to which an added VLAN mapping is applied is running, the mapping is reflected immediately. Also, when deletions are applied for multiple rings, they are all reflected at the same time. If a VLAN mapping is changed during ring operation, a loop might occur.

Command examples

1.
```
(config)# axrp vlan-mapping 1 vlan add 8-10
```
Adds VLAN IDs 8, 9, and 10 to VLAN mapping ID 1.

(3) Deleting VLANs

Points to note

Delete a VLAN ID from a VLAN mapping already set. If the ring to which the deleted VLAN mapping is applied is running, the deletion is reflected immediately. Also, when deletions are applied for multiple rings, they are all reflected at the same time. If a VLAN mapping is changed during ring operation, a loop might occur.

Command examples

1. `(config)# axrp vlan-mapping 1 vlan remove 8-9`

   Deletes VLAN IDs 8 and 9 from VLAN mapping ID 1.

24.1.6 Configuring a VLAN group

Points to note

VLAN mappings can be assigned to a VLAN group so that the VLAN IDs can be made to belong to the VLAN group used for the Ring Protocol. As many as two VLAN groups can be set for a single ring. As many as 128 VLAN mapping IDs can be set for a VLAN group by list specification.

Command examples

1.
```
(config)# axrp 1
(config-axrp)# vlan-group 1 vlan-mapping 1
```

   Sets VLAN mapping ID 1 for VLAN group 1.

24.1.7 Configuring modes and ring ports (for single rings and multi-ring configurations without shared links)

Figure 24-1: Single ring configuration shows a single ring configuration, and *Figure 24-2: Multi-ring configuration without shared links* shows a multi-ring configuration without shared links.

Figure 24-1: Single ring configuration

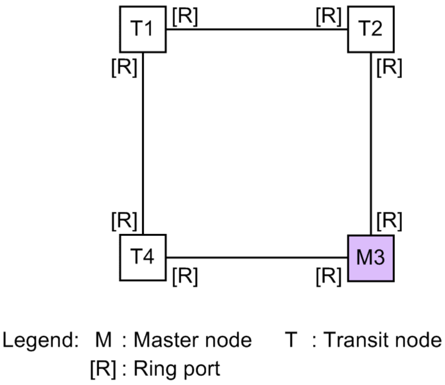
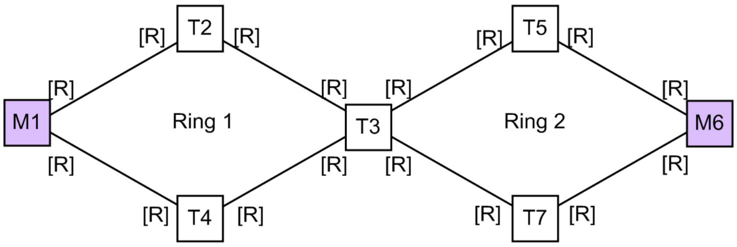


Figure 24-2: Multi-ring configuration without shared links



Legend: M : Master node T : Transit node
[R] : Ring port

The mode and ring port settings for master nodes and transit nodes in a single ring configuration or multi-ring configuration without shared links are the same.

(1) Master nodes

Points to note

Set the operating mode for the Switch to master mode in a ring. The Ethernet interface or port channel interface can be specified for a ring port. Set two ring ports for each ring. The M3 node in *Figure 24-1: Single ring configuration* and the M1 and M6 nodes in *Figure 24-2: Multi-ring configuration without shared links* correspond to this setting.

Command examples

1.
```
(config)# axrp 2
(config-axrp)# mode master
```
Sets the operation mode for ring ID 2 to master mode.

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# axrp-ring-port 2
(config-if)# exit
(config)# interface gigabitethernet 1/0/2
(config-if)# axrp-ring-port 2
```
Switches to the interface mode for ports 1/0/1 and 1/0/2, and sets the target interface as the ring port for ring ID 2.

(2) Transit node

Points to note

Set the operating mode for the Switch to transit mode in a ring. The Ethernet interface or port channel interface can be specified for a ring port. Set two ring ports for each ring. The T1, T2, and T4 nodes in *Figure 24-1: Single ring configuration*, and the T2, T3, T4, T5, and T7 nodes in *Figure 24-2: Multi-ring configuration without shared links* correspond to this setting.

Command examples

1.
```
(config)# axrp 2
(config-axrp)# mode transit
```

Sets the operating mode for ring ID 2 to transit mode.

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# axrp-ring-port 2
(config-if)# exit
(config)# interface gigabitethernet 1/0/2
(config-if)# axrp-ring-port 2
```

Switches to the interface mode for ports 1/0/1 and 1/0/2, and sets the target interface as the ring port for ring ID 2.

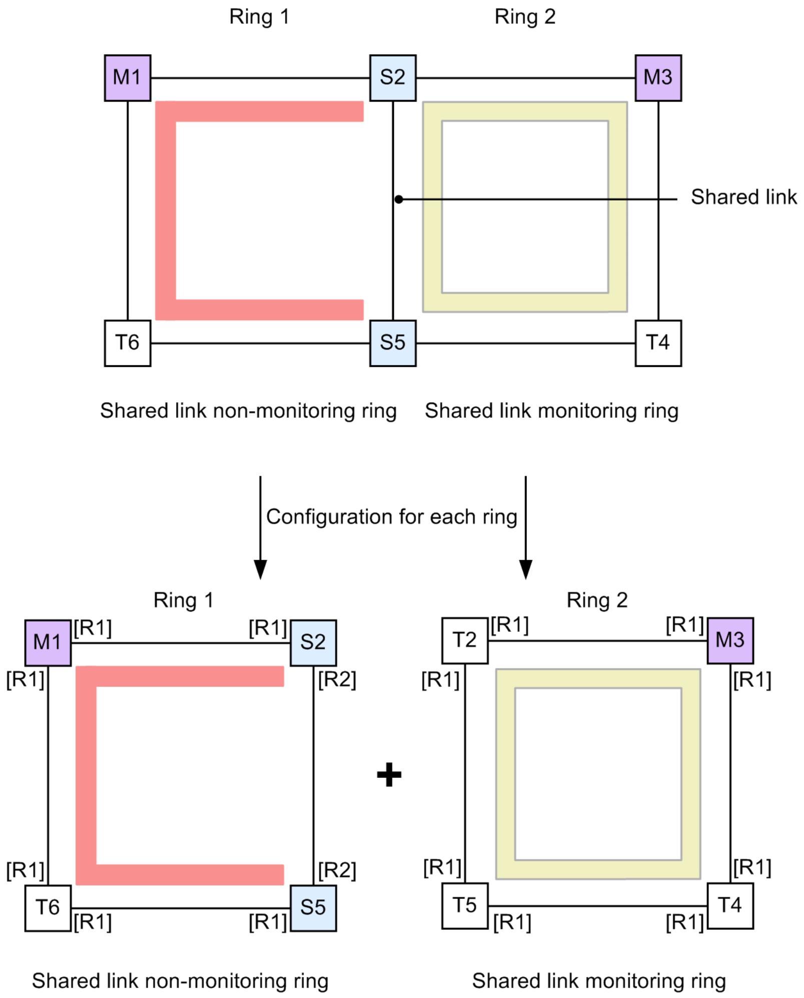
24.1.8 Configuring modes and ring ports (for multi-ring configurations with shared links)

This section gives the parameter setting patterns for modes and ring ports for multi-ring configurations with shared links.

(1) Multi-ring configurations with shared links (basic configuration)

The following figure shows a multi-ring configuration with shared links (basic configuration).

Figure 24-3: Multi-ring configurations with shared links (basic configuration)


Ring 1
Ring 2
M1
S2
M3
Shared link
T6
S5
T4
Shared link non-monitoring ring
Shared link monitoring ring
Configuration for each ring
Ring 1
[R1]
[R1]
M1
S2
[R1]
[R2]
[R1]
[R2]
T6
S5
[R1]
[R1]
Ring 2
T2
[R1]
[R1]
M3
[R1]
[R1]
[R1]
[R1]
T5
T4
[R1]
[R1]
Shared link non-monitoring ring
Shared link monitoring ring

Legend: M : Master node T : Transit node S : Shared node
[R1] : Ring port
[R2] : Ring port (port on the shared link of a terminal node in a shared link non-monitoring ring)
🟥 : Monitoring path for ring 1 🟨 : Monitoring path for ring 2

(a) Master nodes for shared link monitoring rings

This is the same as the master node for a single ring. For details, see *24.1.7 Configuring modes and ring ports (for single rings and multi-ring configurations without shared links) (1) Master nodes*. The M3 node in *Figure 24-3: Multi-ring configurations with shared links (basic configuration)* corresponds to this setting.

(b) Transit nodes for shared link monitoring rings

This is the same as transit nodes for a single ring. For details, see *24.1.7 Configuring modes and ring ports (for single rings and multi-ring configurations without shared links) (2) Transit node*. The T2, T4, and T5 nodes in *Figure 24-3: Multi-ring configurations with shared links (basic configuration)* correspond to this setting.

(c) Master nodes for shared link non-monitoring rings

Points to note

Set the operating mode for the Switch to master mode in a ring. This configuration also sets the attributes of the ring that is configured by the Switch and the associations with the Switch in the ring for the shared link non-monitoring ring. The Ethernet interface or port channel interface can be specified for a ring port. Set two ring ports for each ring. The M1 node in *Figure 24-3: Multi-ring configurations with shared links (basic configuration)* corresponds to this setting.

Command examples

1.
```
(config)# axrp 1
(config-axrp)# mode master ring-attribute rift-ring
```
Sets the operating mode of ring ID 1 to the master mode, and sets the ring attributes for the shared link non-monitoring ring.

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# axrp-ring-port 1
(config-if)# exit
(config)# interface gigabitethernet 1/0/2
(config-if)# axrp-ring-port 1
```
Switches to the interface mode for ports 1/0/1 and 1/0/2, and sets the target interface as the ring port for ring ID 1.

(d) Transit nodes for shared link non-monitoring rings

This is the same as transit nodes for a single ring. For details, see *24.1.7 Configuring modes and ring ports (for single rings and multi-ring configurations without shared links) (2) Transit node*. The T6 node in *Figure 24-3: Multi-ring configurations with shared links (basic configuration)* corresponds to this setting.

(e) Terminal nodes (transit) for shared link non-monitoring rings

Points to note

Set the operating mode for the Switch to transit mode in a ring. This configuration also sets the attributes of the ring that is configured by the Switch, and the associations with the Switch in the ring, for the terminal node of the shared link non-monitoring ring. To distinguish the terminal nodes of the shared link non-monitoring ring when more than two exist in the configuration, this configuration specifies the edge node ID (1 or 2). The S2 and S5 nodes in *Figure 24-3: Multi-ring configurations with shared links (basic configuration)* correspond to this setting. For the ring port setting, this configuration specifies `shared-edge` only for the port on the shared link. Ring port [R2] of the S2 and S5 nodes in *Figure 24-3: Multi-ring configurations with shared links (basic configuration)* correspond to this setting.

Command examples

1.
```
(config)# axrp 1
(config-axrp)# mode transit ring-attribute rift-ring-edge 1
```
Sets the operating mode for ring ID 1 to transit mode, sets the ring attributes for the terminal node of the shared link non-monitoring ring, and sets the edge node ID to 1.

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# axrp-ring-port 1
(config-if)# exit
(config)# interface gigabitethernet 1/0/2
```

```
(config-if)# axrp-ring-port 1 shared-edge
```

Switches to the interface mode for ports 1/0/1 and 1/0/2, and sets the target interface as the ring port for ring ID 1. The shared-edge parameter is also set to port 1/0/2 as a shared link.

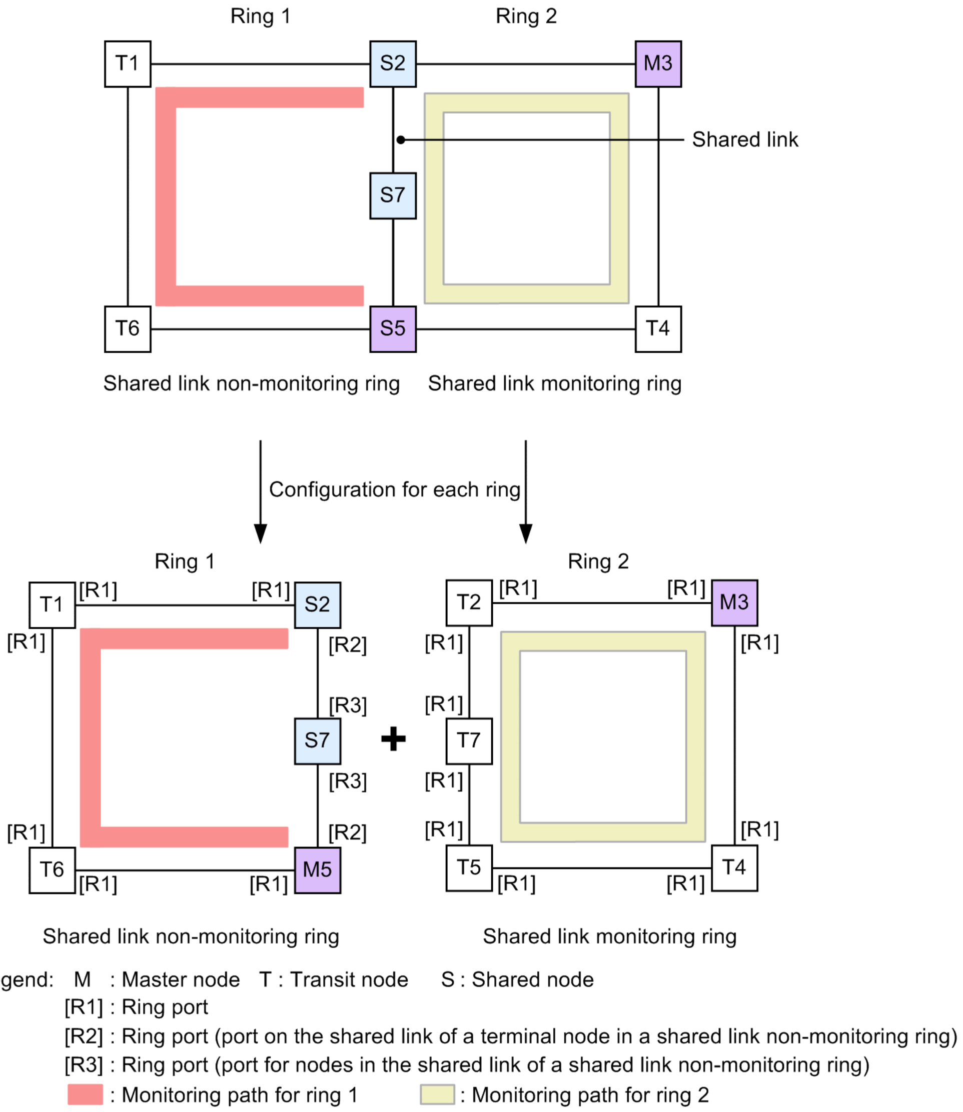
Notes

For the edge node ID, set a different ID for the other of two terminal nodes in the shared link non-monitoring ring.

(2) Multi-ring configurations with shared links (extended configuration)

The figure below shows a multi-ring configuration with shared links (extended configuration). For details about settings other than those for the terminal node (master node) of a shared link non-monitoring ring and the nodes (transit) for shared links in a shared link non-monitoring ring, see *(1) Multi-ring configurations with shared links (basic configuration)*.

Figure 24-4: Multi-ring configurations with shared links (extended configuration)


Ring 1
Ring 2
T1
S2
M3
Shared link
S7
T6
S5
T4
Shared link non-monitoring ring
Shared link monitoring ring
Configuration for each ring
Ring 1
T1
[R1]
[R1]
S2
[R1]
[R2]
[R3]
S7
[R3]
[R2]
[R1]
T6
[R1]
[R1]
M5
+
Ring 2
T2
[R1]
[R1]
M3
[R1]
[R1]
[R1]
T7
[R1]
[R1]
[R1]
T5
[R1]
[R1]
T4
Shared link non-monitoring ring
Shared link monitoring ring
Legend: M : Master node T : Transit node S : Shared node
[R1] : Ring port
[R2] : Ring port (port on the shared link of a terminal node in a shared link non-monitoring ring)
[R3] : Ring port (port for nodes in the shared link of a shared link non-monitoring ring)
🟥 : Monitoring path for ring 1
🟨 : Monitoring path for ring 2

(a) Terminal nodes for shared link non-monitoring rings (master nodes)

Points to note

Set the operating mode for the Switch to master mode in a ring. This configuration also sets the attributes of the ring that is configured by the Switch, and the associations with the Switch in the ring, for the terminal node of the shared link non-monitoring ring. To distinguish the terminal nodes of the shared link non-monitoring ring when more than two exist in the configuration, this configuration specifies the edge node ID (1 or 2). The M5 node in *Figure 24-4: Multi-ring configurations with shared links (extended configuration)* corresponds to this setting. For the ring port setting, this configuration specifies `shared-edge` only for the port on the shared link. Ring port [R2] of the M5 node in *Figure 24-4: Multi-ring configurations with shared links (extended configuration)* corresponds to this setting.

Command examples

1.
```
(config)# axrp 1
(config-axrp)# mode master ring-attribute rift-ring-edge 2
```

Sets the operating mode for ring ID 1 to master mode, sets the ring attribute for the terminal node of the shared link non-monitoring ring, and sets the edge node ID to 2.

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# axrp-ring-port 1
(config-if)# exit
(config)# interface gigabitethernet 1/0/2
(config-if)# axrp-ring-port 1 shared-edge
```

Switches to the interface mode for ports 1/0/1 and 1/0/2, and sets the target interface as the ring port for ring ID 1. The shared-edge parameter is also set to port 1/0/2 as a shared link.

Notes

For the edge node ID, set a different ID for the other of two terminal nodes in the shared link non-monitoring ring.

(b) Nodes (transit) within shared links for shared link non-monitoring rings

Points to note

Set the operating mode for the Switch to transit mode in a ring. The S7 node in *Figure 24-4: Multi-ring configurations with shared links (extended configuration)* corresponds to this setting. The `shared` parameter is specified for both ring ports, and they are set as the shared port. Ring port [R3] for the S7 node in *Figure 24-4: Multi-ring configurations with shared links (extended configuration)* corresponds to this setting.

Command examples

1.
```
(config)# axrp 1
(config-axrp)# mode transit
```

Sets the operating mode for ring ID 1 to transit mode.

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# axrp-ring-port 1 shared
(config-if)# exit
(config)# interface gigabitethernet 1/0/2
(config-if)# axrp-ring-port 1 shared
```

Switches to the interface mode for ports 1/0/1 and 1/0/2, and sets the target interface as the shared link port for ring ID 1.

Notes

1. When a port is set by specifying `shared` for the transit node within a shared link for a shared link monitoring ring, the Ring Protocol functionality will not function properly.
2. Master mode cannot be specified for a node for which `shared` is specified within a share link in a shared link non-monitoring ring.

24.1.9 Configuring various parameters

(1) Disabling the Ring Protocol functionality

Points to note

Specify commands to disable the Ring Protocol functionality. Note that when the Ring Protocol functionality is disabled while running, loops might occur in the network configuration. Therefore, before disabling the Ring Protocol functionality, use the `shutdown` command or other means to stop any interfaces running the Ring Protocol functionality.

Command examples

1.
```
(config)# axrp 1
(config-axrp)# disable
```

Switches to the axrp configuration mode for corresponding ring ID 1. The `disable` command is executed to disable the Ring Protocol functionality.

(2) Health-check frame sending interval

Points to note

Set the health-check frame sending interval for the master node or terminal nodes on a shared link non-monitoring ring. This setting is ignored if performed for other nodes.

Command examples

1.
```
(config)# axrp 1
(config-axrp)# health-check interval 500
```

Sets the sending interval for health check frames to 500 ms.

Notes

For a multi-ring configuration, set the same value for the health-check frame sending interval in the same ring for the master node and the terminal nodes of shared link non-monitoring rings. If these values are different, fault detection will not be performed properly.

(3) Health-check frame reception hold time

Points to note

Set the health-check frame reception hold time for the master node. This setting is ignored if performed for other nodes. The reception hold time can be changed to adjust the time needed to detect faults.

Set the reception hold time (value set using the `health-check holdtime` command) to a value greater than the sending interval (value set using the `health-check interval` command).

Command examples

1. `(config)# axrp 1`

```
(config-axrp)# health-check holdtime 1500
```

Sets the reception hold time for health check frames to 1500 ms.

(4) Flush-control frame reception hold time

Points to note

Set the flush-control frame reception hold time for transit nodes. This setting is ignored if performed for other nodes. The flush-control frame reception hold time for transit nodes (value set using the `forwarding-shift-time` command) must be a value greater than the sending interval for health check frames for the master node (value set by the `health-check interval` command). If the ring port of a transit node is changed to the forwarding status before the master node detects restoration from an incorrect setting, a loop might occur temporarily.

Command examples

1. `(config)# axrp 1`

```
(config-axrp)# forwarding-shift-time 100
```

Sets the reception hold time for flush control frames to 100 seconds.

(5) Setting primary ports

Points to note

Set the primary port for a master node. Specify an interface with a ring port (using the `axrp-ring-port` command) specified for the master node. Note that operation will not be performed regardless of this setting if the Switch is the terminal of a shared link non-monitoring ring. Normally, because primary ports are automatically assigned, when a setting or change is performed using the `axrp-primary-port` command to switch the primary port, ring operation is stopped.

Command examples

1. `(config)# interface port-channel 10`

```
(config-if)# axrp-primary-port 1 vlan-group 1
```

Switches to the port channel interface configuration mode, sets the corresponding interface for ring ID 1, and sets the primary port for VLAN group ID 1.

(6) Enabling the path switch-back suppression functionality and setting suppression times

Points to note

Set the time to suppress path switch-back operation after fault restoration has been detected on the master node. Note that when `infinity` is specified for the suppression time, path switch-back operation is suppressed until the `clear axrp preempt-delay` operation command is executed.

Command examples

1. `(config)# axrp 1`

```
(config-axrp)# preempt-delay infinity
```

Switches to configuration mode for ring ID 1, and sets the path switch-back suppression time to `infinity`.

24.1.10 Configuring the multi-fault monitoring functionality

(1) Setting multi-fault monitoring VLANs

Points to note

Set the VLAN to be used as the multi-fault monitoring VLAN for each node in a shared link monitoring ring. Note that VLANs used as the control VLAN and VLAN for data transfer cannot be used. Note that VLAN IDs with the same value as the VLAN ID of a multi-fault monitoring VLAN used in a different ring cannot be used.

Command examples

1.
```
(config)# axrp 1
```
Switches to axrp configuration mode for ring ID 1.

2.
```
(config-axrp)# multi-fault-detection vlan 20
```
Sets VLAN 20 as the multi-fault monitoring VLAN.

Notes

Set the multi-fault monitoring VLAN on all nodes in shared link monitoring rings to which the multi-fault monitoring functionality is applied.

(2) Setting monitoring modes for the multi-fault monitoring functionality

Points to note

Set the monitoring mode for multi-fault monitoring for each node in a shared link monitoring ring, as well as the ring ID of the shared link non-monitoring ring used as the backup ring during multi-fault detection. Sets the monitoring mode to `monitor-enable` for shared nodes performing multi-fault monitoring, and to `transport-only` on other devices. Sets the ring ID of the backup ring for shared nodes.

(a) Shared nodes for shared link monitoring ring

Command examples

1.
```
(config)# axrp 1
```
Switches to axrp configuration mode for ring ID 1.

2.
```
(config-axrp)# multi-fault-detection mode monitor-enable
backup-ring 2
```
Sets the monitoring mode for multi-fault monitoring to `monitor-enable` and the ring ID of the backup ring to 2.

Notes

Set the `monitor-enable` monitoring mode for multi-fault monitoring on the two shared nodes placed at the ends of a shared link. When it is set for just one node, multi-fault monitoring is not performed.

(b) Other nodes for shared link monitoring rings

Command examples

1. `(config)# axrp 1`

   Switches to axrp configuration mode for ring ID 1.

2. `(config-axrp)# multi-fault-detection mode transport-only`

   Sets the monitoring mode for multi-fault monitoring to `transport-only`.

(3) Sending intervals for multi-fault monitoring frame

Points to note

Set the sending interval for multi-fault monitoring frames on shared nodes in a shared link monitoring ring. This setting is ignored if performed for other nodes.

Command examples

1. `(config)# axrp 1`

   `(config-axrp)# multi-fault-detection interval 1000`

   Sets the sending interval for multi-fault monitoring frames to 1000 ms.

(4) Reception hold times for multi-fault monitoring frames

Points to note

Set the reception hold time for multi-fault monitoring frames on shared nodes in a shared link monitoring ring. This setting is ignored if performed for other nodes.

Command examples

1. `(config)# axrp 1`

   `(config-axrp)# multi-fault-detection holdtime 3000`

   Sets the reception hold time for multi-fault monitoring frames to 3000 ms.

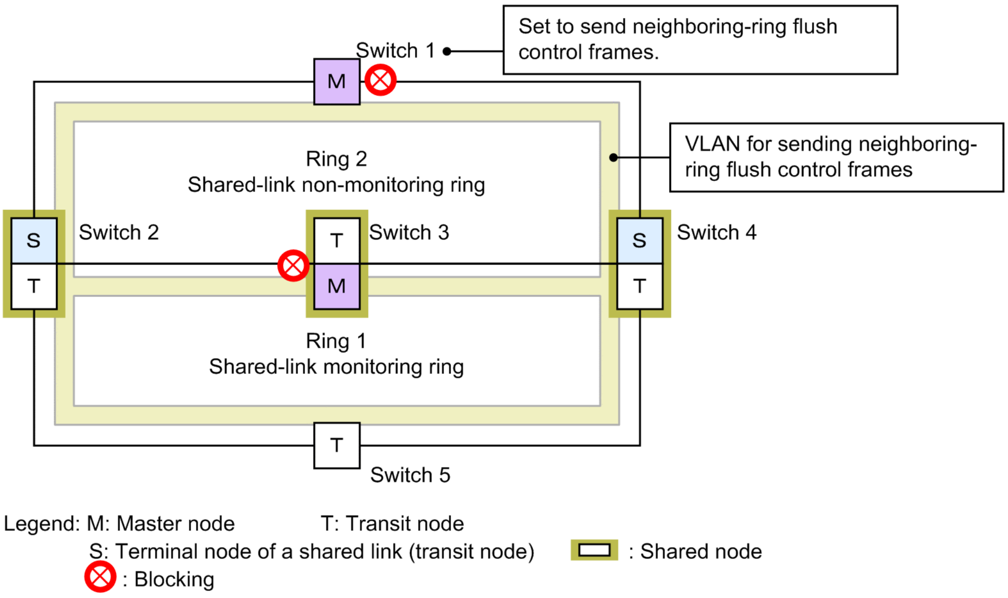
Notes

Set the reception hold time (value set using the `multi-fault-detection holdtime` command) to a value greater than the sending interval of the opposing shared node (value set using the `multi-fault-detection interval` command).

24.1.11 Configuring flush control frames for neighboring rings

The figure below shows a configuration in which both ring ports of the master node are shared links. For such configurations, set the master node of a shared link non-monitoring ring to send flush control frames for neighboring rings.

Figure 24-5: Configurations in which both ring ports of a master node are shared links


Set to send neighboring-ring flush control frames.
Switch 1
M
VLAN for sending neighboring-ring flush control frames
Ring 2
Shared-link non-monitoring ring
S
T
Switch 2
T
M
Switch 3
S
T
Switch 4
Ring 1
Shared-link monitoring ring
T
Switch 5
Legend: M: Master node
T: Transit node
S: Terminal node of a shared link (transit node)
: Shared node
: Blocking

Points to note

In a multi-ring configuration shown in *Figure 24-5: Configurations in which both ring ports of a master node are shared links*, both ring ports of the master node (switch 3 of ring 1) are shared links. In such configurations, set the master node of a shared link non-monitoring ring (switch 1 of ring 2) to send flush control frames for neighboring rings.

At that point, also bind a VLAN, which is used to send flush control frames for neighboring rings, to VLAN mapping on each node of sending-destination rings.

Do not use this VLAN for data transfer and use it only for sending flush control frames for neighboring rings.

Command examples

1.
```
(config)# axrp 2
(config-axrp)# flush-request-transmit vlan 10
```

Enters configuration mode for ring ID 2 (master node of a shared link non-monitoring ring) and sets it to send flush control frames for neighboring rings to VLAN ID 10 when a fault or recovery occurs on ring ID 2.

24.2 Operation

24.2.1 List of operation commands

The following table describes the operation commands for the Ring Protocol.

Table 24-2: List of operation commands

Command name	Description
show axrp	Shows Ring Protocol information.
clear axrp	Clears Ring Protocol statistics.
clear axrp preempt-delay	Clears the path switch-back suppression status for a ring.
restart axrp	Restarts a Ring Protocol program.
dump protocols axrp	Outputs to a file detailed event trace information and control table information collected by the Ring Protocol program.
show port[#1]	Shows the usage status of the Ring Protocol for a port.
show vlan[#2]	Shows the usage status of the Ring Protocol for a VLAN.

#1

For details, see *16. Ethernet* in the manual *Operation Command Reference Vol.1 For Version 11.10*.

#2

See *19. VLAN* in the manual *Operation Command Reference Vol.1 For Version 11.10*.

24.2.2 Checking Ring Protocol statuses

(1) Checking the configuration settings and operation statuses

The `show axrp` command can be used to check the Ring Protocol settings and operation status. Use it to check whether Ring Protocol settings set by using configuration commands have been applied properly. The `show axrp` *<ring id list>* command can be used to check the status information for each ring.

The information displayed differs depending on the contents of `Oper State` item. If `enable` is displayed for `Oper State`, the Ring Protocol functionality is running. The operation status of all items is indicated by the contents displayed. When `-` is displayed for `Oper State`, the item has not had its status obtained by the required configuration command. When `Not Operating` is displayed for `Oper State`, the Ring Protocol functionality cannot run because a conflict exists in the configuration. When `-` or `Not Operating` is displayed for `Oper State`, check the configuration.

The following figures show examples of the `show axrp` command and `show axrp detail` command.

Figure 24-6: Results of executing the show axrp command

```
> show axrp
Date 20XX/01/27 12:00:00 UTC

Total Ring Counts:4

Ring ID:1
 Name:RING#1
 Oper State:enable           Mode:Master     Attribute:-

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              0/1        primary/forwarding    0/2        secondary/blocking
 2              0/1        secondary/blocking    0/2        primary/forwarding

Ring ID:2
 Name:RING#2
 Oper State:enable           Mode:Transit    Attribute:-

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              1(ChGr)    -/forwarding          2(ChGr)    -/forwarding
 2              1(ChGr)    -/forwarding          2(ChGr)    -/forwarding

Ring ID:3
 Name:
 Oper State:disable          Mode:-          Attribute:-

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              -          -/-                   -          -/-
 2              -          -/-                   -          -/-

Ring ID:4
 Name:RING#4
 Oper State:enable           Mode:Transit    Attribute:rift-ring-edge(1)
 Shared Edge Port:0/3

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              0/3        -/-                   0/4        -/forwarding
 2              0/3        -/-                   0/4        -/forwarding
>
```

The `show axrp detail` command can be used to check statistics and detailed information about the ring status for the master node. 0 is displayed for statistics unless the Ring Protocol functionality is enabled (`enable` is displayed for `Oper State`).

Figure 24-7: Results of executing the show axrp detail command

```
> show axrp detail
Date 20XX/01/27 12:00:00 UTC

Total Ring Counts:4

Ring ID:1
 Name:RING#1
 Oper State:enable           Mode:Master     Attribute:-
 Control VLAN ID:5           Ring State:normal
 Health Check Interval  (msec):1000
 Health Check Hold Time (msec):3000
 Flush Request Counts:3

 VLAN Group ID:1
  VLAN ID:6-10,12
  Ring Port:0/1         Role:primary      State:forwarding
  Ring Port:0/2         Role:secondary    State:blocking

 VLAN Group ID:2
  VLAN ID:16-20,22
  Ring Port:0/1         Role:secondary    State:blocking
  Ring Port:0/2         Role:primary      State:forwarding

Last Transition Time:20XX/01/24 10:00:00
Fault Counts    Recovery Counts    Total Flush Request Counts
1               1                  12

Ring ID:2
 Name:RING#2
 Oper State:enable           Mode : Transit    Attribute : -
 Control VLAN ID:15
 Forwarding Shift Time (sec):10
 Last Forwarding:flush request receive

 VLAN Group ID:1
  VLAN ID  :26-30,32
  Ring Port:1(ChGr)     Role:-            State:forwarding
  Ring Port:2(ChGr)     Role:-            State:forwarding

 VLAN Group ID:2
  VLAN ID:36-40,42
  Ring Port:1(ChGr)     Role:-            State:forwarding
  Ring Port:2(ChGr)     Role:-            State:forwarding

Ring ID:3
 Name:
 Oper State:disable          Mode:-          Attribute:-
 Control VLAN ID:-

 VLAN Group ID:1
  VLAN ID:-
  Ring Port:-           Role:-            State:-
  Ring Port:-           Role:-            State:-

 VLAN Group ID:2
  VLAN ID:-
  Ring Port:-           Role:-            State:-
  Ring Port:-           Role:-            State:-

Ring ID:4
 Name:RING#4
 Oper State:enable           Mode:Transit    Attribute:rift-ring-edge(1)
 Shared Edge Port:0/3
 Control VLAN ID:45
 Health Check Interval  (msec):1000
 Forwarding Shift Time (sec):10
 Last Forwarding:flush request receive

 VLAN Group ID:1
  VLAN ID:46-50,52
  Ring Port:0/3         Role:-            State:-
  Ring Port:0/4         Role:-            State:forwarding

 VLAN Group ID:2
  VLAN ID:56-60,62
  Ring Port:0/3         Role:-            State:-
  Ring Port:0/4         Role:-            State:forwarding
>
```

When the multi-fault monitoring functionality is applied, the `show axrp detail` command can be used to check information about the multi-fault monitoring status.

Figure 24-8: Results of executing the show axrp detail command when the multi-fault monitoring functionality is applied

```
> show axrp detail
Date 20XX/03/10 12:00:00 UTC

Total Ring Counts:2

Ring ID:10
 Name:RING#10
 Oper State:enable           Mode:Master     Attribute:-
 Control VLAN ID:10          Ring State:normal
 Health Check Interval  (msec):1000
 Health Check Hold Time (msec):3000
 Flush Request Counts:3

 VLAN Group ID:1
```

```
  VLAN ID:100-150
  Ring Port:0/1         Role:primary      State:forwarding
  Ring Port:0/2         Role:secondary    State:blocking

 VLAN Group ID:2
  VLAN ID:151-200
  Ring Port:0/1         Role:primary      State:forwarding
  Ring Port:0/2         Role:secondary    State:blocking

Last Transition Time:20XX/03/01 10:00:00
Fault Counts    Recovery Counts    Total Flush Request Counts
1               1                  12

Multi Fault Detection State:normal
 Mode:monitoring    Backup Ring ID:20
 Control VLAN ID:500
 Multi Fault Detection Interval  (msec):2000
 Multi Fault Detection Hold Time (msec):6000

Ring ID:20
 Name:RING#20
 Oper State:enable           Mode:Transit    Attribute:rift-ring-edge(1)
 Shared Edge Port:0/1
 Control VLAN ID:20
 Health Check Interval  (msec):1000
 Forwarding Shift Time (sec):10
 Last Forwarding:flush request receive

 VLAN Group ID:1
  VLAN ID:100-150
  Ring Port:0/1         Role:-            State:-
  Ring Port:0/3         Role:-            State:forwarding

 VLAN Group ID:2
  VLAN ID:151-200
  Ring Port:0/1         Role:-            State:-
  Ring Port:0/3         Role:-            State:forwarding
>
```

Chapter

25. Using the Ring Protocol with Spanning Tree Protocols/GSRP

This chapter explains how to use the Ring Protocol on the same device as a Spanning Tree Protocol or GSRP.

25.1 Using the Ring Protocol with Spanning Tree Protocols

The Switch can use the Ring Protocol together with a Spanning Tree Protocol. For details about the protocol types for Spanning Tree Protocols that can be used with the Ring Protocol, see *18.3 Compatibility between Layer 2 switch functionality and other functionality*. For details about the Ring Protocol, see *23. Description of the Ring Protocol*.

25.1.1 Overview

The Ring Protocol and a Spanning Tree Protocol can be used together on the same device, to configure a network that uses the Ring Protocol for the core network and a Spanning Tree Protocol for the access network. For example, when a network consists entirely of Spanning Tree Protocols and only the core network is changed to the Ring Protocol, a significant share of existing facilities for the access network can be diverted without any changes. Note that the Ring Protocol can be used with Spanning Tree Protocols for both single rings and multi-rings (including multi-rings with shared links).

The figures below give examples of the Ring Protocol being used with Spanning Tree Protocols for single ring configurations or multi-ring configurations. Switches A/G/I, B/F/J, and C/D/K each comprise a Spanning Tree topology. The Ring Protocol and Spanning Tree Protocol are used at the same time for Switches A to D and F to G.

Figure 25-1: Example using the Ring Protocol and Spanning Tree Protocols together (single ring configuration)

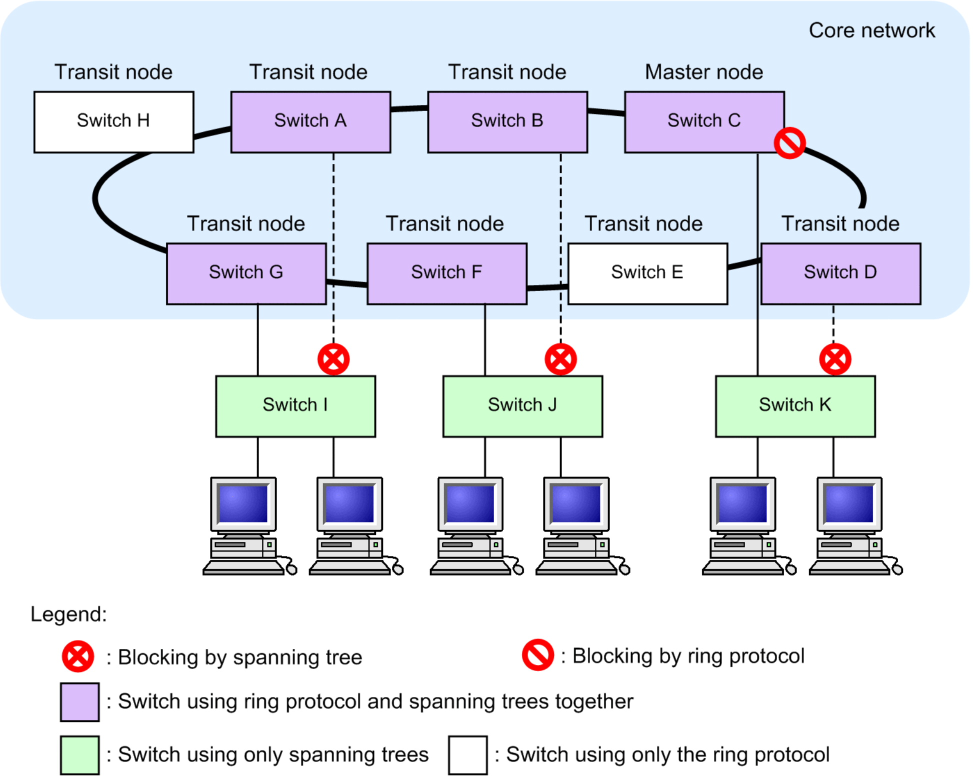
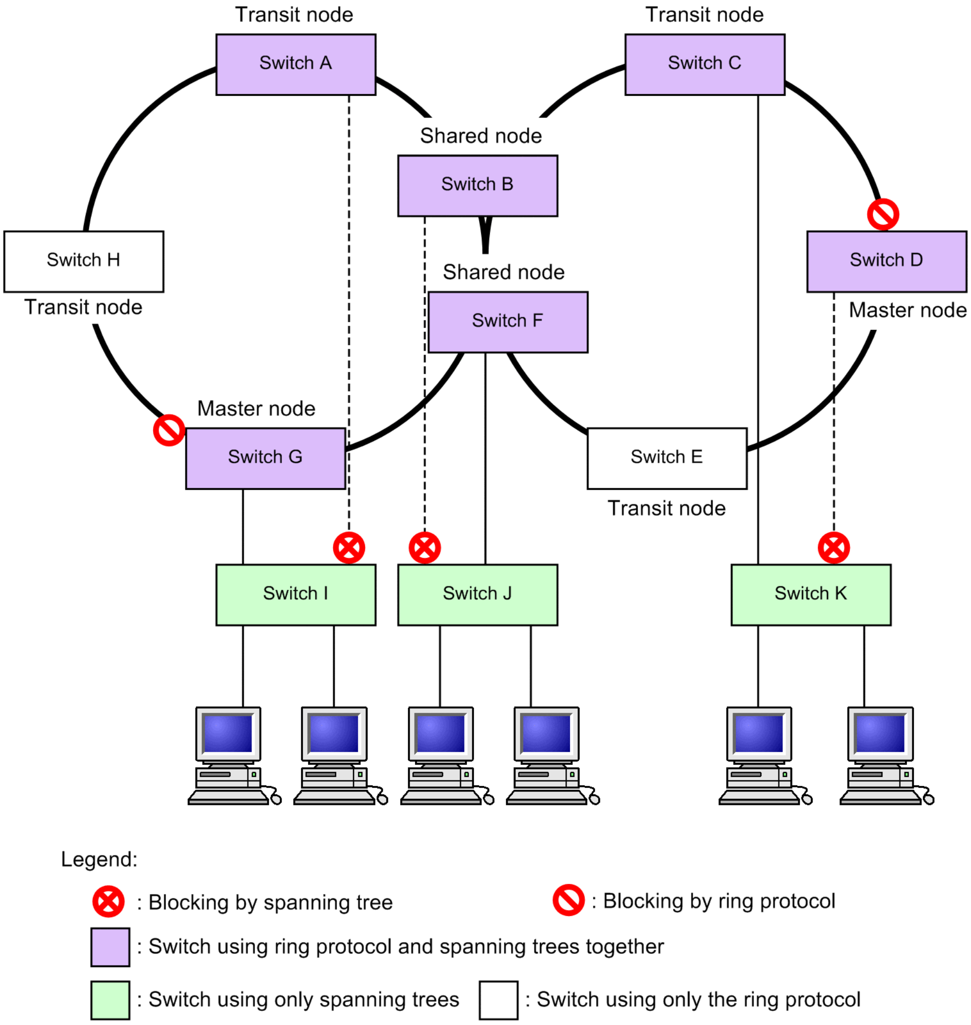


Figure 25-2: Example using the Ring Protocol and Spanning Tree Protocols together (multi-ring configuration)



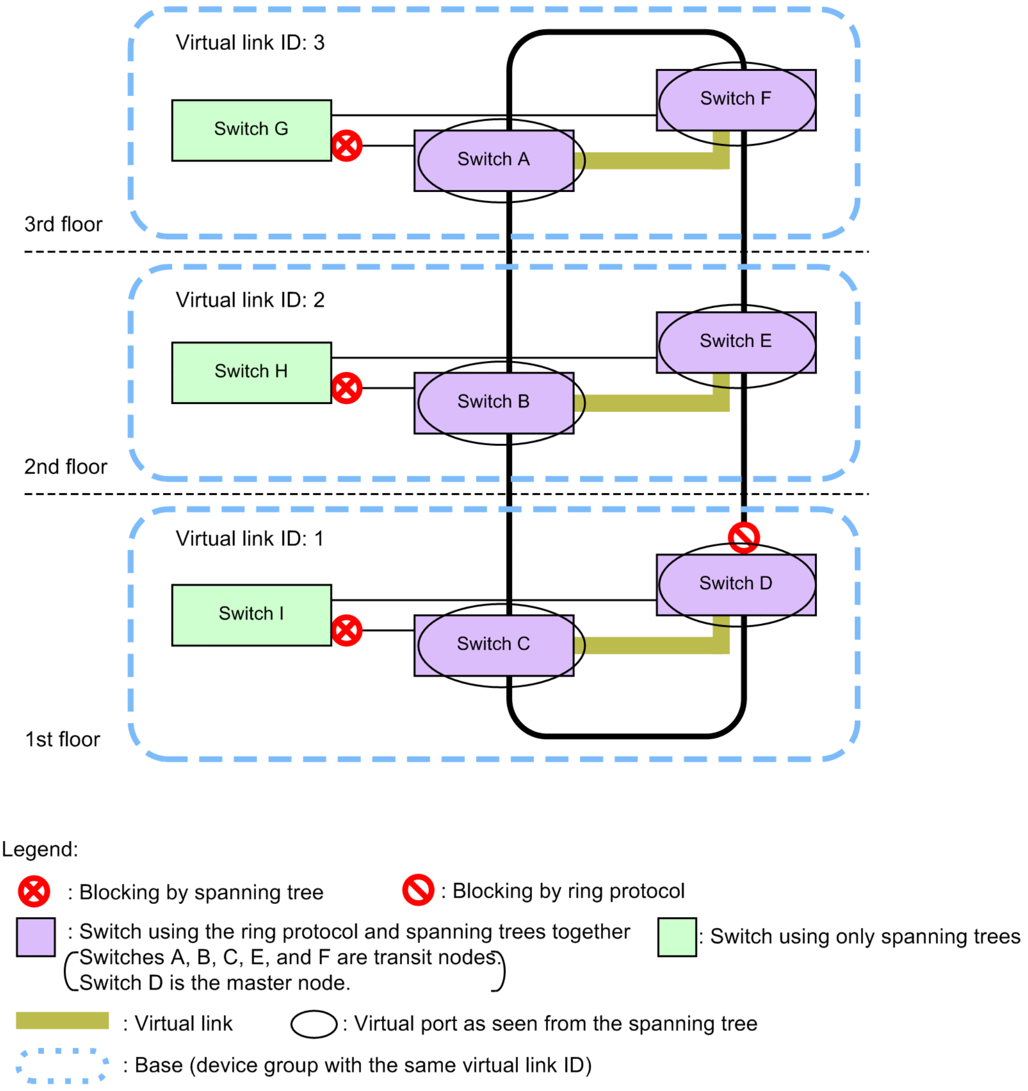
25.1.2 Operating specifications

To use the Ring Protocol and Spanning Tree Protocols together, a virtual line must be connected between any two devices on which both functionalities exist. This virtual line is called a virtual link. Virtual links are built between two devices on a ring network. Building a virtual link requires a virtual link ID for identifying the virtual link, and a virtual link VLAN for sending and receiving control frames between virtual links.

Nodes using the Ring Protocol and Spanning Tree Protocols together comprise a Spanning Tree topology with devices that have the same virtual link ID as that of the local device. Device groups with the same virtual link ID are called bases, and each base comprises an independent Spanning Tree topology.

The following figure gives an overview of virtual links.

Figure 25-3: Overview of virtual links


Virtual link ID: 3
Switch G
Switch A
Switch F
3rd floor
Virtual link ID: 2
Switch H
Switch B
Switch E
2nd floor
Virtual link ID: 1
Switch I
Switch C
Switch D
1st floor
Legend:
: Blocking by spanning tree
: Blocking by ring protocol
: Switch using the ring protocol and spanning trees together
Switches A, B, C, E, and F are transit nodes.
Switch D is the master node.
: Switch using only spanning trees
: Virtual link
: Virtual port as seen from the spanning tree
: Base (device group with the same virtual link ID)

Note: Each floor comprises an independent spanning tree topology.

(1) Virtual link VLANs

A virtual link VLAN is used to send and receive control frames between virtual links. One of the VLANs managed as a VLAN for data transfer for the ring port is used as the virtual link VLAN. A virtual link VLAN can use the same VLAN ID on multiple bases.

(2) Handling control VLANs for the Ring Protocol

Control VLANs for the Ring Protocol are not subject to Spanning Tree Protocols.

Therefore, a tree of corresponding VLANs is not built for PVST+. Also, the transfer status for Single Spanning Tree and Multiple Spanning Tree is not applied.

(3) Ring port statuses and configuration setting values

The transfer status of the VLAN for data transfer for a ring port is determined by the Ring Protocol.

For example, when the `Blocking` status is determined by a Spanning Tree topology, if the Ring Protocol determines it to be `Forwarding`, the status of the port is `Forwarding`. Therefore, when a topology is built in which the ring port is `Blocking` for the Spanning Tree Protocol, a loop might occur. This means that for a Spanning Tree Protocol used with the Ring Protocol and for which the ring port is always `Forwarding`, the initial value of the bridge priority for the Switch is automatically raised so that the Switch becomes the root bridge or next item in priority. Any values set by configuration will be used for operation.

The following table describes the value set for bridge priority.

Table 25-1: Value set for bridge priority

Configuration items	Related configuration	Initial value
Bridge priority	spanning-tree single priority spanning-tree vlan priority spanning-tree mst root priority	0

Note that the port for a virtual link runs with a fixed value because values set by configuration are not applied.

The following table describes the values set for virtual link ports.

Table 25-2: Values set for virtual link ports

Configuration items	Related configuration	Initial value (fixed)
Link type	spanning-tree link-type	point-to-point
Port priority	spanning-tree port-priority spanning-tree single port-priority spanning-tree vlan port-priority spanning-tree mst port-priority	0
Path cost	spanning-tree cost spanning-tree single cost spanning-tree vlan cost spanning-tree mst cost	1

(4) Spanning Tree functionality for ring ports

The following Spanning Tree functionality does not work for ring ports.

- BPDU filter
- BPDU guard
- Loop guard functionality
- Root guard functionality
- PortFast functionality

(5) Clearing the MAC address table during Spanning Tree topology changes

When the topology is changed for a Spanning Tree Protocol, a flush control frame is sent so that MAC address table entries are cleared for the entire single ring or multi-ring network. Each device receiving this in the ring network clears MAC address table entries for ring ports for which the Ring Protocol is running. Note that the base device for which the topology change occurs clears MAC address table entries through the Spanning Tree Protocol.

(6) Temporary blocking for ports other than ring ports

When one of the following events occurs on a device using both the Ring Protocol and a Spanning Tree Protocol, ports for the Spanning Tree Protocol other than for the ring port are temporarily put in `Blocking` status.

- Switch startup (including restarting of the switch)
- Application of the configuration file to a running configuration

- Executing the `restart vlan` command
- Executing the `restart spanning-tree` command

When the topology within an access network is built before control frames can be sent and received by the Spanning Tree Protocol over a virtual link, no ports are changed to `Blocking`, because this alone will not cause a loop configuration. However, because a loop configuration will occur across the ring network and access network if this is left as is, this functionality is used to temporarily set the `Blocking` status to prevent loops. This functionality can also run on ports for which PortFast functionality is set, and sets the `Blocking` status when any of the following occur:

- 20 seconds elapse after an event occurred
- 6 seconds elapse after reception when a control frame is received over a virtual link within 20 seconds after an event occurred

To run this functionality effectively, configure the setting values within the ranges shown in the table below. If these values are not set within range, loops might occur temporarily.

Table 25-3: Values for setting the Blocking status temporarily for ports other than ring ports

Configuration items	Related configuration	Value set
Reception hold time for Ring Protocol flush control frames	forwarding-shift-time	10 seconds or less (default value of 10 seconds)
Spanning Tree control frame sending interval	spanning-tree single hello-time spanning-tree vlan hello-time spanning-tree mst hello-time	2 seconds or less (default value of 2 seconds)

25.1.3 Compatibility with various Spanning Tree Protocols

(1) Compatibility with PVST+

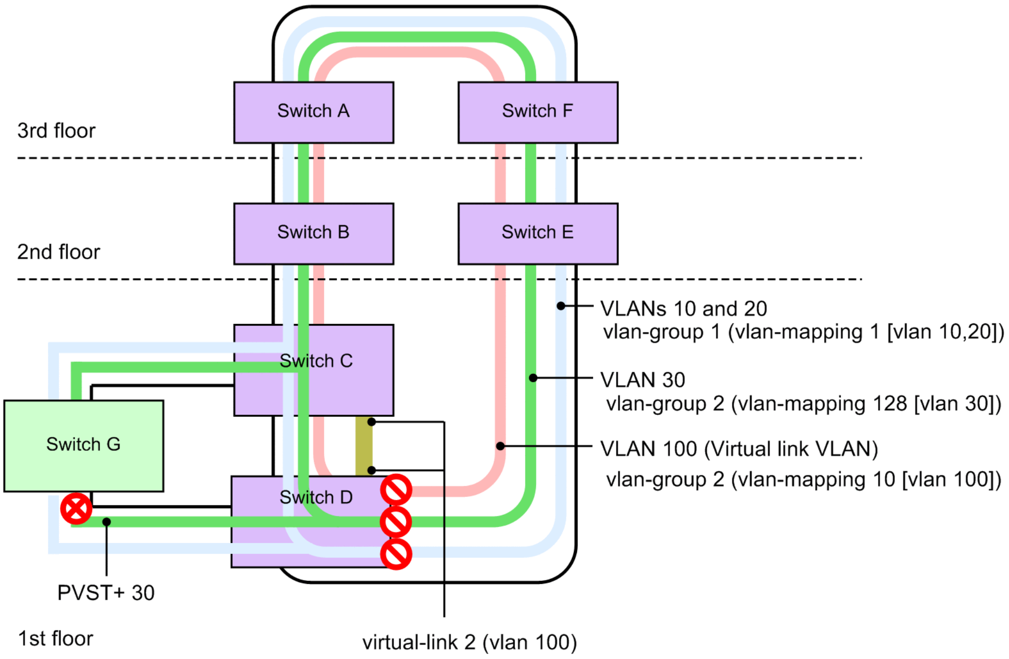
For PVST+, if only one VLAN is set for the VLAN mapping of the Ring Protocol, the VLAN can be used with the Ring Protocol. When the `axrp virtual-link` configuration command is used to set a virtual link, topologies are built by virtual links, and usage with the Ring Protocol starts.

Under the initial Ring Protocol configuration settings, all running PVST+ instances are stopped, and then started sequentially for VLANs for which a VLAN mapping is set. If multiple VLANs are set for a VLAN mapping, PVST+ will not run for the VLANs. Note that loops might occur for VLANs for which PVST+ is stopped. Perform port blockage or other actions to prevent loop configurations.

Because virtual links cannot be built when the `axrp virtual-link` configuration command has not been used to set a virtual link, the intended topology cannot be built, which might cause loops to occur.

The figure below shows a configuration in which PVST+ and the Ring Protocol are used together. In the figure, because only one VLAN 30 is set for VLAN mapping 128, it runs as PVST+. Because multiple VLANs are set for VLAN mapping 1, PVST+ cannot run. Also, because VLAN 100 is set as the virtual link VLAN for switches C and D, a virtual link is built between both switches.

Figure 25-4: Configuration using PVST+ and the Ring Protocol together


3rd floor
2nd floor
1st floor
Switch A
Switch F
Switch B
Switch E
Switch C
Switch D
Switch G
VLANs 10 and 20
vlan-group 1 (vlan-mapping 1 [vlan 10,20])
VLAN 30
vlan-group 2 (vlan-mapping 128 [vlan 30])
VLAN 100 (Virtual link VLAN)
vlan-group 2 (vlan-mapping 10 [vlan 100])
PVST+ 30
virtual-link 2 (vlan 100)

Switches A, B, E, and F : Switches comprising a ring protocol using VLANs 10, 20, 30, and 100
Switches C and D : Switches using a ring protocol using VLANs 10, 20, and 30 together with PVST+ 30. VLAN 100 is used as a virtual link VLAN.
Switch G : Switch using only PVST+ 30

Legend:

⊗ : Blocking by spanning tree   🚫 : Blocking by ring protocol

🟪 : Switch using the ring protocol and spanning trees together   🟩 : Switch using only spanning trees

▬ : Virtual link

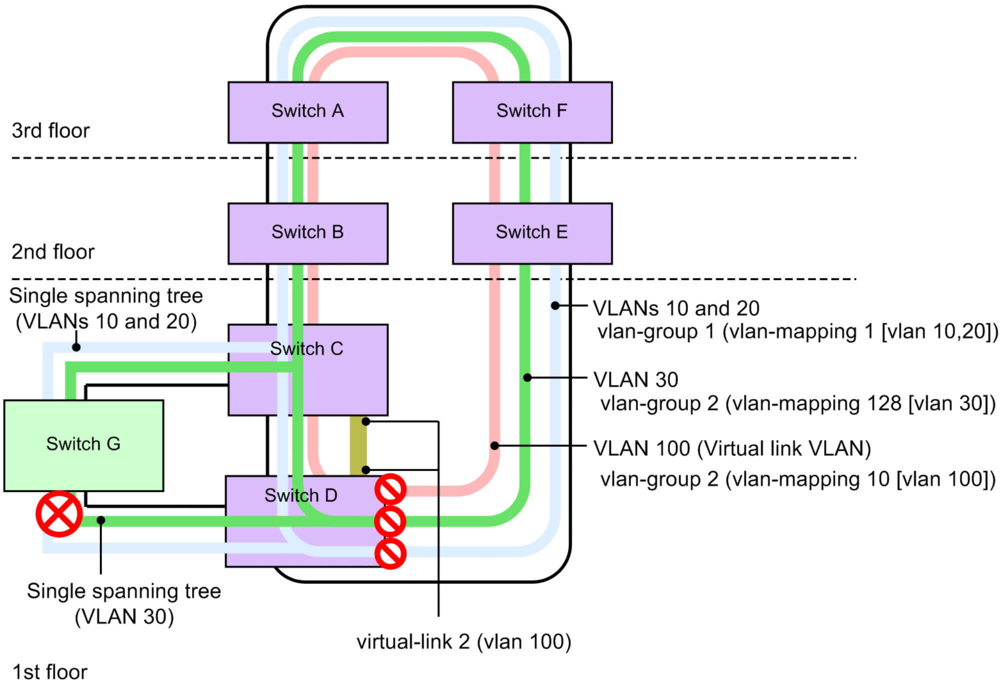
(2) Compatibility with Single Spanning Tree

Single Spanning Tree can be used with all data VLANs for which the Ring Protocol is running.

For Single Spanning Tree, when the `axrp virtual-link` configuration command is used to set a virtual link, a topology based on the virtual link is built and usage with the Ring Protocol starts. When the `axrp virtual-link` configuration command is not used to set a virtual link, the intended topology cannot be built because virtual links cannot be built. As a result, loops might occur.

The figure below shows a configuration in which Single Spanning Tree and the Ring Protocol are used together. In the figure, Single Spanning Tree is set for switches C, D, and G, and two VLAN groups for the Ring Protocol are set for switches A, B, C, D, E, and F. Each topology for Single Spanning Tree is applied to the VLANs belonging to all VLAN groups (all VLAN mappings). Also, because VLAN 100 is set as the virtual link VLAN for switches C and D, a virtual link is built between both switches.

Figure 25-5: Configuration using Single Spanning Tree and the Ring Protocol together


Switch A
Switch F
3rd floor
Switch B
Switch E
2nd floor
Single spanning tree
(VLANs 10 and 20)
Switch C
Switch G
Switch D
VLANs 10 and 20
vlan-group 1 (vlan-mapping 1 [vlan 10,20])
VLAN 30
vlan-group 2 (vlan-mapping 128 [vlan 30])
VLAN 100 (Virtual link VLAN)
vlan-group 2 (vlan-mapping 10 [vlan 100])
Single spanning tree
(VLAN 30)
virtual-link 2 (vlan 100)
1st floor

Switches A, B, E, and F	: Switches comprising a ring protocol using VLANs 10, 20, and 30
Switches C and D	: Switches using a ring protocol using VLANs 10, 20, and 30 together with a single spanning tree VLAN 100 is used as a virtual link VLAN.
Switch G	: Switch using only a single spanning tree

Legend:

⊗ : Blocking by spanning tree 🚫 : Blocking by ring protocol

🟪 : Switch using the ring protocol and spanning trees together 🟩 : Switch using only spanning trees

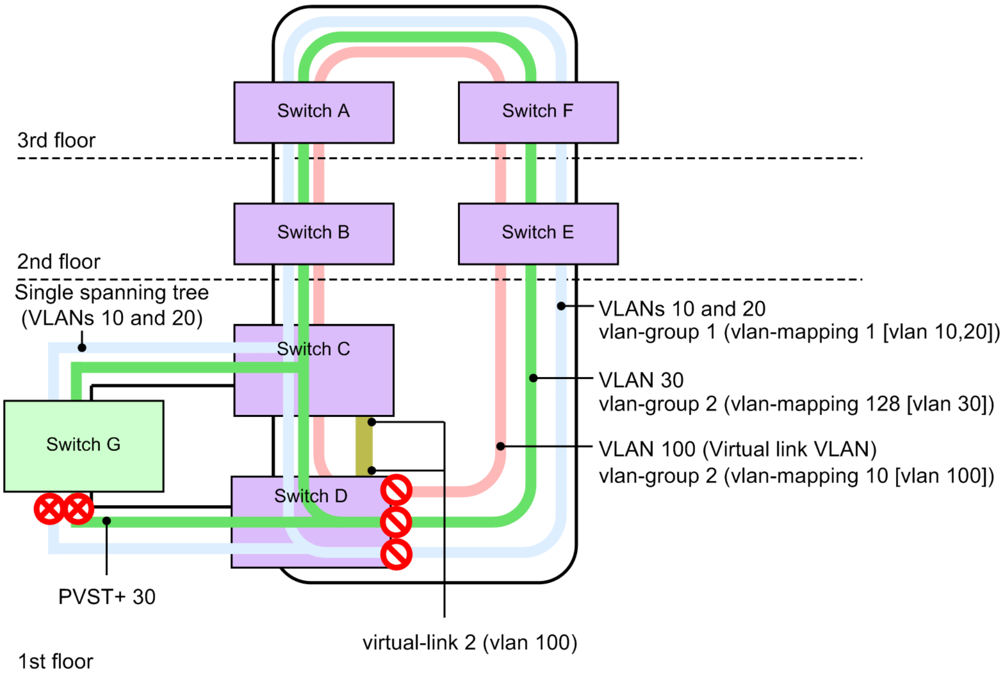
▬ : Virtual link

(3) Running PVST+ and Single Spanning Tree at the same time

Even when used with the Ring Protocol, PVST+ and Single Spanning Tree can be used at the same time. In this case, all VLANs not running with PVST+ are run as Single Spanning Tree (the same as for normal concurrent operation).

The figure below shows a configuration in which Single Spanning Tree, PVST+, and the Ring Protocol are used together. In the figure, because only one VLAN 30 is set for VLAN mapping 128, it runs as PVST+. Because PVST+ is not running for VLAN mapping 1, it runs as Single Spanning Tree, and reflects the topology. Also, because VLAN 100 is set as the virtual link VLAN for switches C and D, a virtual link is built between both switches.

Figure 25-6: Configuration using Single Spanning Tree, PVST+, and the Ring Protocol together


Switch A
Switch F
3rd floor
Switch B
Switch E
2nd floor
Single spanning tree
(VLANs 10 and 20)
Switch C
Switch G
Switch D
VLANs 10 and 20
vlan-group 1 (vlan-mapping 1 [vlan 10,20])
VLAN 30
vlan-group 2 (vlan-mapping 128 [vlan 30])
VLAN 100 (Virtual link VLAN)
vlan-group 2 (vlan-mapping 10 [vlan 100])
PVST+ 30
virtual-link 2 (vlan 100)
1st floor

Switches A, B, E, and F	: Switches comprising a ring protocol using VLANs 10, 20, and 30
Switches C and D	: Switches using a ring protocol using VLANs 10, 20, and 30 together with PVST+ 30 and a single spanning tree VLAN 100 is used as a virtual link VLAN.
Switch G	: Switch using PVST+ 30 and a single spanning tree together

Legend:

⊗ : Blocking by spanning tree 🚫 : Blocking by ring protocol

🟪 : Switch using the ring protocol and spanning trees together 🟩 : Switch using only spanning trees

▬ : Virtual link

(4) Compatibility with Multiple Spanning Tree

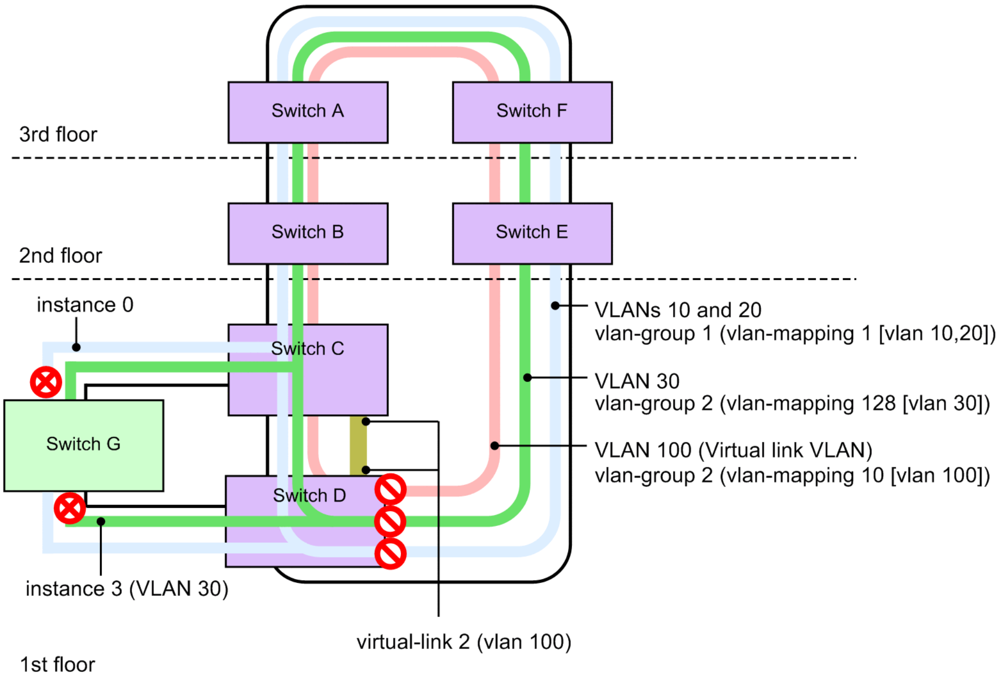
Multiple Spanning Tree can be used with all VLANs for data transfer for which the Ring Protocol is running.

For Multiple Spanning Tree, when the `axrp virtual-link` configuration command is used to set a virtual link, a topology based on the virtual link is built and usage with the Ring Protocol starts. When the `axrp virtual-link` configuration command is not used to set a virtual link, the intended topology cannot be built because virtual links cannot be built. As a result, loops might occur.

When the same VLAN is set for the VLAN belonging to the MST instance and the Ring Protocol VLAN mapping, it can be run together for both the MST instance and the Ring Protocol. If the set VLANs do not match, the unmatched VLAN is put in `Blocking` status.

The figure below shows a configuration in which Multiple Spanning Tree and the Ring Protocol are used together. In the figure, Multiple Spanning Tree is set for switches C, D, and G, and two VLAN groups for the Ring Protocol are set for switches A, B, C, D, E, and F. The topology is reflected to Multiple Spanning Tree with VLAN group 1 of the Ring Protocol as CIST and VLAN group 2 as MST instance 3. Also, because VLAN 100 is set as the virtual link VLAN for switches C and D, a virtual link is built between both switches.

Figure 25-7: Configuration using Multiple Spanning Tree and the Ring Protocol together


Switch A
Switch F
3rd floor
Switch B
Switch E
2nd floor
instance 0
Switch C
VLANs 10 and 20
vlan-group 1 (vlan-mapping 1 [vlan 10,20])
VLAN 30
vlan-group 2 (vlan-mapping 128 [vlan 30])
Switch G
VLAN 100 (Virtual link VLAN)
vlan-group 2 (vlan-mapping 10 [vlan 100])
Switch D
instance 3 (VLAN 30)
virtual-link 2 (vlan 100)
1st floor

Switches A, B, E, and F : Switches comprising a ring protocol using VLANs 10, 20, and 30

Switches C and D : Switches using a ring protocol using VLANs 10, 20, and 30 together with a multiple spanning tree
VLAN 100 is used as a virtual link VLAN.

Switch G : Switch using only a multiple spanning tree

Legend:

⊗ : Blocking by spanning tree

🚫 : Blocking by ring protocol

🟪 : Switch using the ring protocol and spanning trees together

🟩 : Switch using only spanning trees

▬ : Virtual link

(5) VLANs that cannot be run together

- VLANs with only the Ring Protocol applied

  When PVST+ is stopped by, for example, configuration settings, the VLAN only has the Ring Protocol applied.

  During Single Spanning Tree operation or Multiple Spanning Tree operation, VLANs for data transfer handled by the Ring Protocol must run together.

- VLANs that have only PVST+ applied

  When a VLAN mapping not belonging to a VLAN group is set for the Ring Protocol, the VLAN has only PVST+ applied.

- VLANs that have only Single Spanning Tree applied

  VLANs that do not belong to a VLAN group for the Ring Protocol have only Single Spanning Tree applied.

- VLANs that have only Multiple Spanning Tree applied

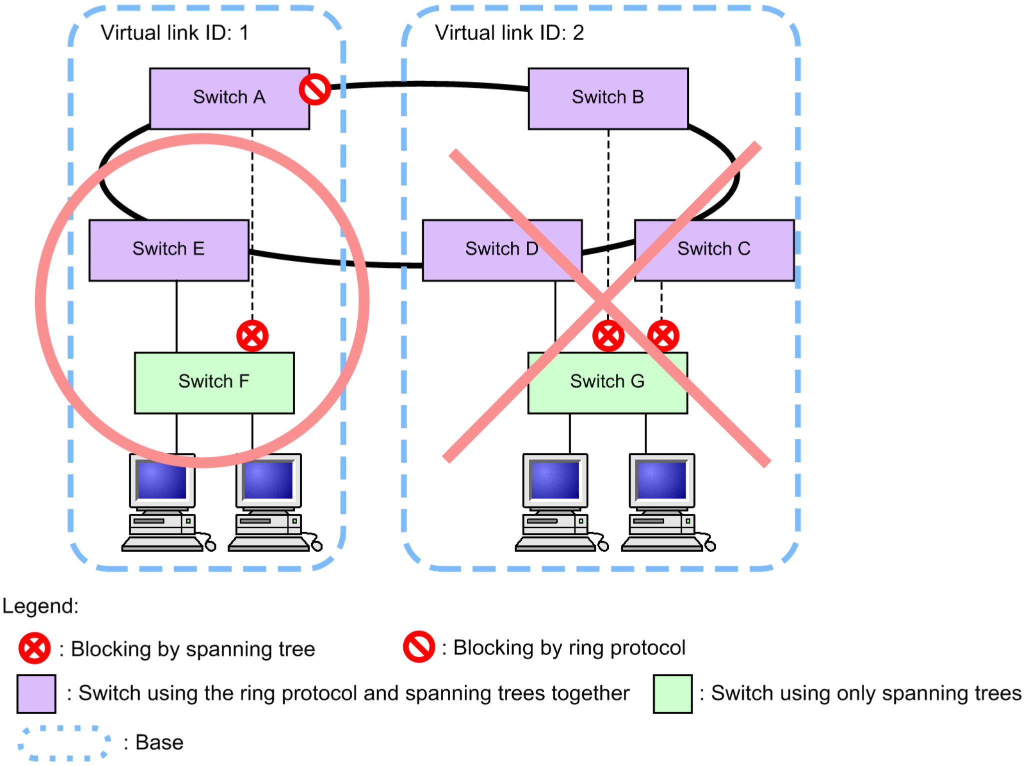
  VLANs that do not belong to a VLAN group for the Ring Protocol have only Multiple Spanning Tree applied.

25.1.4 Prohibited configurations

(1) Number of switches per base

Two Switches that use the Ring Protocol and a Spanning Tree Protocol together can be placed per base. A base cannot be configured with three or more switches. The following figure shows a prohibited configuration for virtual links.

Figure 25-8: Prohibited configuration for virtual links


Virtual link ID: 1
Virtual link ID: 2
Switch A
Switch B
Switch E
Switch D
Switch C
Switch F
Switch G
Legend:
: Blocking by spanning tree
: Blocking by ring protocol
: Switch using the ring protocol and spanning trees together
: Switch using only spanning trees
: Base

25.1.5 Notes on using of the Ring Protocol and Spanning Tree Protocols together

(1) Associations between virtual link VLANs and VLAN mappings

VLANs specified for virtual link VLANs must belong (be set in the VLAN mapping and VLAN group) to the VLAN for data transfer within a ring.

(2) Valid settings for virtual link VLANs

- Settings for ring networks

  For both single ring and multi-ring configurations (including multi-ring configurations with shared links) on ring networks comprising a virtual link, the virtual link VLAN needs to be set for the VLAN for data transfer. The setting must be specified for all nodes for which control frames might be sent or received between virtual links. If there are insufficient settings, virtual links cannot be used to send and receive control frames between base nodes, possibly causing faults to be mistakenly detected.

- Settings for Spanning Tree networks

  Because virtual link VLANs are used within ring networks, they cannot be used for downstream Spanning Tree Protocols. Therefore, loops might occur when a virtual link VLAN is set for a downstream port controlled by a Spanning Tree Protocol.

(3) Spanning Tree Protocols for which no virtual link VLAN is set

If no virtual link VLAN is set, the intended topology cannot be built because virtual links cannot be built. As a result, loops might occur.

(4) Stopping Spanning Tree Protocols by Ring Protocol settings

Under the initial Ring Protocol configuration settings, all running PVST+ instances and Multiple Spanning Tree are stopped. Note that loops might occur for VLANs for which PVST+ or Multiple Spanning Tree is stopped. Perform port blockage or other actions to prevent loop configurations.

(5) Building networks when the Ring Protocol and Spanning Tree Protocols are used together

The basic configuration of a network using the Ring Protocol and a Spanning Tree Protocol is a loop. Before building a Spanning Tree Protocol on an access network for an existing ring network, bring the configuration port (physical port or channel group) on the Spanning Tree network down, such as by setting the `shutdown` command.

(6) Fault monitoring times for the Ring Protocol and sending intervals for Spanning Tree BPDUs

Set the fault monitoring time for health check frames for the Ring Protocol (`health-check holdtime`) to a value less than the timeout detection time for Spanning Tree BPDUs (*hello-time* x 3 (in seconds)). If a greater value is set and a fault occurs in the ring network, the Spanning Tree Protocol detects a BPDU timeout before the Ring Protocol detects a fault, causing the topology to change, and possibly creating a loop.

(7) Dealing with program restart on transit nodes

When restarting the Ring Protocol program (`restart axrp` operation command), first put the configuration port on the Spanning Tree network (physical port or channel group) into the down state (for example, by setting `shutdown`). After restart, either wait for the reception hold time for flush control frames on the transit node (`forwarding-shift-time`) to time out, or after the Forwarding transition time for control VLANs (`forwarding-delay-time`) is used to perform path switching, clear the shutdown (for example) on the port put into the down state.

(8) Dealing with one-way link faults on ring networks

The Ring Protocol does not detect ring faults for one-way link faults. When a one-way link fault occurs on a ring network, because virtual link control frames can no longer be sent or received, the Spanning Tree Protocol might mistakenly detect a BPDU timeout. This might cause a loop that lasts until the one-way link fault is resolved.

When the Ring Protocol and the IEEE 802.3ah/UDLD functionality are used together, one-way link faults can be detected to prevent the occurrence of the loops that they cause.

(9) Procedures for restoring from multi-faults on environments used with Spanning Tree Protocols

When faults occur in multiple places in a ring network (multi-fault), virtual link control frames can no longer be sent and received, causing topology changes for the Spanning Tree Protocol. Multi-faults include when faults occur on both ring ports for a device using both the Ring Protocol and a Spanning Tree Protocol. In these cases, perform the following to restore all faults within a ring network:

1. Bring the configuration port of the Spanning Tree network (physical port or channel group) down such as by `shutdown`.
2. Restore the faults in the ring network, to have the master node detect ring fault restoration.
3. Clear `shutdown` for the configuration port of the Spanning Tree network to allow restoration.

(10) Compatibility between VLAN mappings for the Ring Protocol and VLANs belonging to MST instances of Multiple Spanning Tree

When a change in configuration causes the settings for VLAN mappings for the Ring Protocol and VLANs belonging to MST instances of Multiple Spanning Tree to no longer match, the unmatched VLANs might be put in `Blocking` status, preventing communication.

25.2 Using the Ring Protocol with GSRP

The Switch can use the Ring Protocol and GSRP together. For details about the Ring Protocol, see *23. Description of the Ring Protocol*.

25.2.1 Operational overview

For switches using the Ring Protocol and GSRP together, the VLAN mappings for the Ring Protocol and the VLAN information for GSRP VLAN groups need to match. The ring ports for the switches are not subject to GSRP control, and the data transfer status for the ring ports is controlled by the Ring Protocol.

Fault monitoring and path switching for when a fault occurs are performed independently by the Ring Protocol on ring networks and by GSRP on GSRP networks. However, switches that switch to the master during path switching on a GSRP network clear the MAC address table for GSRP switches and aware/unaware switches. At the same time, a flush control frame for the ring network is sent to clear the MAC address tables of switches configuring the ring network.

GSRP direct links use the same line as ring networks, but can also use another line.

The following figure shows an example of the Ring Protocol and GSRP being used together.

Figure 25-9: Example of the Ring Protocol and GSRP being used together (when direct links are used on a ring network)

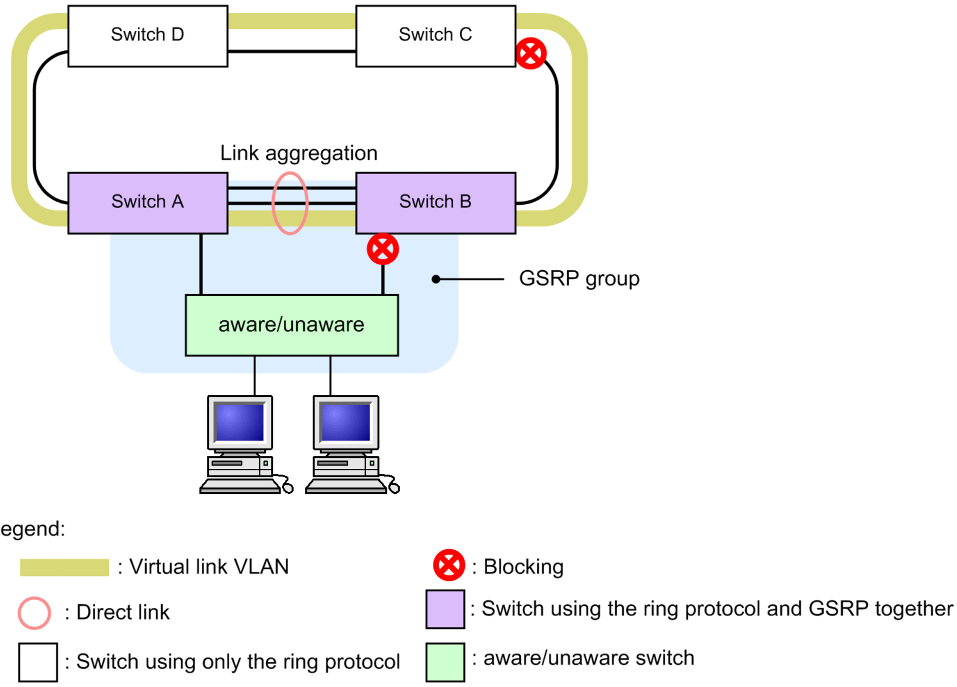
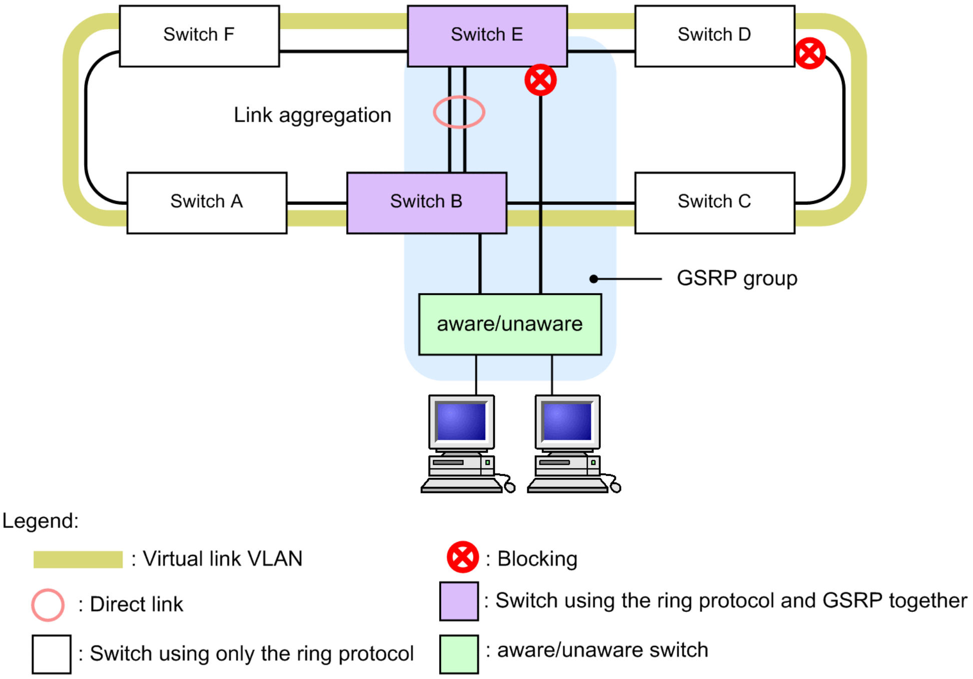


Figure 25-10: Example of the Ring Protocol and GSRP being used together (when direct links are not used on a ring network)



25.2.2 Conditions for combined usage

This section describes the conditions for using the Ring Protocol and GSRP together.

(1) VLAN setting conditions for running the Ring Protocol and GSRP together

Match all VLANs in VLAN mappings for the Ring Protocol and VLANs in GSRP VLAN groups.

(2) VLAN setting conditions for running the Ring Protocol and GSRP separately

There is no need to make all VLANs run together. When running each VLAN with a different protocol, make sure that there is no matching VLAN between those for Ring Protocol VLAN mapping and those for GSRP VLAN groups.

25.2.3 Handling ring ports

Ring ports are not subject to GSRP control, regardless of whether the `gsrp exception-port` configuration command is set. The data transfer status of a ring port is controlled only by the Ring Protocol.

Note that settings by the following configuration commands are ignored for ring ports:

- gsrp reset-flush-port (ports for which port resetting is used)
- gsrp no-flush-port (ports that do not send GSRP flush request frames)

25.2.4 Handling control VLANs for the Ring Protocol

When a Ring Protocol control VLAN is set for a GSRP VLAN group, the corresponding VLAN belongs outside the VLAN group. VLANs belonging outside of a VLAN group are not displayed by the `show gsrp` operation command.

25.2.5 Clearing MAC address tables during GSRP network switching

When the Ring Protocol and GSRP are used together and GSRP network path switching occurs, the MAC address tables of the devices configuring the ring network need to be cleared. If these MAC address tables are not cleared, communication might not be restored in a timely manner. The MAC address tables of the devices on the ring network can be cleared by using the virtual link

VLANs set on the ring network during the transition to the GSRP master to send flush control frames for the ring network. This virtual link VLAN must belong to the VLAN for data transfer group for the Ring Protocol.

When a flush control frame sent by the GSRP master is received by a device in the ring, its MAC address table is cleared. Note that the sending count follows that in the GSRP configuration (`flush-request-count`).

When the Ring Protocol and GSRP are run on different VLANs, each protocol is unaffected by any path switching occurring due to faults. Therefore, because the MAC address tables do not need to be cleared, virtual link VLANs do not need to be set.

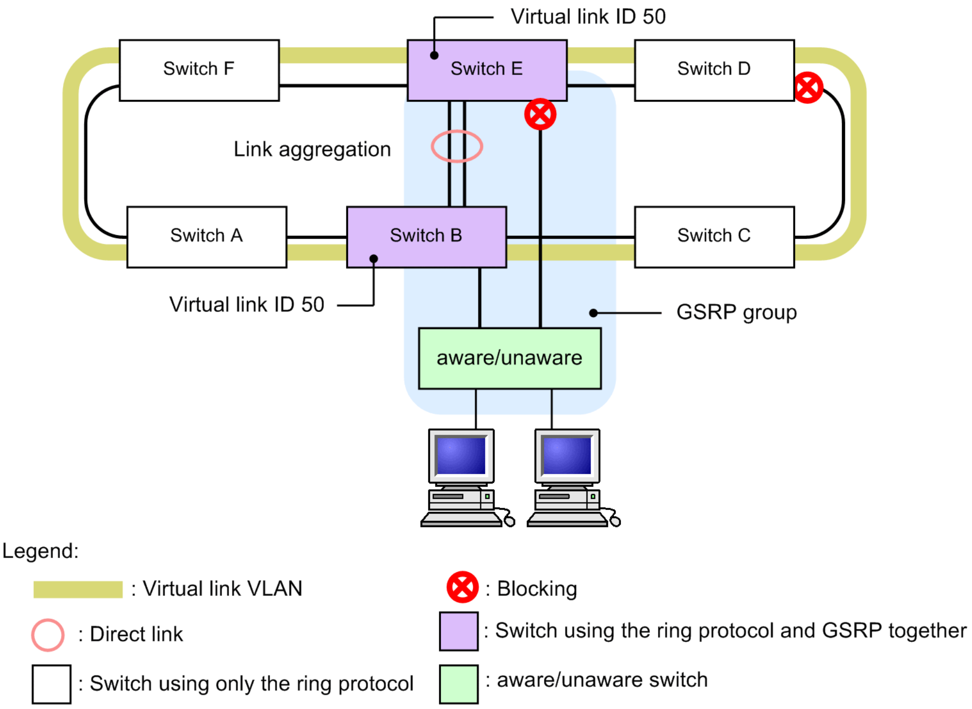
25.2.6 Notes on running the Ring Protocol and GSRP together

(1) Setting virtual link VLANs

When the Ring Protocol and GSRP are used together, a virtual link VLAN needs to be set to send flush control frames. This virtual link VLAN must belong to the VLAN for data transfer group for the Ring Protocol.

The figure below shows virtual link ID settings. The same virtual link ID needs to be set for the same GSRP group device. Also, a unique value needs to be set within the ring network in which the same virtual link VLAN is set. When virtual link ID 50 is set for Switches A, C, D, and F, which do not have the same GSRP group, MAC address tables can no longer be cleared by flush control frames for the corresponding devices.

Figure 25-11: Virtual link ID settings



(2) Changing Ring Protocol VLAN mappings or GSRP VLAN groups

When the Ring Protocol and GSRP are used together, all VLANs for Ring Protocol VLAN mappings and VLANs for GSRP VLAN groups need to match. If they no longer match due to a configuration change, VLANs affected by the changes might switch to `Blocking` status, preventing transmission for some VLANs.

Therefore, when the configuration is changed to use Ring Protocol and GSRP together, the `priority`, `backup-lock`, or other command needs to be set on the GSRP backup device to prevent switching to the master before the change is made.

(3) Number of VLANs that can be set per VLAN group

When 511 or more VLANs are made to belong to a VLAN group used with the Ring Protocol, ring ports might temporarily change to `Blocking` status when the corresponding VLAN group changes status.

Make sure that no more than 510 VLANs are made to belong to a VLAN group used with the Ring Protocol.

(4) GSRP VLAN group-only control functionality

When the Ring Protocol and GSRP are used together, the ports for VLANs not belonging to a VLAN group might be changed to `Blocking` status for the following situations, even if the GSRP VLAN group-only control functionality is set.

- The Ring Protocol is not running due, for example, to an incorrect Ring Protocol configuration

  The VLAN set for the control VLAN of the ring ID for which the Ring Protocol functionality is not running properly might be in the `Blocking` status. Note that the ring port is not in `Blocking` status.

- Ring Protocol functionality has been disabled by the `disable` command

  The VLAN set for the control VLAN of the ring ID for which the Ring Protocol functionality has been disabled might be in the `Blocking` status. Note that the ring port is not in `Blocking` status.

- The conditions for using the Ring Protocol and GSRP together as shown in *25.2.2 Conditions for combined usage* are not met.

  VLANs for which the conditions for using the Ring Protocol and GSRP together are not met might be in the `Blocking` status.

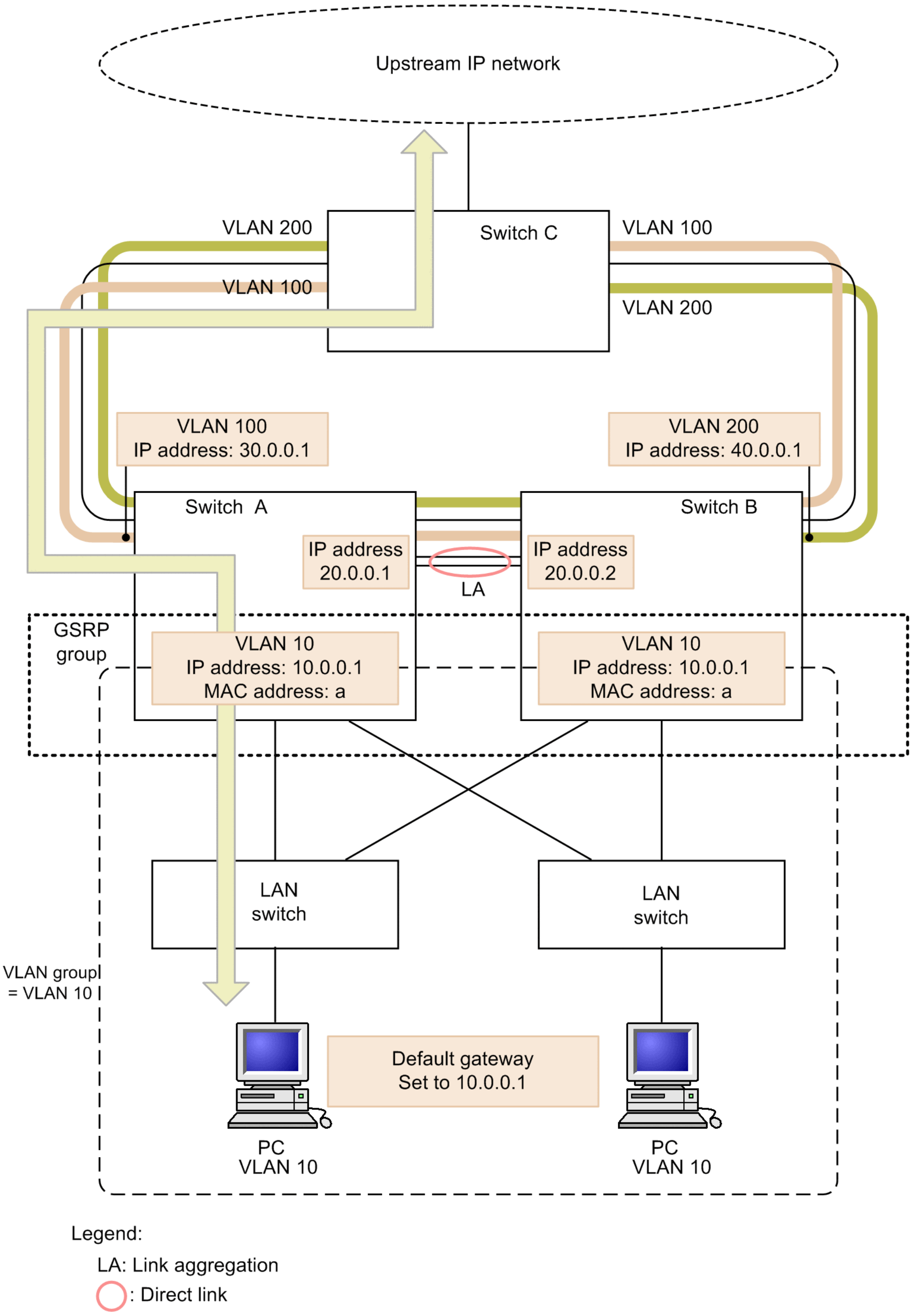
(5) Applying the Layer 3 redundancy switching functionality

When the Ring Protocol and GSRP are used together for the same data VLAN, the Layer 3 redundancy switching functionality cannot be applied. When connecting a GSRP network and ring network by applying such functionality, set each different data VLAN for the Ring Protocol and GSRP, and run them separately.

25.2.7 Overview of standalone operation (example using the Layer 3 redundancy switching functionality)

When the Ring Protocol and GSRP are run separately on different VLANs, the Layer 3 redundancy switching functionality is used to connect to the ring network. The figure below shows an example of this. Layer 3 forwarding is performed from the downstream network (such as a computer) over Switch A, so that communication is performed with the upstream network through the ring network for VLAN 100. When a fault occurs on Switch A, Layer 3 forwarding is performed by Switch B (when direct link failure detection functionality is set) for the downstream network and upstream network, and communication is performed through the ring network for VLAN 200.

Figure 25-12: Layer 3 redundancy switching functionality (during normal operation)

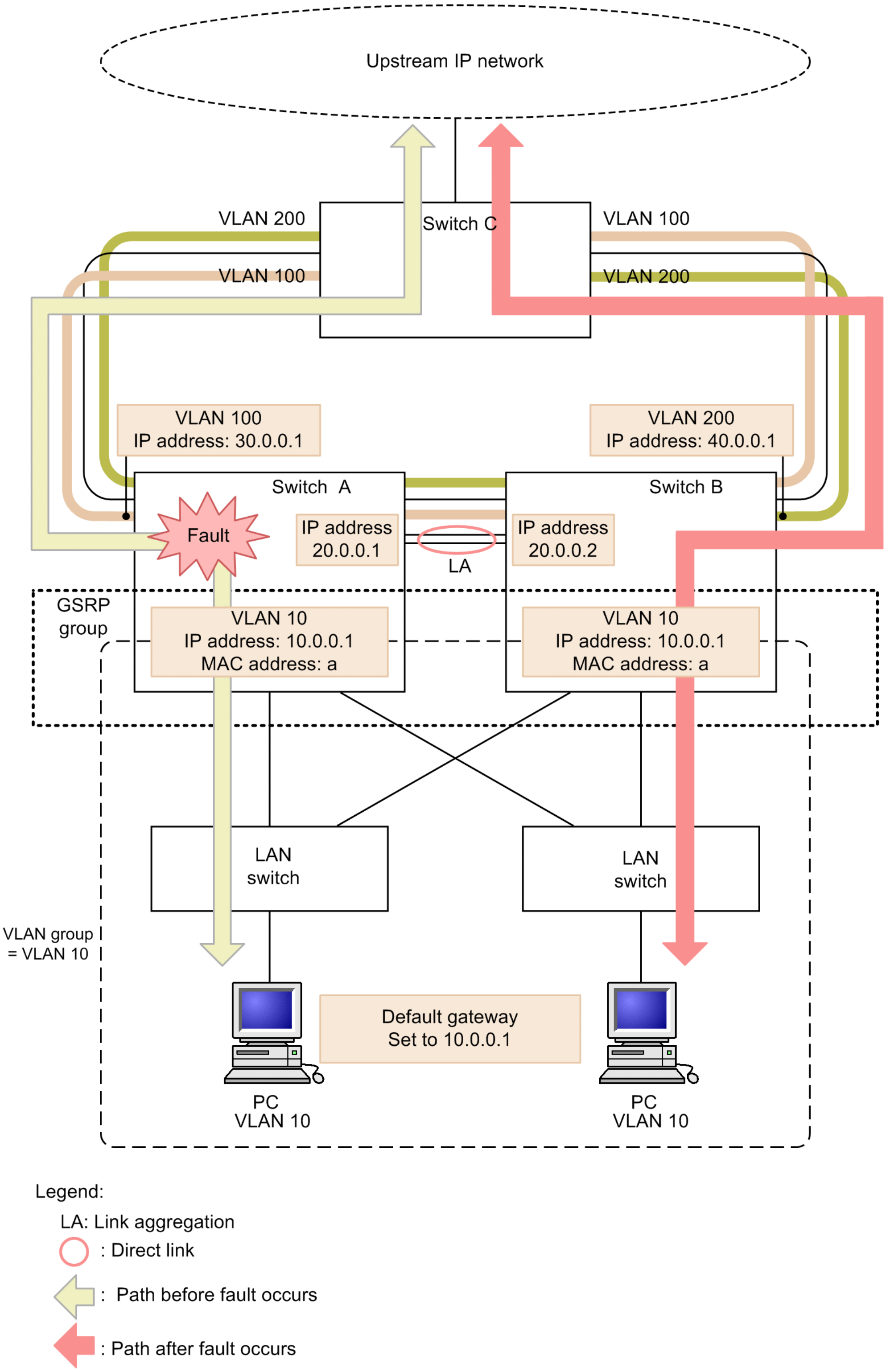


Legend:

LA: Link aggregation

○: Direct link

Figure 25-13: Layer 3 redundancy switching functionality (when a fault occurs)



25.3 Virtual link configuration

Virtual links can be set to use the Ring Protocol and Spanning Tree Protocol on the same device. Note that when the Ring Protocol and GSRP are used together, a virtual link VLAN needs to be set up to send flush frames.

25.3.1 List of configuration commands

The following table describes the configuration commands for virtual links.

Table 25-4: List of configuration commands

Command name	Description
axrp virtual-link	Sets a virtual link ID.

25.3.2 Configuring virtual links

Points to note

Set a virtual link ID and virtual link VLAN. Virtual links can be set so that the Ring Protocol can be used together with a Spanning Tree Protocol or GSRP. Make sure that you set the same virtual link ID and virtual link VLAN for partner devices within the same base, and that the used virtual link VLAN is selected from those used for data transfer.

Command examples

1. `(config)# axrp virtual-link 10 vlan 100`

   Sets the virtual link ID to 10, and the virtual link VLAN to 100.

25.3.3 Configuring the Ring Protocol and PVST+ together

Points to note

When the Ring Protocol and PVST+ are used together, the VLAN IDs to be used together need to be set in a VLAN mapping. In this case, only one VLAN ID is specified for the VLAN mapping. When a VLAN ID other than that for a VLAN used with PVST+ is set for the VLAN mapping, PVST+ will not run on the VLAN.

Command examples

1. `(config)# axrp vlan-mapping 1 vlan 10`

   Sets a VLAN mapping ID of 1, and sets VLAN ID 10 to be used with PVST+.

2. `(config)# axrp vlan-mapping 2 vlan 20,30`

   Sets a VLAN mapping ID of 2, and sets VLAN IDs 20 and 30 to be used for the Ring Protocol only.

3.
   ```
   (config)# axrp 1
   (config-axrp)# vlan-group 1 vlan-mapping 1-2
   ```

   Sets VLAN mapping IDs 1 and 2 for VLAN group 1.

25.3.4 Configuring the Ring Protocol and Multiple Spanning Tree together

Points to note

When the Ring Protocol and Multiple Spanning Tree are used together, the VLAN IDs to be used together need to be set in a VLAN mapping. In this case, the VLAN ID specified for the VLAN mapping and the VLAN ID specified for the VLAN belonging to the MST instance must match. If the VLAN mapping and VLAN ID for the VLAN belonging to the MST instance do not match, all ports for the VLAN that does not match will be in the `Blocking` status.

Command examples

1.
```
(config)# axrp vlan-mapping 1 vlan 10,20,30
```
Sets a VLAN mapping ID of 1, and sets VLAN IDs 10, 20, and 30 to be used together with MST instance 10.

2.
```
(config)# axrp vlan-mapping 2 vlan 40,50
```
Sets a VLAN mapping ID of 2, and sets VLAN IDs 40 and 50 to be used together with MST instance 20.

3.
```
(config)# axrp 1
(config-axrp)# vlan-group 1 vlan-mapping 1-2
(config-axrp)# exit
```
Sets VLAN mapping IDs 1 and 2 for VLAN group 1.

4.
```
(config)# spanning-tree mst configuration
(config-mst)# instance 10 vlans 10,20,30
```
Sets VLAN IDs 10, 20, and 30 specified for `vlan-mapping 1`, for the VLAN belonging to MST instance 10, and starts usage with the Ring Protocol.

5.
```
(config-mst)# instance 20 vlans 40,50
```
Sets VLAN IDs 40 and 50 specified for `vlan-mapping 2`, for the VLAN belonging to MST instance 20, and starts usage with the Ring Protocol.

25.3.5 Configuring the Ring Protocol and GSRP together

Points to note

When the Ring Protocol and GSRP are used together, the VLAN IDs to be used together need to be set for the VLAN mapping and GSRP VLAN group. The VLAN mapping ID and GSRP VLAN group ID do not need to match.

Command examples

1.
```
(config)# axrp vlan-mapping 1 vlan 10,15
```
Sets a VLAN mapping ID of 1, and sets VLAN IDs 10 and 15 to be used together with GSRP.

2.
```
(config)# axrp 1
```

```
(config-axrp)# vlan-group 1 vlan-mapping 1
(config-axrp)# exit
```

Sets VLAN mapping ID 1 for VLAN group 1.

3.
```
(config)# gsrp 1
(config-gsrp)# vlan-group 3 vlan 10,15
```

Sets VLANs ID 10 and 15 used together with the Ring Protocol for GSRP VLAN group 3.

25.4 Virtual link operation

25.4.1 List of operation commands

The following table describes the operation commands for virtual links.

Table 25-5: List of operation commands

Command name	Description
show spanning-tree	Shows the application status of virtual links in a Spanning Tree Protocol.
show gsrp	Shows the application of virtual links in GSRP.

25.4.2 Checking the status of virtual links

Use the `show spanning-tree` command to check virtual link information. Check `Port Information` to confirm the existence of virtual link ports.

The following figure shows the result of executing the `show spanning-tree` command.

Figure 25-14: Results of executing the show spanning-tree command

```
> show spanning-tree vlan 2
Date 20XX/11/04 11:39:43 UTC
VLAN 2              PVST+ Spanning Tree:Enabled  Mode:PVST+
  Bridge ID        Priority:4096      MAC Address:0012.e205.0900
    Bridge Status:Designated
  Root Bridge ID   Priority:0         MAC Address:0012.e201.0900
    Root Cost:0
    Root Port:0/2-3(VL:10)                            ... 1
  Port Information
    0/1     Up     Status:Forwarding  Role:Designated
    VL(10)  Up     Status:Forwarding  Role:Root       ... 1
>
```

1. `VL` indicates a virtual link ID.

The `show gsrp detail` command can be used to check whether a virtual link is running. Check `Virtual Link ID` for the virtual link ID and virtual link VLAN.

Figure 25-15: Results of executing the show gsrp detail command

```
>show gsrp detail
Date 20XX/04/10 12:00:00 UTC

GSRP ID: 3
 Local MAC Address       : 0012.e2a8.2527
 Neighbor MAC Address    : 0012.e2a8.2505
 Total VLAN Group Counts : 3
 GSRP VLAN ID            : 105
 Direct Port             : 0/10-11
 GSRP Exception Port     : 0/1-5
 No Neighbor To Master   : manual
 Backup Lock             : disable
 Port Up Delay           : 0
 Last Flush Receive Time : -
 Layer 3 Redundancy      : On
 Virtual Link ID         : 100(VLAN ID : 20)

                         Local               Neighbor
 Advertise Hold Time     : 5                   5
 Advertise Hold Timer    : 4                   -
 Advertise Interval      : 1                   1
 Selection Pattern       : ports-priority-mac  ports-priority-mac
 VLAN Group ID      Local State         Neighbor State
 1                  Backup              Master
 2                  (disable)           -
 8                  Master              -
>
```

Chapter

26. Description of IGMP Snooping and MLD Snooping

IGMP snooping and MLD snooping are functionality that control multicast traffic within a VLAN for Layer 2 switching. This chapter explains IGMP snooping and MLD snooping.

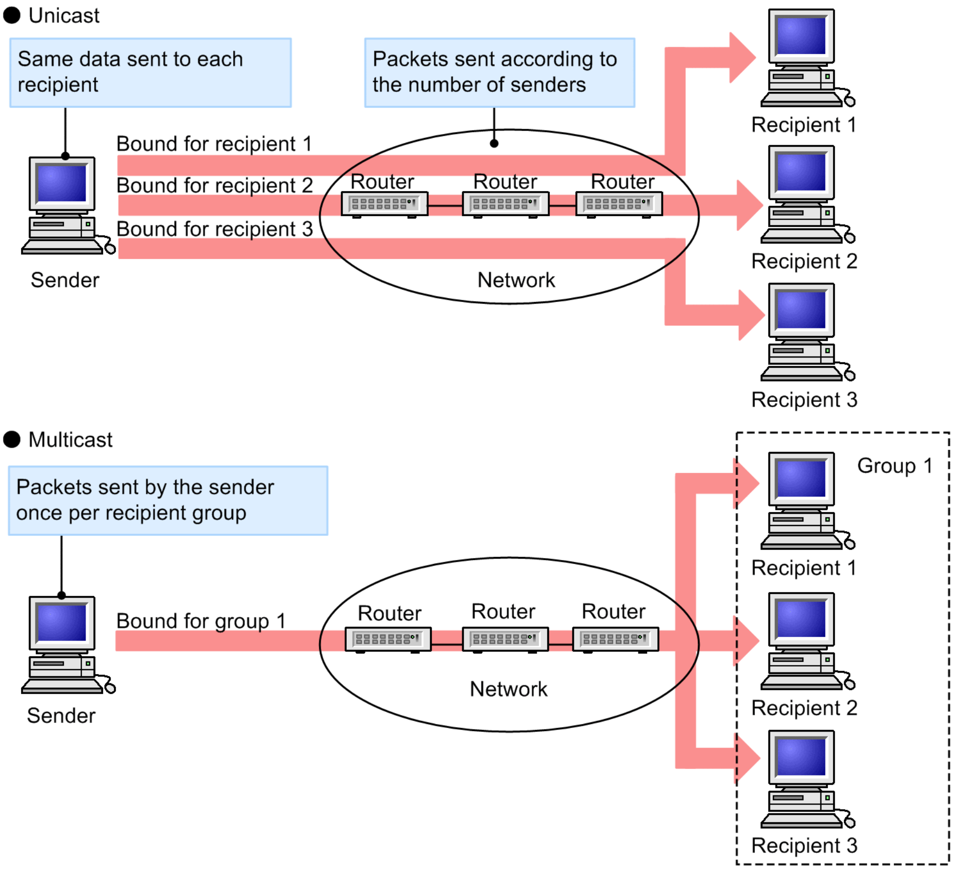
26.1 Overview of IGMP snooping and MLD snooping

This section gives an overview of multicast, IGMP snooping, and MLD snooping.

26.1.1 Overview of multicast

When the same information is sent by unicast to multiple recipients, the load increases for both the sender and the network because the sender replicates and sends data for each recipient. With multicast, on the other hand, the sender sends data to a selected group within the network. Because the sender does not need to replicate data for each recipient, network load can be reduced regardless of the number of recipients. The following figure gives an overview of multicast.

Figure 26-1: Overview of multicast



When multicast is used for transmission, a multicast group address is used for the destination address. The following table describes multicast group addresses.

Table 26-1: Multicast group address

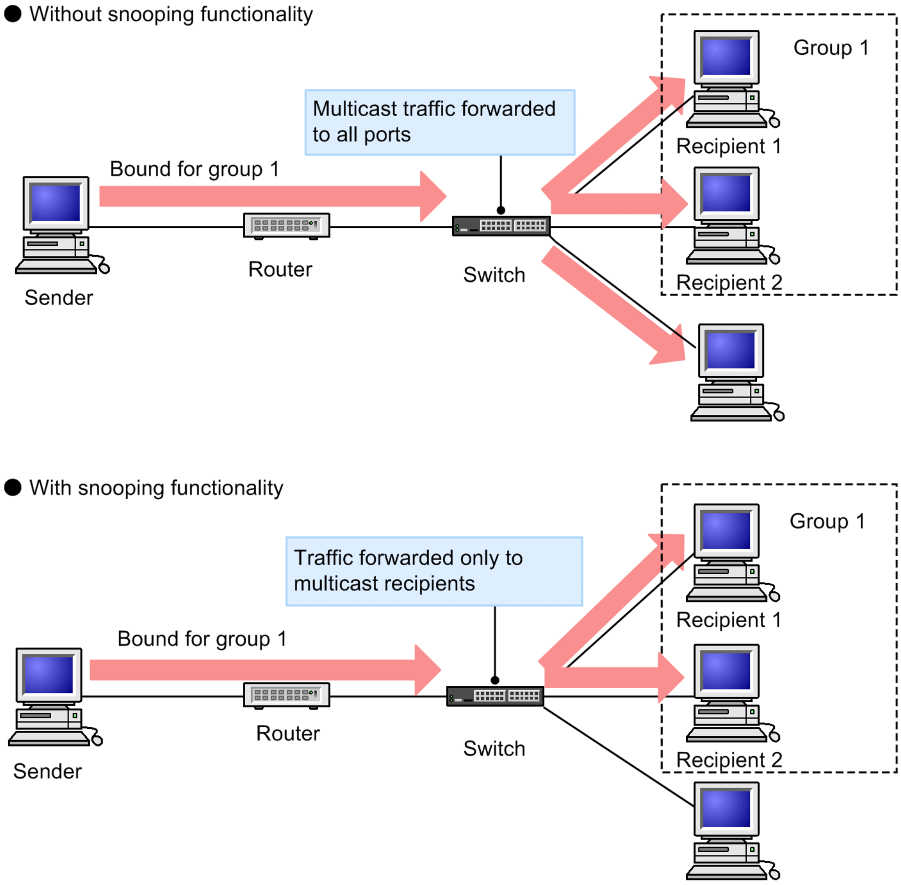
Protocol	Address range
IPv4	224.0.0.0-239.255.255.255
IPv6	IPv6 addresses whose highest 8 bits are `ff` (in hexadecimal)

26.1.2 Overview of IGMP snooping and MLD snooping

Layer 2 switches forward multicast traffic to all ports within a VLAN. Therefore, when multicast is used on a network to which a Layer 2 switch is connected, unnecessary multicast traffic might be sent to ports that have no multicast traffic recipients.

IGMP snooping and MLD snooping monitor IGMP or MLD messages and forward multicast traffic to ports to which recipients are connected. This functionality can be used to suppress the forwarding of unnecessary multicast traffic for more efficient use of networks. The following figure gives an overview of IGMP snooping and MLD snooping.

Figure 26-2: Overview of IGMP snooping and MLD snooping


● Without snooping functionality
Multicast traffic forwarded to all ports
Bound for group 1
Group 1
Recipient 1
Recipient 2
Sender
Router
Switch
● With snooping functionality
Traffic forwarded only to multicast recipients
Bound for group 1
Group 1
Recipient 1
Recipient 2
Sender
Router
Switch

To detect ports to which multicast traffic recipients are connected, the Switch monitors group management protocol packets. The group management protocol sends and receives group membership information between router hosts by using IGMP on IPv4 networks and MLD on IPv6 networks. The protocol detects packets sent from the host, indicating group participation and leave, to learn the connected ports to which multicast traffic should be forwarded.

26.2 Functionality supported for IGMP snooping and MLD snooping

The following table describes the IGMP snooping and MLD snooping functionality supported by the Switch.

Table 26-2: Supported functionality

Item		Support	Remarks
Interface type		Full Ethernet support Only Ethernet V2 frame formats	--
Supported IGMP version Supported MLD version		IGMP: Version 1, 2, and 3 MLD: Version 1, and 2	--
Learning for this functionality MAC address range[#1]	IPv4	0100.5e00.0000 to 0100.5e7f.ffff	For details, see RFC 1112.
	IPv6	3333.0000.0000 to 3333.ffff.ffff	For details, see RFC 2464.
Learning for this functionality IP address range[#2]	IPv4	224.0.0.0-239.255.255.255	--
	IPv6	IPv6 addresses whose highest 8 bits are `ff` (in hexadecimal)	--
IGMP querier MLD querier		Querier operation is performed according to the IGMPv2 or IGMPv3 and MLDv1 or MLDv2 specifications	--
Settings for multicast router connection ports		Static settings by configuration	--
IGMP instant leave		Instant leave due to IGMPv2 Leave messages, or IGMPv3 Report (leave request) messages for which the multicast address record type is CHANGE_TO_INCLUDE_MODE	--

Legend: --: Not applicable

#1: When not used with IPv4 or IPv6 multicast

#2: When used with IPv4 or IPv6 multicast

26.3 IGMP snooping

The following explains IGMP snooping functionality and its operation. The format and timers for IGMP messages sent and received by the Switch conform to RFC 2236. Also, the format and values set for IGMP version 3 (abbreviated hereafter to IGMPv3) messages conform to RFC 3376.

If IGMP snooping is not used at the same time as IPv4 multicast or IPv6 multicast, the MAC address control method is used to control forwarding for multicast traffic. If IGMP snooping is used at the same time as IPv4 multicast or IPv6 multicast, the IP address control method is used to control forwarding for multicast traffic.

26.3.1 MAC address control method

(1) MAC address learning

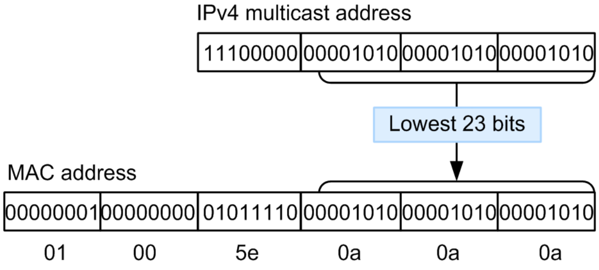
For VLANs for which IGMP snooping is set, multicast MAC addresses are dynamically learned when IGMP messages are received. The learned multicast MAC addresses are registered to the MAC address table.

(a) Registering entries

When an IGMPv1 or IGMPv2 Report message or IGMPv3 Report (membership request) message is received, the multicast MAC address is learned from the multicast group address included in the message, and an entry is created that forwards traffic bound for a multicast group only to ports for which IGMPv1, IGMPv2, or IGMPv3 Report messages have been received.

Destination MAC addresses for IPv4 multicast data are generated by copying the lowest 23 bits of the IP address to the MAC address. Therefore, MAC addresses will be redundant for IP addresses for which the lower 23 bits are the same. For example, the multicast MAC address for both 224.10.10.10 and 225.10.10.10 is 0100.5E0A.0A0A. These addresses are treated as packets bound for the same MAC address by Layer 2 forwarding. The following figure shows the correspondence between IPv4 multicast addresses and MAC addresses.

Figure 26-3: Correspondence between IPv4 multicast addresses and MAC addresses



(b) Deleting entries

Learned multicast MAC addresses are deleted in any of the following cases when group members no longer exist on all ports:

- An IGMPv2 Leave message is received.

  Group-Specific Query messages are sent from the Switch to the port that received IGMPv2 Leave messages, twice every second (Group-Specific Query messages are only sent when a querier is set and are sent from a representative querier otherwise). If there is no response, only that port is deleted from the entries (forwarding of multicast traffic to this port is suppressed). If no group members are left in all ports in the VLAN, the entry itself is deleted.

  When IGMP instant leave is used and an IGMPv2 Leave message is received, the corresponding port is instantly deleted from the entries. Even when a querier is set, Group-Specific Query messages are not sent.

- An IGMPv3 Report (leave request) message is received.

  Group-Specific Query messages are sent from the Switch to the port that received IGMPv3 Report (leave request) messages, twice every second (Group-Specific Query messages are only sent when a querier is set and are sent from a representative querier otherwise). If there is no response, only that port is deleted from the entries (forwarding of multicast traffic to this port is suppressed). If no group members are left in all ports in the VLAN, the entry itself is deleted. However, when an IGMPv3 Report message whose multicast address record type is BLOCK_OLD_SOURCES is received, Group-Specific Query messages are sent, and entry deletion processing is performed only when a querier has been set for the local device.

  When IGMP instant leave is used, and an IGMPv3 Report (leave request) message whose multicast address record type is CHANGE_TO_INCLUDE_MODE is received, the corresponding port is immediately deleted from the entries. Even when a querier is set, Group-Specific Query messages are not sent.

- A set time elapses after an IGMPv1, IGMPv2, or IGMPv3 Report (membership request) message is received.

  Multicast routers regularly send Query messages to check that group members exist in directly connected interfaces. When the Switch receives an IGMP Query message from a router, it forwards it to all ports in the VLAN. If there is no response to the IGMP Query message, only that port is deleted from the entries. When no response is received from any port, the entry itself is deleted.

  If the Switch does not receive an IGMPv1, IGMPv2, or IGMPv3 Report (membership request) message within 260 seconds, it deletes the corresponding entries.

  When another device is the representative querier for a VLAN running with IGMPv3, the timeout time is calculated from IGMPv3 Query messages (QQIC field) from the representative querier. If the local device is the representative querier, or is running with IGMPv2, the time is 125 seconds. In this case, 125 seconds is used for the Query Interval on the corresponding VLAN.

  Note:

  > The timeout time is calculated as follows: *query-interval* (value of the QQIC field) x 2 + *query-response-interval*.

(2) Layer 2 forwarding for IPv4 multicast packet

Layer 2 forwarding within VLANs receiving IPv4 multicast packets is performed based on MAC address. Layer 2 forwarding based on IGMP snooping results is performed for all ports that receive IGMP Report (membership request) messages whose IP multicast address is mapped to the same MAC address.

Because the multicast MAC address for both 224.10.10.10 and 225.10.10.10 as shown in the example for *(a)Registering entries* in *(1) MAC address learning* is 0100.5E0A.0A0A, when Layer 2 forwarding is performed for multicast data bound for 224.10.10.10, it is also forwarded to ports receiving IGMP Report (membership request) messages bound for 225.10.10.10.

26.3.2 IP address control method

The `swrt_multicast_table` command can be set on the Switch to use both IPv4 multicast and IGMP snooping at the same time on the same VLAN. When using IPv4 multicast and IGMP snooping at the same time, make sure that you use IPv4 multicasts on the corresponding VLAN.

(1) IP address learning

Multicast IP addresses are learned dynamically when IGMP messages are received on VLANs for which IGMP snooping is set. Information about learned multicast IP addresses is set in multicast forwarding entries for IPv4 multicast.

(a) Registering entries

When an IGMPv1or IGMPv2 Report message or IGMPv3 Report (membership request) message is received, the multicast IP address is learned from the multicast group address included in the message, and an entry is created that forwards traffic bound for the multicast group only to ports for which IGMPv1, IGMPv2, or IGMPv3 Report messages were received.

(b) Deleting entries

Learned multicast IP addresses are deleted in any of the following cases when group members no longer exist on all ports:

- An IGMPv2 Leave message is received.

  Group-Specific Query messages are sent from the Switch to the port that received IGMPv2 Leave messages, twice every second (Group-Specific Query messages are only sent when the Switch is the representative querier). If there is no response, only that port is deleted from the entries (forwarding of multicast traffic to this port is suppressed). If no group members are left in all ports in the VLAN, the entry itself is deleted.

  When IGMP instant leave is used and an IGMPv2 Leave message is received, the corresponding port is instantly deleted from the entries.

- An IGMPv3 Report (leave request) message is received.

  When an IGMPv3 Report (leave request) message whose multicast address record type is CHANGE_TO_INCLUDE_MODE is received, Group-Specific Query messages are sent from the Switch to the port that received the message, twice every second (Group-Specific Query messages are only sent when the Switch is the representative querier). If there is no response, only that port is deleted from the entries (forwarding of multicast traffic to this port is suppressed). If no group members are left in all ports in the VLAN, the entry itself is deleted. When an IGMPv3 Report message whose multicast address record type is BLOCK_OLD_SOURCES is received, Group-and-Source-Specific Query messages are sent from the Switch, twice every second (Group-and-Source-Specific Query messages are only sent when the Switch is the representative querier). Entries are deleted on timeout regardless of the response to Group-Source-and-Specific Query messages.

  When IGMP instant leave is used, and an IGMPv3 Report (leave request) message whose multicast address record type is CHANGE_TO_INCLUDE_MODE is received, the corresponding port is immediately deleted from the entries.

  Note:

  > The timeout time is calculated as follows: *query-interval* (value of the QQIC field) x 2 + *query-response-interval*.

- A set time elapses after an IGMPv1, IGMPv2, or IGMPv3 Report (membership request) message is received.

  Multicast routers regularly send Query messages to check that group members exist in directly connected interfaces. When the Switch receives an IGMP Query message from a router, it forwards it to all ports in the VLAN. If there is no response to the IGMP Query message, only that port is deleted from the entries. When no response is received from any port, the entry itself is deleted.

  The timeout time for deleting entries is 260 seconds (default value) for the Switch. If the switch does not receive an IGMPv1, IGMPv2, or IGMPv3 Report (membership request) message within 260 seconds, it deletes the corresponding entries.

  When another device is the representative querier for a VLAN running with IGMPv3, the timeout time is calculated from IGMPv3 Query messages (QQIC field) from the representative querier. If the local device is the representative querier, or is running with IGMPv2, the default value is used. In this case, 125 seconds is used for the Query Interval on the corresponding VLAN.

Note:

The timeout time is calculated as follows: *query-interval* (value of the QQIC field) x 2 + *query-response-interval*.

(2) Layer 2 forwarding for IPv4 multicast packet

Layer 2 forwarding within VLANs receiving IPv4 multicast packets is performed based on IP address. Layer 2 forwarding based on IGMP snooping results is performed for all ports that receive IGMP Report (membership request) messages.

(3) Layer 3 forwarding for IPv4 multicast packet

When Layer 3 forwarding based on IPv4 multicast is performed between VLANs, and IGMP snooping is running on the forwarding destination VLAN, multicast traffic for which Layer 3 forwarding is performed is forwarded according to the learning results for IGMP snooping within the forwarding destination VLAN.

(4) Specific query transmission during concurrent usage of IPv4 multicast

IPv4 multicast can be run so that when the Switch is the representative querier in the VLAN, Group-Specific Queries or Group-and-Source-Specific Queries sent due to IGMP Leave message or IGMPv3 Report (leave request) message reception are sent to all ports in the VLAN and not just the recipient port.

26.3.3 Connections with multicast routers

In addition to the hosts that have already joined a group, the forwarding destinations for multicast packets also include neighboring multicast routers. When the Switch and a multicast router are connected and IGMP snooping is used, the port connected to the multicast router to forward multicast packets to the router (abbreviated hereafter to multicast router port) can be specified by configuration.

The Switch forwards all multicast packets to the specified multicast router port.

Also, because IGMP is a protocol for sending and reception between router hosts, IGMP messages are accepted by routers and hosts. The Switch forwards IGMP messages as shown in the following table.

Table 26-3: Operation for each IGMPv1 or IGMPv2 message

IGMP message type	Transfer port within the VLAN	Remarks
Membership Query	Forwarded to all ports.	
Version 2 Membership Report	Forwarded only to multicast router ports.	
Leave Group	Not forwarded to any port when group members still exist for other ports. Forwarded to multicast router ports when no group members exist for other ports.	#
Version 1 Membership Report	Forwarded only to multicast router ports.	

#

This is the forwarding operation when a querier is set for the local device. If no querier has been set, forwarding is always performed to multicast router ports. However, if a port that has not received an IGMPv1, IGMPv2, or IGMPv3 Report (membership request) message receives an IGMPv2 Leave message, the IGMPv2 Leave message is not forwarded regardless of the querier settings.

Table 26-4: Operation for each IGMPv3 message

IGMPv3 message type		Transfer port within the VLAN	Remarks
Version3 Membership Query		Forwarded to all ports.	
Version 3 Membership Report	Membership Request Report	Forwarded only to multicast router ports.	
	Leave Request Report	Not forwarded to any port when group members still exist for other ports. Forwarded to multicast router ports when no group members exist for other ports.	#

#

This is the forwarding operation when a querier is set for the local device. If no querier has been set, forwarding is always performed to multicast router ports. However, if a port that has not received an IGMPv1, IGMPv2, or IGMPv3 Report (membership request) message receives an IGMPv3 Report (leave request) message, the IGMPv3 Report (leave request) message is not forwarded regardless of the querier settings.

26.3.4 IGMP querier functionality

The IGMP querier functionality is used by the Switch to send IGMP Query messages by proxy to recipient hosts on environments where no multicast router exists in the VLAN, and only hosts that send and receive multicast packets exist. Multicast routers regularly send IGMP Query messages and then check for reception from hosts to determine whether group members exist. If no multicast router exists, group members can no longer be monitored because no response is received from recipient hosts. This functionality enables the IGMP snooping functionality even when no multicast routers exist in the VLAN. The Switch sends an IGMP Query message every 125 seconds.

In order to use the IGMP querier functionality, an IP address must be set for VLANs using the IGMP snooping functionality.

When devices sending IGMP Query messages exist in a VLAN, the IGMP Query message transmission source with the lowest IP address becomes the representative querier, and it sends IGMP Query messages. If another device in the VLAN is the representative querier, the Switch stops using the IGMP querier functionality to send Query messages.

If the representative querier stops, such as due to a malfunction, a new representative querier is chosen. When the Switch is determined to be the representative querier, such as due to a malfunction on another device in the VLAN, IGMP Query message transmission is started. The monitoring time for representative queriers on the Switch is 255 seconds.

By default, the version for IGMP Queries sent by the Switch is IGMPv2. After the Switch is running, the IGMP Query version follows the IGMP version of the representative querier.

26.3.5 IGMP instant leave

IGMP instant leave stops multicast communication to the corresponding ports as soon as an IGMPv2 Leave or IGMPv3 Report (leave request) message is received.

For IGMPv3 Report (leave request) messages, only those whose multicast address record type is CHANGE_TO_INCLUDE_MODE are supported by this functionality.

26.4 MLD snooping

The following explains MLD snooping functionality and its operation. The format and established values for MLD messages sent and received by the Switch conform to RFC 2710. Also, the format and set values for MLD version 2 (abbreviated hereafter to MLDv2) messages conform to RFC 3810.

If MLD snooping is not used at the same time as IPv6 multicast, the MAC address control method is used to control forwarding for multicast traffic. If MLD snooping is used at the same time as IPv6 multicast, the IP address control method is used to control forwarding for multicast traffic.

26.4.1 MAC address control method

(1) MAC address learning

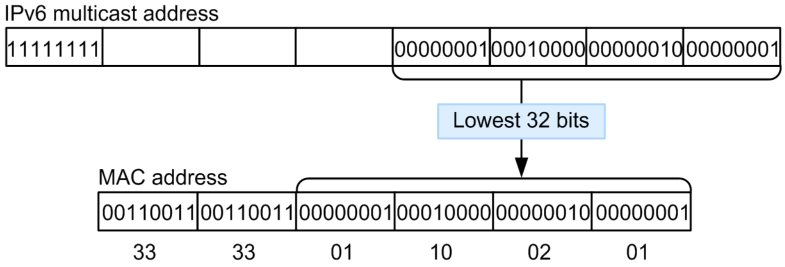
For VLANs for which MLD snooping is set, multicast MAC addresses are dynamically learned when MLD messages are received. The learned multicast MAC addresses are registered to the MAC address table.

(a) Registering entries

When an MLDv1 Report message and or MLDv2 Report (membership request) message is received, the multicast MAC address is learned from the multicast group address included in the message, and an entry is created that forwards traffic bound for a multicast group only to ports for which MLDv1 or MLDv2 Report messages have been received. Destination MAC addresses for IPv6 multicast data are generated by copying the lowest 32 bits of the IP address to the MAC address.

IPv6 multicast addresses have two types of formats for group ID fields that identify multicast groups: a 112-bit format and a 32-bit format. When group ID fields use the 112-bit address format, duplicate MAC addresses occur the same as for IPv4 multicast addresses. The following figure shows the correspondence between IPv6 multicast addresses and MAC addresses.

Figure 26-4: Correspondence between IPv6 multicast addresses and MAC addresses



(b) Deleting entries

Learned multicast MAC addresses are deleted in any of the following cases when group members no longer exist on all ports:

- An MLDv1 Done message is received.

  Group-Specific Query messages are sent from the Switch to the port that received MLDv1 Done messages, twice every second (Group-Specific Query messages are only sent when a querier is set and are sent from a representative querier otherwise). If there is no response, only that port is deleted from the entries (forwarding of multicast traffic to this port is suppressed). If no group members are left in all ports in the VLAN, the entry itself is deleted.

- An MLDv2 Report (leave request) message is received.

  Group-Specific Query messages are sent from the Switch to the port that received MLDv2 Report (leave request) messages, twice every second (Group-Specific Query messages are only sent when a querier is set and are sent from a representative querier otherwise). If there is no response, only that port is deleted from the entries (forwarding of multicast traffic to this port is suppressed). If no group members are left in all ports in the VLAN, the entry itself is deleted. However, when an MLDv2 Report message whose multicast address record type is BLOCK_OLD_SOURCES is received, Group-Specific Query messages are sent and entry deletion processing is performed only when a querier has been set for the local device.

- A set time elapses after an MLDv1 or MLDv2 Report (membership request) message is received.

  Multicast routers regularly send MLD Query messages to check that group members exist in directly connected interfaces. When the Switch receives an MLD Query message from a router, it forwards it to all ports in the VLAN. If there is no response to the MLD Query message, only that port is deleted from the entries. When no response is received from any port, the entry itself is deleted.

  If the Switch does not receive an MLDv1 or MLDv2 Report (membership request) message within 260 seconds, it deletes the corresponding entries.

  The timeout time for deleting entries is 260 seconds (default value) for the Switch. If the switch does not receive an MLDv1 or MLDv2 Report (membership request) message within 260 seconds, it deletes the corresponding entries.

  When another device is the representative querier for a VLAN running with MLDv2, the timeout time is calculated from MLDv2 Query messages (QQIC field) from the representative querier. If the local device is the representative querier, or is running with MLDv1, the default value is used. In this case, 125 seconds is used for the Query Interval on the corresponding VLAN.

  Note:

  > The timeout time is calculated as follows: *query-interval* (value of the QQIC field) x 2 + *query-response-interval*.

(2) Layer 2 forwarding for IPv6 multicast packets

Layer 2 forwarding within VLANs receiving IPv6 multicast packets is performed based on MAC address, just as for IPv4 multicast packets. Layer 2 forwarding based on MLD snooping results is performed for all ports that receive MLD Report (membership request) messages whose IPv6 multicast address is mapped to the same MAC address.

26.4.2 IP address control method

The `swrt_multicast_table` command can be set on the Switch to use both IPv6 multicast and MLD snooping at the same time on the same VLAN. When using IPv6 multicast and MLD snooping at the same time, make sure that you use IPv6 multicasts on the corresponding VLAN.

(1) IP address learning

Multicast IP addresses are learned dynamically when MLD messages are received on VLANs for which MLD snooping is set. Information about learned multicast IP addresses is set in multicast forwarding entries for IPv6 multicast.

(a) Registering entries

When an MLDv1 Report message or MLDv2 Report (membership request) message is received, the multicast IP address is learned from the multicast group address included in the message, and an entry is created that forwards traffic bound for the multicast group only to ports for which MLDv1 or MLDv2 Report messages were received.

(b) Deleting entries

Learned multicast IP addresses are deleted in any of the following cases when group members no longer exist on all ports:

- An MLDv1 Done message is received.

  Group-Specific Query messages are sent from the Switch to the port that received MLDv1 Done messages, twice every second (Group-Specific Query messages are only sent when the Switch is the representative querier). If there is no response, only that port is deleted from the entries (forwarding of multicast traffic to this port is suppressed). If no group members are left in all ports in the VLAN, the entry itself is deleted.

- An MLDv2 Report (leave request) message is received.

  When an MLDv2 Report (leave request) message whose multicast address record type is CHANGE_TO_INCLUDE_MODE is received, Group-Specific Query messages are sent from the Switch to the port that received the message, twice every second (Group-Specific Query messages are only sent when the Switch is the representative querier). If there is no response, only that port is deleted from the entries. If no group members are left in all ports in the VLAN, the entry itself is deleted. When an MLDv2 Report message whose multicast address record type is BLOCK_OLD_SOURCES is received, Group-and-Source-Specific Query messages are sent from the Switch, twice every second (Group-and-Source-Specific Query messages are only sent when the Switch is the representative querier). Entries are deleted on timeout regardless of the response to Group-Source-and-Specific Query messages.

  Note:

  > The timeout time is calculated as follows: *query-interval* (value of the QQIC field) x 2 + *query-response-interval*.

- A set time elapses after an MLDv1 or MLDv2 Report (membership request) message is received.

  Multicast routers regularly send MLD Query messages to check that group members exist in directly connected interfaces. When the Switch receives an MLD Query message from a router, it forwards it to all ports in the VLAN. If there is no response to the MLD Query message, only that port is deleted from the entries. When no response is received from any port, the entry itself is deleted.

  The timeout time for deleting entries is 260 seconds (default value) for the Switch. If the switch does not receive an MLDv1 or MLDv2 Report (membership request) message within 260 seconds, it deletes the corresponding entries.

  The timeout time is set dynamically as follows:

  - When another device is the representative querier (for MLDv2 operation)

    The timeout time is calculated from MLDv2 Query messages (QQIC field) from the representative querier.

  - When the local device is the representative querier

    The timeout time is calculated from Query Interval set for the local device regardless of MLDv1 or MLDv2 (with the default value used if no Query Interval is set).

  - When another device is the representative querier (for MLDv1 operation)

    The timeout time is calculated from Query Interval set for the local device (with the default value used if no Query Interval is set).

  Note:

  > The timeout time is calculated as follows: *query-interval* (value of the QQIC field) x 2 + *query-response-interval*.

(2) Layer 2 forwarding for IPv6 multicast packets

Layer 2 forwarding within VLANs receiving IPv6 multicast packets is performed based on IP address. Layer 2 forwarding based on MLD snooping results is performed for all ports that receive MLD Report (membership request) messages.

(3) Layer 3 forwarding for IPv6 multicast packets

When Layer 3 forwarding based on IPv6 multicast is performed between VLANs and MLD snooping is running on the forwarding destination VLAN, multicast traffic for which Layer 3 forwarding is performed is forwarded according to the learning results for MLD snooping within the forwarding destination VLAN.

(4) Specific query transmission during concurrent usage of IPv6 multicast

IPv6 multicast can be run so that when the Switch is the representative querier in the VLAN, Group-Specific Queries or Group-and-Source-Specific Queries sent due to MLD Done message or MLDv2 Report (leave request) message reception are sent to all ports in the VLAN, and not just the recipient port.

26.4.3 Connections with multicast routers

In addition to the hosts that have already joined a group, the forwarding destinations for multicast packets also include neighboring multicast routers. When the Switch and a multicast router are connected and MLD snooping is used, the port connected to the multicast router to forward multicast packets to the router (abbreviated hereafter to a multicast router port) can be specified by configuration.

The Switch forwards all multicast packets to the specified multicast router port.

Also, because MLD is a protocol for sending and reception between routers and hosts, MLD messages are accepted by routers and hosts. The Switch forwards MLD messages as shown in the following table.

Table 26-5: Operation for each MLDv1 message

MLDv1 message type	Transfer port within the VLAN	Remarks
Multicast Listener Query	Forwarded to all ports.	
Multicast Listener Report	Forwarded only to multicast router ports.	
Multicast Listener Done	Not forwarded to any port when group members still exist for other ports. Forwarded to multicast router ports when no group members exist for other ports.	#

#

This is the forwarding operation when a querier is set for the local device. If no querier has been set, forwarding is always performed to multicast router ports. However, if a port that has not received an MLDv1 or MLDv2 Report (membership request) message receives an MLDv1 Done message, the MLDv1 Done message is not forwarded regardless of the querier settings.

Table 26-6: Operation for each MLDv2 message

MLDv2 message type		Transfer port within the VLAN	Remarks
Version2 Multicast Listener Query		Forwarded to all ports.	
Version2 Multicast Listener Report	Membership Request Report	Forwarded only to multicast router ports.	

MLDv2 message type		Transfer port within the VLAN	Remarks
	Leave Request Report	Not forwarded to any port when group members still exist for other ports. Forwarded to multicast router ports when no group members exist for other ports.	#

#

This is the forwarding operation when a querier is set for the local device. If no querier has been set, forwarding is always performed to multicast router ports. However, if a port that has not received an MLDv1 or MLDv2 Report (membership request) message receives an MLDv2 Report (leave request) message, the MLDv2 Report (leave request) message is not forwarded regardless of the querier settings.

26.4.4 MLD querier functionality

The MLD querier functionality is used by the Switch to send MLD Query messages by proxy to recipient hosts on environments where no multicast router exists in the VLAN, and only hosts that send and receive multicast packets exist. Multicast routers regularly send MLD Query messages and then check for reception from hosts to determine whether group members exist. If no multicast router exists, group members can no longer be monitored because no response is received from recipient hosts. This functionality enables the MLD snooping functionality even when no multicast routers exist in the VLAN. The Switch sends an MLD Query message every 125 seconds.

In order to use the MLD querier functionality, an IP address must be set for VLANs using the MLD snooping functionality.

When devices sending MLD Query messages exist in a VLAN, the MLD Query message transmission source with the lowest IP address becomes the representative querier, and it sends MLD Query messages. If another device in the VLAN is the representative querier, the Switch stops using the MLD querier functionality to send Query messages.

If the representative querier stops, such as due to a malfunction, a new representative querier is chosen. When the Switch is determined to be the representative querier, such as due to a malfunction on another device in the VLAN, MLD Query message transmission is started. The monitoring time for representative queriers on the Switch is 255 seconds.

By default, the version for MLD Queries sent by the Switch is MLDv1. Once the device is running, the MLD Query version follows the MLD version of the representative querier.

26.5 Notes on IGMP snooping and MLD snooping usage

(1) Notes on use with other functionality

For details, see *18.3 Compatibility between Layer 2 switch functionality and other functionality*.

(2) Control packet flooding

Because multicast traffic that is subject to suppression by IGMP snooping or MLD snooping is data traffic, flooding needs to be performed within a VLAN so that the routing protocol and other control packets can be received by all routers and all hosts. Therefore, the Switch forwards packets with destination IP addresses contained in the address ranges shown in the table below to all ports on the VLAN. Packets with destination IP addresses outside the address ranges shown in the following table are forwarded according to learning results for IGMP snooping or MLD snooping.

Table 26-7: Control packet flooding

Protocol	Address range
IGMP snooping	224.0.0.0/24
MLD snooping	ff02::/16

Note that multicast group addresses that duplicate multicast MAC addresses for control packets cannot be used. The following table describes multicast group addresses that cannot be used for addresses outside the address ranges shown in the above table.

Table 26-8: Multicast group addresses that cannot be used with the MAC address control method

Protocol	Multicast group address
IGMP snooping	224.128.0.0/24
	225.0.0.0/24
	225.128.0.0/24
	226.0.0.0/24
	226.128.0.0/24
	227.0.0.0/24
	227.128.0.0/24
	228.0.0.0/24
	228.128.0.0/24
	229.0.0.0/24
	229.128.0.0/24
	230.0.0.0/24
	230.128.0.0/24
	231.0.0.0/24
	231.128.0.0/24
	232.0.0.0/24
	232.128.0.0/24

Protocol	Multicast group address
	233.0.0.0/24
	233.128.0.0/24
	234.0.0.0/24
	234.128.0.0/24
	235.0.0.0/24
	235.128.0.0/24
	236.0.0.0/24
	236.128.0.0/24
	237.0.0.0/24
	237.128.0.0/24
	238.0.0.0/24
	238.128.0.0/24
	239.0.0.0/24
	239.128.0.0/24

When addresses shown in the above table are used for multicast group addresses, multicast data bound for corresponding multicast group addresses will be forwarded to all ports in the VLAN.

When setting a trunk port, make sure that it does not receive any untagged control packets. Set a native VLAN in the configuration if untagged control packets are to be handled by the trunk port.

(3) Setting multicast router ports

(a) Redundant configurations

When Spanning Tree Protocols are used for a redundant configuration and the connection with the router might change due to topology changes by a Spanning Tree Protocol, a multicast router port must be set for all ports that might connect with the router.

(b) Connections between Layer 2 switches

On VLANs that contain only multiple Layer 2 switches, a multicast router port must be set for ports connecting to Layer 2 switches handling multicast traffic transmission hosts.

When a redundant configuration is used, a multicast router port must be set for all ports that might connect to Layer 2 switches handling transmission hosts.

(4) Connections with IGMP version 3 hosts

One of the following needs to be performed when the Switch is connected to an IGMPv3 host:

- Use IPv4 multicast for the corresponding VLAN and set the IGMP version to 3.
- Set an IP address so that the corresponding router connected to the IGMPv3 router becomes the representative querier.

Use a configuration in which IGMPv3 messages from IGMPv3 hosts are not split into fragments.

(5) Connections with MLD version 2 hosts

One of the following needs to be performed when the Switch is connected to an MLDv2 host:

- Use IPv6 multicast for the corresponding VLAN and set the MLD version to 2.

- Set an IP address so that the corresponding router connected to the MLDv2 router becomes the representative querier.

Use a configuration in which IGMPv2 messages from IGMPv2 hosts are not split into fragments.

(6) Executing operation commands to relearn entries

In addition to the operation commands for IGMP and MLD snooping, if the commands below are executed, any learned entries are cleared and then relearned. After these operation commands are executed, multicast communication will be cut off temporarily.

- The `running-config` command is overwritten by the `copy` command
- The `restart vlan` command is executed.

(7) Concurrent usage with IPv4 multicast functionality

(a) Temporary communication stoppage when an IGMP snooping setting is added

When an IGMP snooping setting is added to a VLAN using IPv4 multicast, multicast communication stops temporarily. After the IGMP snooping setting is configured, multicast communication is restarted when an IGMP Report (membership request) is received.

(b) Combined usage with static group participation functionality

For VLANs using the static group participation functionality for IPv4 multicast, some IGMP Reports (membership requests) from hosts might not be sent. When this functionality is used with IGMP snooping and IGMP Reports (membership requests) are not sent, set a multicast router port for ports needed for multicast communication on VLANs using static group participation functionality because multicast communication cannot be performed.

(8) Concurrent usage with IPv6 multicast functionality

(a) Temporary communication stoppage when an MLD snooping setting is added

When an MLD snooping setting is added to a VLAN using IPv6 multicast, multicast communication stops temporarily. After the MLD snooping setting is configured, multicast communication is restarted when an MLD Report (membership request) is received.

(b) Combined usage with static group participation functionality

For VLANs using the static group participation functionality for IPv6 multicast, some MLD Reports (membership requests) from hosts might not be sent. When this functionality is used with MLD snooping and MLD Reports (membership requests) are not sent, set a multicast router port for ports needed for multicast communication on VLANs using static group participation functionality because multicast communication cannot be performed.

(9) IGMP instant leave

When IGMP instant leave is used and an IGMPv2 Leave or IGMPv3 Report (leave request) message is received, multicast communication to the corresponding port stops immediately. Therefore, when this functionality is used, we recommend that you place only one recipient terminal for each multicast group on the connection port.

When multiple recipient terminals in the same multicast group are placed on a connection port, multicast communication to other recipients stops temporarily. In this case, multicast communication is restarted when an IGMP Report (membership request) message is received from the recipient.

Chapter

27. Settings and Operation for IGMP Snooping and MLD Snooping

IGMP snooping and MLD snooping are functions that use Layer 2 to control multicast traffic within a VLAN. This chapter explains how to set and use IGMP snooping and MLD snooping.

27.1 Configuration of IGMP snooping

27.1.1 List of configuration commands

The following table describes the configuration commands for IGMP snooping.

Table 27-1: List of configuration commands

Command name	Description
ip igmp snooping (global)	Use `no ip igmp snooping` to suppress IGMP snooping functionality for the Switch.
ip igmp snooping (interface)	Sets IGMP snooping functionality for the specified interface.
ip igmp snooping fast-leave	Sets IGMP instant leave.
ip igmp snooping mrouter interface	Sets IGMP multicast router ports.
ip igmp snooping querier	Sets IGMP querier functionality.

27.1.2 Configuring IGMP snooping

Points to note

To run IGMP snooping, specify the settings below for the VLAN used in VLAN interface configuration mode.

In the following, IGMP snooping functionality is enabled for VLAN 2.

Command examples

1.
```
(config)# interface vlan 2
(config-if)# ip igmp snooping
```

Switches to the VLAN interface configuration mode for VLAN 2, and enables IGMP snooping functionality.

27.1.3 Configuring the IGMP querier functionality

Points to note

When no multicast router exists within a VLAN for which IGMP snooping is set, IGMP querier functionality needs to be run. Specify the following settings for the VLAN interface configuration mode for the corresponding VLAN.

Command examples

1.
```
(config-if)# ip igmp snooping querier
```

Enables IGMP querier functionality.

Notes

This setting is enabled if only if an IPv4 address is set for the corresponding interface.

27.1.4 Configuring multicast router ports

Points to note

When a multicast router is connected within a VLAN for which IGMP snooping is set, specify the settings below for the VLAN interface configuration mode of the corresponding VLAN. The following shows an example where the multicast router is connected to the gigabit Ethernet interface on port 1/0/1 within the target VLAN.

Command examples

1. `(config-if)# ip igmp snooping mrouter interface gigabitethernet 1/0/1`

   Specifies the multicast router port for the corresponding interface.

27.2 IGMP snooping operation

27.2.1 List of operation commands

The following table describes the operation commands for IGMP snooping.

Table 27-2: List of operation commands

Command name	Description
show igmp-snooping	Shows IGMP snooping information.
clear igmp-snooping	Clears IGMP snooping information.
restart snooping	Restarts the snooping program.
dump protocols snooping	Outputs event trace information and control table information to a file.

27.2.2 Checking IGMP snooping

The following describes the IGMP snooping contents to be checked when IGMP snooping functionality is used.

(1) Check after configuration

Execute the `show igmp-snooping` command to check that the settings related to IGMP snooping are correct.

Figure 27-1: Displayed status for IGMP snooping settings

```
> show igmp-snooping 100
Date 20XX/10/01 15:20:00 UTC
VLAN: 100
  IP address: 192.168.11.20/24    Querier: enable
  IGMP querying system: 192.168.11.20
  Querier version: V2
  IPv4 Multicast routing: Off
  Fast-leave: On
  Port(5): 0/1-5
  Mrouter-port: 0/1,3
  Group Counts: 3
```

(2) During operation

Execute the following command to check the status of IGMP snooping during operation.

- Use the `show igmp-snooping group` command to check learned MAC addresses, IPv4 multicast addresses forwarded within a VLAN, and a list of forwarding destination port statuses.

Figure 27-2: Results of executing the show igmp-snooping group command

```
> show igmp-snooping group 100
Date 20XX/02/01 15:20:00 UTC
VLAN counts: 1
VLAN: 100  Group counts: 3  IPv4 Multicast routing: Off
  Group Address     MAC Address         Version         Mode
  224.10.10.10      0100.5e0a.0a0a      V2              -
    Port-list:0/1-3
  225.10.10.10      0100.5e0a.0a0a      V3              INCLUDE
    Port-list:0/1-2
  239.192.1.1       0100.5e40.0101      V2,V3           EXCLUDE
    Port-list:0/1
```

- Use the `show igmp-snooping port` command to check the participation group display example for each port.

Figure 27-3: Results of executing the show igmp-snooping port command

```
> show igmp-snooping port 0/1
Date 20XX/10/01 15:20:00 UTC
Port 0/1  VLAN counts: 2
  VLAN: 100  Group counts: 2
    Group Address     Last Reporter      Uptime     Expires
    224.10.10.10      192.168.1.3        00:10      04:10
    239.192.1.1       192.168.1.3        02:10      03:00
  VLAN: 150  Group counts: 1
    Group Address     Last Reporter      Uptime     Expires
    239.10.120.1      192.168.15.10      01:10      02:30
```

27.3 Configuration of MLD snooping

27.3.1 List of configuration commands

The following table describes the configuration commands for MLD snooping.

Table 27-3: List of configuration commands

Command name	Description
ipv6 mld snooping	Enables MLD snooping functionality.
ipv6 mld snooping mrouter interface	Sets MLD multicast router ports.
ipv6 mld snooping querier	Sets MLD querier functionality.
no ipv6 mld snooping	Disables MLD snooping functionality.

27.3.2 Configuring MLD snooping

Points to note

To run MLD snooping, specify the settings below for the VLAN used in the interface configuration mode of the VLAN interface. In the following example, MLD snooping functionality is enabled for VLAN 2.

Command examples

1.
```
(config)# interface vlan 2
(config-if)# ipv6 mld snooping
```
Switches to the VLAN interface configuration mode for VLAN 2, and enables MLD snooping functionality.

27.3.3 Configuring the MLD querier functionality

Points to note

When no multicast router exists within a VLAN for which MLD snooping is set, MLD querier functionality needs to be run. The following sets the VLAN interface configuration mode for the corresponding VLAN.

Command examples

1.
```
(config-if)# ipv6 mld snooping querier
```
Enables MLD querier functionality.

Notes

This setting is enabled only if an IPv6 address is set for the corresponding interface.

27.3.4 Configuring multicast router ports

Points to note

When a multicast router is connected within a VLAN for which MLD snooping is set, specify the settings below for the VLAN interface configuration mode of the corresponding VLAN. The following shows an example where the multicast router is connected to the gigabit Ethernet interface on port 1/0/1 within the target VLAN.

Command examples

1. `(config-if)# ipv6 mld snooping mrouter interface gigabitethernet 1/0/1`

   Specifies the multicast router port for the corresponding interface.

27.4 MLD snooping operation

27.4.1 List of operation commands

The following table describes the operation commands for MLD snooping.

Table 27-4: List of operation commands

Command name	Description
show mld-snooping	Shows MLD snooping information.
clear mld-snooping	Clears MLD snooping information.
restart snooping	Restarts the snooping program.
dump protocols snooping	Outputs event trace information and control table information to a file.

27.4.2 Checking MLD snooping

The following describes the MLD snooping contents to be checked when MLD snooping functionality is used.

(1) After configuring settings

Execute the `show mld-snooping` command to check that the settings related to MLD snooping are correct.

Figure 27-4: Displayed status for MLD snooping settings

```
> show mld-snooping 100
Date 20XX/02/01 15:20:00 UTC
VLAN: 100
  IP address: fe80::b1    Querier: enable
  MLD querying system: fe80::b1
  Querier version: V1
  IPv6 Multicast routing: Off
  Querier version: V2
  Port(5): 0/1-5
  Mrouter-port: 0/1,3
  Group Counts: 3
```

(2) During operation

Execute the following command to check the status of MLD snooping during operation.

- Use the `show mld-snooping group` command to check learned MAC addresses, IPv6 multicast addresses forwarded within a VLAN, and a list of forwarding destination port statuses.

Figure 27-5: Results of executing the show mld-snooping group command

```
> show mld-snooping group 100
Date 20XX/02/01 15:20:00 UTC
VLAN: counts: 1
VLAN: 100  Group counts: 2  IPv6 Multicast routing: Off
  Group Address     MAC Address        Version      Mode
  ff35::1           3333:0000:0001     V1,V2        EXCLUDE
    Port-list:0/1-3
  ff35::2           3333:0000:0002     V2           EXCLUDE
    Port-list:0/1-2
```

- Use the `show mld-snooping port` command to check the participation group display example for each port.

Figure 27-6: Results of executing the show mld-snooping port command

```
> show mld-snooping port 0/1
Date 20XX/12/01 15:20:00 UTC
Port  0/1  VLAN counts: 1
  VLAN: 100  Group counts: 2
    Group Address      Last Reporter      Uptime     Expires
    ff35::1            fe80::b2           00:10      04:10
    ff35::2            fe80::b3           02:10      03:00
```

Appendix

A. Relevant standards

A.1 TELNET/FTP

Table A-1: Relevant standards and recommendations for TELNET/FTP

Name (month and year issued)	Title
RFC 854 (May 1983)	TELNET PROTOCOL SPECIFICATION
RFC 855 (May 1983)	TELNET OPTION SPECIFICATIONS
RFC 959 (October 1985)	FILE TRANSFER PROTOCOL (FTP)

A.2 RADIUS or TACACS+

Table A-2: Relevant standards and recommendations for RADIUS and TACACS+

Name (month and year issued)	Title
RFC 2865 (June 2000)	Remote Authentication Dial In User Service (RADIUS)
RFC 2866 (June 2000)	RADIUS Accounting
RFC 3162 (August 2001)	RADIUS and IPv6
draft-grant-tacacs-02 (January 1997)	The TACACS+ Protocol Version 1.78

A.3 NTP

Table A-3: Relevant standard and recommendation for NTP

Name (month and year issued)	Title
RFC 1305 (March 1992)	Network Time Protocol (Version 3) Specification, Implementation and Analysis

A.4 DNS

Table A-4: Relevant standards and recommendations for DNS resolver

Name (month and year issued)	Title
RFC 1034 (March 1987)	Domain names - concepts and facilities
RFC 1035 (March 1987)	Domain names - implementation and specification

A.5 Ethernet

Table A-5: Relevant standards for Ethernet interfaces

Type	Standards	Name
10BASE-T, 100BASE-TX, 1000BASE-T, 100BASE-FX, 1000BASE-X, 10GBASE-R	IEEE 802.3x-1997	IEEE Standards for Local and Metropolitan Area Networks: Specification for 802.3 Full Duplex Operation
	IEEE 802.2 1998 Edition	IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 2: Logical Link Control
	IEEE 802.3 2000 Edition	Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer Specifications
	IEEE 802.3ah 2004	Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks
	IEEE Std 802.3u-1995	Type 100BASE-T MAC parameters, Physical Layer, MAUs, and Repeater for 100 Mb/s Operation
10GBASE-R	IEEE 802.3ae Standard-2002	Media Access Control(MAC) Parameters, Physical Layer, and Management Parameters for 10 Gb/s Operation
40GBASE-R	IEEE 802.3ba Standard-2010	Media Access Control Parameters, Physical Layers, and Management Parameters for 40 Gb/s and 100 Gb/s Operation

A.6 Link aggregation

Table A-6: Relevant standard for link aggregation

Standards	Name
IEEE 802.3ad (IEEE Std 802.3ad-2000)	Aggregation of Multiple Link Segments

A.7 VLAN

Table A-7: Relevant standard and recommendation for VLANs

Standards	Name
IEEE 802.1Q (IEEE Std 802.1Q-2003)	Virtual Bridged Local Area Networks#

#: GVRP/GMRP is not supported.

A.8 Spanning Tree Protocols

Table A-8: Relevant standards and recommendation for Spanning Tree Protocols

Standards	Name
IEEE 802.1D (ANSI/IEEE Std 802.1D-1998 Edition)	Media Access Control (MAC) Bridges (The Spanning Tree Algorithm and Protocol)
IEEE 802.1t (IEEE Std 802.1t-2001)	Media Access Control (MAC) Bridges - Amendment 1
IEEE 802.1w (IEEE Std 802.1w-2001)	Media Access Control (MAC) Bridges - Amendment 2: Rapid Reconfiguration

Standards	Name
IEEE 802.1s (IEEE Std 802.1s-2002)	Virtual Bridged Local Area Networks - Amendment 3: Multiple Spanning Trees

A.9 IGMP snooping and MLD snooping

Table A-9: Relevant standards and recommendation for IGMP snooping and MLD snooping

Name (month and year issued)	Title
RFC 4541 (May 2006)	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

B. Acknowledgments

[SNMP]

****

Copyright 1988-1996 by Carnegie Mellon University

All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

****

Some of this software has been modified by BBN Corporation and is a derivative of software developed by Carnegie Mellon University. Use of the software remains subject to the original conditions set forth above.

****

Some of this software is Copyright 1989 by TGV, Incorporated but subject to the original conditions set forth above.

****

Some of this software is Copyright (C) 1983,1988 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of California at Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty.

****

* Primary Author:

Steve Waldbusser

* Additional Contributors:

Erik Schoenfelder (schoenfr@ibr.cs.tu-bs.de): additions, fixes and enhancements for Linux by 1994/1995.

David Waitzman: Reorganization in 1996.

Wes Hardaker <hardaker@ece.ucdavis.edu>: Some bug fixes in his UC

Davis CMU SNMP distribution were adopted by David Waitzman

David Thaler <thalerd@eecs.umich.edu>: Some of the code for making the agent embeddable into another application were adopted by David Waitzman

Many more over the years...

[NTP]

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

Copyright (C) David L. Mills 1992-2003 Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.

[PIM sparse-mode pimd]

```
/*
 * Copyright (c) 1998-2001
 * The University of Southern California/Information Sciences Institute.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. Neither the name of the project nor the names of its contributors
 *    may be used to endorse or promote products derived from this software
 *    without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS''
AND
```

```
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 */
/*
 * Part of this program has been derived from mrouted.
 * The mrouted program is covered by the license in the accompanying file
 * named "LICENSE.mrouted".
 *
 * The mrouted program is COPYRIGHT 1989 by The Board of Trustees of
 * Leland Stanford Junior University.
 *
 */
```

[pim6dd]

```
/*
 * Copyright (C) 1998 WIDE Project.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. Neither the name of the project nor the names of its contributors
 *    may be used to endorse or promote products derived from this software
 *    without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS''
AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE
LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF
 * SUCH DAMAGE.
 */
```

[pim6sd]

```
/*
 * Copyright (C) 1999 LSIIT Laboratory.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. Neither the name of the project nor the names of its contributors
 *    may be used to endorse or promote products derived from this software
 *    without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 */
/*
 *  Questions concerning this software should be directed to
 *  Mickael Hoerdt (hoerdt@clarinet.u-strasbg.fr) LSIIT Strasbourg.
 *
 */
/*
 * This program has been derived from pim6dd.
 * The pim6dd program is covered by the license in the accompanying file
 * named "LICENSE.pim6dd".
 */
/*
 * This program has been derived from pimd.
 * The pimd program is covered by the license in the accompanying file
 * named "LICENSE.pimd".
 *
 */
```

[RADIUS]

Copyright 1992 Livingston Enterprises, Inc.

Livingston Enterprises, Inc. 6920 Koll Center Parkway Pleasanton, CA 94566

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Livingston Enterprises, Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Livingston Enterprises, Inc. Livingston Enterprises, Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

[totd]

WIDE

Copyright (C) 1998 WIDE Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by WIDE Project and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

University of Tromso

Author: Feike W. Dillema, The Pasta Lab, Institutt for Informatikk University of Tromso, Norway

Invenia Innovation A.S.

Author: Feike W. Dillema, Invenia Innovation A.S., Norway.

Todd C. Miller

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[libtacplus]

Copyright (C) 1998, 2001, 2002, Juniper Networks, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[tftp]

Copyright (C) 1983, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[libfetch]

Copyright (C) 1998 Dag-Erling Coïdan Smørgrav

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer in this position and unchanged.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[IPv6 DHCP]

Copyright (C) 1998-2004 WIDE Project.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright

notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright

[iides]

DISCLAIMED.

[Net-SNMP]

CMU/UCD

Networks Associates Technology, Inc

Cambridge Broadband Ltd.

Sun Microsystems, Inc.

Sparta, Inc

DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Cisco/BUPTNIC

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Apache License Version 2.0

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

Index