

AX2500S Software Manual

Configuration Guide Vol. 1

For Version 3.5

AX25S-S001X-70

Alaxala

Relevant products

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

Export restrictions

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

Trademarks

Ethernet is a registered trademark of Xerox Corporation.

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

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

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

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

Wake-on-LAN is a registered trademark of IBM Corporation.

MagicPacket is a registered trademark of Advanced Micro Devices, Inc.

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

Reading and storing this manual

Before you use the equipment, carefully read the manual and make sure that you understand all safety precautions. After reading the manual, keep it in a convenient place for easy reference.

Notes

Information in this document is subject to change without notice.

Editions history

January 2013 (Edition 8) AX25S-S001X-70

Copyright

All Rights Reserved, Copyright(C),2010, 2013, ALAXALA Networks, Corp.

History of Amendments

[Ver.3.5 (Edition 8)]

Summary of amendments

Location and title	Changes
2 Switch Configuration	<ul style="list-style-type: none">● The AX2530S-24TD, AX2530S-48TD, and AX2530S-24S4XD models were added.
3 Capacity Limit	<ul style="list-style-type: none">● The AX2530S-24TD, AX2530S-48TD, and AX2530S-24S4XD models were added.● Maximum number of logins that are possible from remote operation terminals to a Switch was changed in <i>Login Security and RADIUS</i>.
8 Login Security and RADIUS	<ul style="list-style-type: none">● Maximum number of remote login users was changed in <i>Overview of login control</i>.
11 Device Management	<ul style="list-style-type: none">● A description about adding a tag dedicated to Web authentication was added to the description about restoring switch information.
12 Power Saving Functionality	<ul style="list-style-type: none">● The AX2530S-24TD, AX2530S-48TD, and AX2530S-24S4XD models were added.
14 Ethernet	<ul style="list-style-type: none">● The AX2530S-24TD, AX2530S-48TD, and AX2530S-24S4XD models were added.● A description about a 30 cm direct attach cable was added.
15 Link Aggregation	<ul style="list-style-type: none">● A description of the standby link functionality was added.
17 MAC Address Learning	<ul style="list-style-type: none">● Change of SML status was added as a trigger when the MAC address table is cleared.

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

[Ver.3.4 (Edition 7)]

Summary of amendments

Location and title	Changes
Command Operations	<ul style="list-style-type: none">● Descriptions about customizing CLI settings were added.● Descriptions of <i>Display restrictions applying to command line completion and Help functionality</i> in the notes for the CLI were changed.
Device Management	<ul style="list-style-type: none">● Notes on support for Long Life Solution were changed.● Descriptions about CLI environment information were added to the switch information saved to a backup file.

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

Location and title	Changes
Capacity Limit	<ul style="list-style-type: none"> The following descriptions were added to the capacity limits in 3.2.3 <i>Layer 2 switching</i>: <ul style="list-style-type: none"> - Spanning Tree Protocols - Ring Protocol The following descriptions were added to the capacity limits in 3.2.4 <i>IP interface</i>: <ul style="list-style-type: none"> - Maximum number of interfaces that allow VLAN-based reception control to work - IPv6 interfaces
Command Operations	<ul style="list-style-type: none"> Descriptions of <i>Display restrictions applying to command line completion and Help functionality</i> in the notes for the CLI were changed.
Login Security and RADIUS	<ul style="list-style-type: none"> Descriptions for IPv6 were added for setting login security. NAS-IPv6-Address was added to the supported RADIUS attributes.
Host Names and DNS	<ul style="list-style-type: none"> This section was added.
Ethernet	<ul style="list-style-type: none"> Descriptions of using TPIDs other than the standard 0x8100 were deleted from the setting of jumbo frames. Descriptions of setting the link-up detection timer were added.
Layer 2 Switching Overview	<ul style="list-style-type: none"> Restrictions on VLANs were changed. Restrictions on Spanning Tree Protocols were changed. Restrictions on the Ring Protocol were changed.
MAC Address Learning	<ul style="list-style-type: none"> The following triggers were added to the triggers when the MAC address table is cleared: <ul style="list-style-type: none"> - When a flush control frame is received in a network configuration using a Spanning Tree Protocol and the Ring Protocol - When a flush control frame is received in a network configuration using GSRP and the Ring Protocol - When the Switch runs as the master node and the route is switched - When the multi-fault monitoring functionality is enabled and the MAC address table is cleared - When flush control frames for neighboring rings is received
Description of the Ring Protocol	<ul style="list-style-type: none"> The following descriptions were added: <ul style="list-style-type: none"> - Operation when path switchback is suppressed and cleared - Multi-fault monitoring functionality The following descriptions were changed because the master node, shared nodes, and multi-fault monitoring functionality are now supported: <ul style="list-style-type: none"> - Overview of the Ring Protocol - Basic Ring Protocol principles - Ring Protocol network design - Notes on Ring Protocol usage
Settings and Operation for Ring Protocol	<ul style="list-style-type: none"> The following descriptions were added: <ul style="list-style-type: none"> - Enabling the path switchback suppression functionality and setting suppression times - Configuring the multi-fault monitoring functionality

Location and title	Changes
	<ul style="list-style-type: none"> ● Descriptions were changed because the master node and shared nodes are now supported.
Using the Ring Protocol with Spanning Tree Protocols/GSRP	<ul style="list-style-type: none"> ● Descriptions were changed because the Ring Protocol and Spanning Tree Protocols can now be used together. ● Descriptions were changed because Switches now support ring configurations in which switches exist that use both the Ring Protocol and GSRP.
IPv4 Interfaces	<ul style="list-style-type: none"> ● Descriptions of setting up static ARP were added.
IPv6 Interfaces	<ul style="list-style-type: none"> ● This section was added.

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

[Ver.3.2 (Edition 5)]

Summary of amendments

Location and title	Changes
Capacity Limit	<ul style="list-style-type: none"> ● The following items were added to the capacity limits in <i>3.2.3 Layer 2 switching</i>: <ul style="list-style-type: none"> - VLAN tunneling - Tag translation ● The following item was added to the capacity limits in <i>3.2.3 Layer 2 switching</i>: <ul style="list-style-type: none"> - IGMP snooping/MLD snooping
Time Settings and NTP	<ul style="list-style-type: none"> ● As a storage destination, the remote FTP server was added to the description of the backup and restore operation commands.
Ethernet	<ul style="list-style-type: none"> ● Descriptions of 10GBASE-ER were added.
Layer 2 Switching Overview	<ul style="list-style-type: none"> ● Descriptions of VLAN tunneling and tag translation were added to <i>Compatibility between Layer 2 switch functionality and other functionality</i>.
VLAN	<ul style="list-style-type: none"> ● Descriptions of VLAN tunneling and TPID settings were added.
VLAN Extended Functionality	<ul style="list-style-type: none"> ● <i>VLAN Extended Functionality</i> was added. ● <i>Configuration of VLAN tunneling</i> was added. ● <i>Description of tag translation</i> was added. ● <i>Configuration of tag translation</i> was added. ● Descriptions of VLAN tunneling were added to <i>Description of L2 protocol frame transparency functionality</i>.

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

[Ver.3.2 (Edition 4)]

Summary of amendments

Location and title	Changes
Overview of the Switch	<ul style="list-style-type: none">● The AX2530S-24T4X and AX2530S-48T2X models were added.
Switch Configuration	<ul style="list-style-type: none">● The AX2530S-24T4X and AX2530S-48T2X models were added.
Capacity Limit	<ul style="list-style-type: none">● The AX2530S-24T4X and AX2530S-48T2X models were added.● Descriptions for IPv6 conditions were added in 3.2.5 <i>Filters and QoS</i>.
Command Operations	<ul style="list-style-type: none">● Descriptions of <i>Display restrictions applying to command line completion and Help functionality</i> in the notes for the CLI were changed.
Power Saving Functionality	<ul style="list-style-type: none">● The AX2530S-24T4X and AX2530S-48T2X models were added.● Descriptions of <i>When placing a Switch in sleep mode</i> in the notes on saving power were changed.
Ethernet	<ul style="list-style-type: none">● The AX2530S-24T4X and AX2530S-48T2X models were added.

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

[Ver.3.1 (Edition 3)]

Summary of amendments

Location and title	Changes
Overview of the Switch	<ul style="list-style-type: none">● Descriptions were added because OAN was supported.
Capacity Limit	<ul style="list-style-type: none">● Descriptions about the number of lines that can be handled were changed because SPFs were supported for 10BASE-T, 100BASE-TX, and 1000BASE-T.
Command Operations	<ul style="list-style-type: none">● Descriptions of <i>Display restrictions applying to command line completion and Help functionality</i> in the notes on the CLI were changed.
Login Security and RADIUS	<ul style="list-style-type: none">● Descriptions about authentication using RADIUS were changed due to supporting end-by-reject.● Examples of setting the login authentication method were changed because end-by-reject was supported.● Descriptions about registered information on the RADIUS server were changed because the user ID and the password length were extended.
Time Settings and NTP	<ul style="list-style-type: none">● Descriptions about checking the time were added.
Device Management	<ul style="list-style-type: none">● Descriptions on notes about restoring the switch information were changed.
Power Saving Functionality	<ul style="list-style-type: none">● Descriptions were changed because the option for recovering the device from the sleep status in the AX25030S-24S4X model was supported.● Descriptions about saving power for ports were changed.

Location and title	Changes
Ethernet	<ul style="list-style-type: none"> Descriptions were changed because SPFs were supported for 10BASE-T, 100BASE-TX, and 1000BASE-T.
Description of IGMP Snooping and MLD Snooping	<ul style="list-style-type: none"> Descriptions were changed because IGMPv3 was supported.
Settings and Operation for IGMP Snooping and MLD Snooping	<ul style="list-style-type: none"> Descriptions were changed because IGMPv3 was supported.

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

[Ver.3.1 (Edition 2)]

Summary of amendments

Location and title	Changes
Overview of the Switch	<ul style="list-style-type: none"> Descriptions for corresponding to 10G uplinks were added.
Switch Configuration	<ul style="list-style-type: none"> Descriptions for AX2530S-24S4X and 10GBASE-R were added.
Capacity Limit	<ul style="list-style-type: none"> Descriptions for AX2530S-24S4X, 100BASE-FX, and 10GBASE-R were added. Descriptions about AX2530S-24S4X were added to (13) <i>Layer 2 authentication (a) IEEE 802.1X</i>. Descriptions about AX2530S-24S4X were added to (16) <i>Uplink redundancy</i>. (17) <i>SML</i> was added Descriptions about AX2530S-24S4X were added to (18) <i>IEEE 802.3ah/UDLD</i>.
Command Operations	<ul style="list-style-type: none"> Descriptions of <i>Display restrictions applying to command line completion and Help functionality</i> in the notes on the CLI were changed.
Device Management	<ul style="list-style-type: none"> Descriptions about checking the environment status and the temperature history information of the device were added.
Ethernet	<ul style="list-style-type: none"> <i>Description of the 100BASE-FX interface</i> was added. <i>Configuration of the 100BASE-FX interface</i> was added. <i>Description of the 10GBASE-R interface</i> was added. <i>Configuration of the 10GBASE-R interface</i> was added. <i>Description of shared SFP/SFP+ ports</i> was added. <i>Configuration of shared SFP/SFP+ ports</i> was added.
Spanning Tree Protocols	<ul style="list-style-type: none"> Descriptions about 10Gbit/s were added for setting the path cost.

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

Preface

Applicable products and software versions

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

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

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

[24T]:

The description applies to the AX2530S-24T switch.

[24T4X]:

The description applies to the AX2530S-24T4X switch.

[48T]:

The description applies to the AX2530S-48T switch.

[48T2X]:

The description applies to the AX2530S-48T2X switch.

[24S4X]:

The description applies to the AX2530S-24S4X switch.

[24TD]:

The description applies to the AX2530S-24TD switch.

[48TD]:

The description applies to the AX2530S-48TD switch.

[24S4XD]:

The description applies to the AX2530S-24S4XD switch.

[10G model]:

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

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

[OS-L2A]:

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

Corrections to the manual

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

Intended readers

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

Readers must have an understanding of the following:

- The basics of network system management

Manual URL

You can view this manual on our website at:

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

Reading sequence of the manuals

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

- **Learning the basic settings for initial installation, and determining the hardware facility conditions and how to handle the hardware**

AX2500S
Hardware Instruction Manual
(AX25S-H001X)

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

Configuration Guide
Vol.1
(AX25S-S001X)
Vol.2
(AX25S-S002X)

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

Configuration
Command Reference
(AX25S-S003X)

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

Operation Command Reference
(AX25S-S004X)

- **Understanding messages and logs**

Message and Log Reference
(AX25S-S005X)

- **Understanding the MIB**

MIB Reference
(AX25S-S006X)

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

Troubleshooting Guide
(AX25S-T001X)

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
EPU	External redundant Power Unit
ES	End System

Preface

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

Preface

RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REject
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SElector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SFP+	Enhanced Small Form factor Pluggable
SML	Split Multi Link
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
ULR	Uplink Redundant
UPC	Usage Parameter Control

UPC-RED	Usage Parameter Control - Random Early Detection
VAA	VLAN Access Agent
VLAN	Virtual LAN
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

Conventions: The terms "Switch" and "switch"

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

- AX2500S series switch

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

Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

1 KB (kilobyte) is 1024 bytes.

1 MB (megabyte) is 1024^2 bytes.

1 GB (gigabyte) is 1024^3 bytes.

1 TB (terabyte) is 1024^4 bytes.

Contents

1. Overview of the Switch.....	1
1.1 Overview of the Switch.....	2
1.2 Switch features.....	3
2. Switch Configuration.....	9
2.1 Switch model range.....	10
2.1.1 External view.....	10
2.2 Switch components	13
2.2.1 Hardware.....	13
2.2.2 Software	17
3. Capacity Limit.....	19
3.1 Line and module capacities.....	20
3.1.1 Number of lines.....	20
3.1.2 Mounted power supply unit	20
3.1.3 Amount of installed memory.....	21
3.2 Capacity limit.....	22
3.2.1 Login security and RADIUS	22
3.2.2 Link aggregation	22
3.2.3 Layer 2 switch functionality	23
3.2.4 IP interface	28
3.2.5 Filters and QoS	31
3.2.6 Layer 2 authentication functionality	36
3.2.7 DHCP snooping	41
3.2.8 High reliability function based on redundant configurations	41
3.2.9 High reliability function based on network failure detection.....	42
3.2.10 Neighboring device information (LLDP).....	44
4. Login Procedures	45
4.1 Operation terminal-based management	46
4.1.1 Operation terminals.....	46
4.1.2 Connection topology of operation terminals	47
4.1.3 Overview of operation management functionality.....	48
4.2 Starting the switch	50
4.2.1 Workflow from starting to stopping a switch.....	50
4.2.2 Start procedures.....	51
4.2.3 Stop procedure.....	51
4.3 Login and logout.....	52
5. Command Operations	53
5.1 Command input mode.....	54
5.1.1 List of operation commands.....	54
5.1.2 Command input mode.....	54
5.2 CLI operations	56
5.2.1 Command line completion	56
5.2.2 Help.....	56
5.2.3 Entry-error location detection functionality.....	56
5.2.4 Abbreviated-command execution	57
5.2.5 History functionality	57
5.2.6 Paging.....	58
5.2.7 Keyboard command functionality.....	58
5.2.8 Customizing CLI settings	59
5.3 Notes on CLI operation	61
6. Configuration	67
6.1 Configuration.....	68
6.1.1 Configuration at startup.....	68

6.1.2 Configuration during operation	68
6.2 Overview of editing a running configuration	69
6.3 Mode transitions when entering configuration commands.....	70
6.4 Configuration editing procedures	71
6.4.1 Lists of configuration commands and operation commands	71
6.4.2 Starting configuration editing (configure command and configure terminal command)	71
6.4.3 Displaying and checking configuration entries (show command).....	72
6.4.4 Adding, changing, and deleting configuration entries	74
6.4.5 Saving configuration entries to a file	75
6.4.6 Ending configuration editing (exit command).....	76
6.4.7 Notes on configuration editing	76
6.5 Configuration operations	77
6.5.1 Transferring files using the ftp command.....	77
6.5.2 Transferring files using a memory card.....	78
6.5.3 Notes on applying a backup configuration file	79
7. Remote Login	81
7.1 Description	82
7.2 Configuration	83
7.2.1 List of configuration commands	83
7.2.2 Assigning an IP address to the Switch.....	83
7.2.3 Permitting login by using the Telnet protocol	84
7.2.4 Permitting login by using FTP.....	84
7.3 Operation.....	85
7.3.1 List of operation commands.....	85
7.3.2 Checking communication between a remote operation terminal and the Switch	85
8. Login Security and RADIUS.....	87
8.1 Setting login security	88
8.1.1 Lists of configuration and operation commands	88
8.1.2 Overview of login control.....	88
8.1.3 Creating and deleting user accounts	89
8.1.4 Setting the password for switching to administrator mode	89
8.1.5 Permitting login from a remote operation terminal.....	90
8.1.6 Setting the maximum number of concurrent users	90
8.1.7 Setting the IP addresses of remote operation terminals permitted to log in	90
8.2 Description of RADIUS.....	92
8.2.1 Overview of RADIUS	92
8.2.2 Scope of RADIUS implementation.....	92
8.2.3 Authentication using RADIUS	94
8.2.4 Connecting with a RADIUS server.....	97
8.3 RADIUS configuration	99
8.3.1 List of configuration commands	99
8.3.2 Configuring the login authentication method	99
8.3.3 Configuring a RADIUS server group.....	101
8.4 RADIUS operation.....	103
8.4.1 List of operation commands.....	103
8.4.2 Displaying information about the RADIUS servers in effect	103
9. Time Settings and NTP.....	107
9.1 Setting and checking the time	108
9.1.1 Supported specifications	108
9.1.2 Notes on changing the time	110
9.2 Configuration	111
9.2.1 Configuration commands	111
9.2.2 Setting the system clock	111
9.2.3 Acquiring the time periodically from the NTP server.....	111
9.3 Operation.....	113

9.3.1 List of operation commands.....	113
9.3.2 Checking the time	113
9.3.3 Displaying the NTP client information	113
10. Host Names and DNS.....	115
10.1 Description	116
10.2 Configuration	117
10.2.1 List of configuration commands	117
10.2.2 Configuring host names	117
10.2.3 Configuring DNS settings.....	117
11. Device Management	119
11.1 Settings related to status display and system operation	120
11.1.1 List of configuration commands and operation commands	120
11.1.2 Checking the software version	121
11.1.3 Checking the switch status.....	121
11.1.4 Viewing and controlling operation message output	124
11.1.5 Viewing logged data	124
11.2 Backing up and restoring switch information.....	125
11.2.1 List of operation commands	125
11.2.2 Information that is backed up or restored	125
11.3 Failure recovery.....	128
11.3.1 Error locations and recovery processing.....	128
12. Power Saving Functionality	131
12.1 Description of the power saving functionality	132
12.1.1 Supported functionality	132
12.1.2 LED behavior control	133
12.1.3 Port power saving	137
12.1.4 Sleep mode.....	138
12.1.5 Cooling fan control functionality (semi-fanless operation) [48T] [48TD].....	142
12.1.6 Scheduling power saving functionality.....	142
12.1.7 Obtaining and displaying power consumption information	148
12.1.8 Notes on using the power saving functionality.....	149
12.2 Configuration of the power saving functionality	153
12.2.1 List of configuration commands	153
12.2.2 Configuring automatic LED behavior control	154
12.2.3 Configuring the power saving functionality for link-down ports.....	154
12.2.4 Configuring the cooling fan control functionality (semi-fanless operation)	154
12.2.5 Configuring scheduled power saving	154
12.3 Operation of the power saving functionality	158
12.3.1 List of operation commands.....	158
12.3.2 Displaying the LED behavior	158
12.3.3 Displaying the status of port power saving control	158
12.3.4 Displaying the cooling fan control status	158
12.3.5 Displaying the schedule status	158
12.3.6 Displaying the information about power consumption	159
13. Software Management	161
13.1 List of operation commands	162
13.2 Updating software	163
13.2.1 Notes on updating software	163
13.3 Registering a license	164
14. Ethernet	165
14.1 Description of information common to all Ethernet interfaces	166
14.1.1 Network configuration example	166
14.1.2 Physical interfaces	166
14.1.3 Control on the MAC and LLC sublayers	167

14.1.4 MAC address of the Switch.....	168
14.1.5 Order of Ethernet frames	169
14.2 Configuration common to all Ethernet interfaces	170
14.2.1 List of configuration commands	170
14.2.2 Configuring a port that has an Ethernet interface.....	170
14.2.3 Configuring multiple ports at one time	171
14.2.4 Shutting down an Ethernet interface.....	171
14.2.5 Configuring jumbo frames.....	172
14.2.6 Configuring the link-down detection timer.....	173
14.2.7 Configuring the link-up detection timer	173
14.3 Operations common to all Ethernet interfaces.....	174
14.3.1 List of operation commands.....	174
14.3.2 Checking the Ethernet operating status.....	174
14.4 Description of the 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces	175
14.4.1 Functionality.....	175
14.4.2 SFP for 10BASE-T/100BASE-TX/1000BASE-T	183
14.5 Configuration of 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces.....	185
14.5.1 Configuring ports.....	185
14.5.2 Configuring flow control	186
14.5.3 Configuring the automatic MDIX functionality.....	186
14.6 Description of the 100BASE-FX interface [24S4X] [24S4XD]	187
14.6.1 Functionality.....	187
14.6.2 SFP for a 100BASE-FX connection.....	189
14.7 Configuration of the 100BASE-FX interface [24S4X] [24S4XD]	190
14.7.1 Configuring ports.....	190
14.7.2 Configuring flow control	190
14.8 Description of the 1000BASE-X interface	191
14.8.1 Functionality.....	191
14.9 Configuration of the 1000BASE-X interface.....	197
14.9.1 Configuring ports.....	197
14.9.2 Configuring flow control	197
14.10 Description of the 10GBASE-R interface [10G model]	198
14.10.1 Functionality.....	198
14.11 Configuration of the 10GBASE-R interface [10G model]	201
14.11.1 Configuring flow control.....	201
14.12 Description of shared SFP/SFP+ ports [10G model]	202
14.12.1 Functionality.....	202
14.13 Configuration of shared SFP/SFP+ ports [10G model].....	203
14.13.1 Configuring ports.....	203
14.13.2 Configuring flow control	203
15. Link Aggregation	205
15.1 Description of the basic link aggregation functionality	206
15.1.1 Overview	206
15.1.2 Link aggregation configuration.....	206
15.1.3 Supported specifications.....	206
15.1.4 MAC address of the channel group	207
15.1.5 Port allocation for sending frames	207
15.1.6 Notes on using link aggregation	207
15.2 Configuration of the basic link aggregation functionality.....	209
15.2.1 List of configuration commands.....	209
15.2.2 Configuring static link aggregation.....	209
15.2.3 Configuring LACP link aggregation.....	210
15.2.4 Configuring a port channel interface.....	211
15.2.5 Deleting a channel group.....	215
15.3 Description of the link aggregation extended functionality.....	217
15.3.1 Standby link functionality.....	217
15.4 Configuration of the link aggregation extended functionality	219

15.4.1 List of configuration commands	219
15.4.2 Configuration of the standby link functionality	219
15.5 Operation for link aggregation.....	221
15.5.1 List of operation commands.....	221
15.5.2 Checking link aggregation information.....	221
16. Layer 2 Switching Overview	225
16.1 Overview	226
16.1.1 MAC address learning	226
16.1.2 VLAN.....	226
16.2 Supported functionality.....	227
16.3 Compatibility between Layer 2 switch functionality and other functionality	228
17. MAC Address Learning	235
17.1 Description of MAC address learning.....	236
17.1.1 Source MAC address learning.....	236
17.1.2 Detecting a move for MAC address learning	236
17.1.3 Aging and MAC address learning	236
17.1.4 Layer 2 switching by MAC address	236
17.1.5 Registering static entries.....	237
17.1.6 Clearing the MAC address table	237
17.1.7 Notes.....	239
17.2 MAC address learning configuration	241
17.2.1 List of configuration commands	241
17.2.2 Configuring the aging time	241
17.2.3 Configuring static entries	241
17.3 MAC address learning operation.....	243
17.3.1 List of operation commands.....	243
17.3.2 Checking the status of MAC address learning.....	243
17.3.3 Checking the MAC address learning count	243
18. VLAN	245
18.1 Description of the basic VLAN functionality	246
18.1.1 VLAN type	246
18.1.2 Port type.....	246
18.1.3 Default VLAN	247
18.1.4 VLAN priority.....	247
18.1.5 VLAN tags	249
18.1.6 Notes on VLAN usage	251
18.2 Configuration of the basic VLAN functionality.....	252
18.2.1 List of configuration commands	252
18.2.2 Configuring VLANs	252
18.2.3 Configuring ports.....	253
18.2.4 Configuring trunk ports.....	253
18.2.5 Configuring TPIDs for VLAN tags	254
18.3 Description of port VLANs	256
18.3.1 Access ports and trunk ports.....	256
18.3.2 Native VLANs.....	256
18.3.3 Notes on port VLAN usage	256
18.4 Configuration of port VLANs	257
18.4.1 List of configuration commands	257
18.4.2 Configuring a port VLAN	257
18.4.3 Configuring native VLANs for trunk ports	258
18.5 Description of protocol VLANs	260
18.5.1 Overview	260
18.5.2 Distinguishing protocols	260
18.5.3 Protocol ports and trunk ports.....	261
18.5.4 Native VLANs for protocol ports.....	261
18.6 Configuration of protocol VLANs.....	262

18.6.1 List of configuration commands	262
18.6.2 Creating protocol VLANs	262
18.6.3 Configuring native VLAN for protocol ports	264
18.7 Description of MAC VLANs	266
18.7.1 Overview	266
18.7.2 Connections between switches and MAC address settings	266
18.7.3 Linkage with the Layer 2 authentication functionality	267
18.7.4 Optional functionality for MAC ports	268
18.8 Configuration of MAC VLANs.....	270
18.8.1 List of configuration commands	270
18.8.2 Configuring MAC VLANs	270
18.8.3 Configuring native VLANs for MAC ports	273
18.8.4 Configuring tagged frame forwarding on a MAC port	273
18.9 VLAN operation	276
18.9.1 List of operation commands.....	276
18.9.2 Checking VLAN status	276
19. VLAN Extended Functionality	281
19.1 Description of VLAN tunneling	282
19.1.1 Overview	282
19.1.2 Requirements for using VLAN tunneling.....	282
19.1.3 Notes on VLAN tunneling usage.....	282
19.2 Configuration of VLAN tunneling.....	284
19.2.1 List of configuration commands	284
19.2.2 Configuring VLAN tunneling	284
19.3 Description of tag translation.....	285
19.3.1 Overview	285
19.3.2 Notes on using tag translation	285
19.4 Configuration of tag translation	286
19.4.1 List of configuration commands	286
19.4.2 Configuring tag translation	286
19.5 Description of L2 protocol frame transparency functionality	288
19.5.1 Overview	288
19.5.2 Notes on L2 protocol frame transparency functionality	288
19.6 Configuration of the L2 protocol frame transparency functionality.....	289
19.6.1 List of configuration commands	289
19.6.2 Configuring the L2 protocol frame transparency functionality	289
19.7 Description of the inter-port relay blocking functionality.....	290
19.7.1 Overview	290
19.7.2 Notes on using the inter-port relay blocking functionality	290
19.8 Configuration of the inter-port relay blocking functionality	292
19.8.1 List of configuration commands	292
19.8.2 Configuring the inter-port relay blocking functionality	292
19.8.3 Changing blocked ports	293
19.9 Operation for the VLAN extended functionality.....	295
19.9.1 List of operation commands.....	295
19.9.2 Checking the VLAN extended functionality.....	295
20. Spanning Tree Protocols	297
20.1 Overview of Spanning Tree Protocols	298
20.1.1 Overview	298
20.1.2 Types of Spanning Tree Protocols	298
20.1.3 Spanning Tree Protocols and rapid Spanning Tree Protocol	299
20.1.4 Configuration components for Spanning Tree topologies	301
20.1.5 Designing Spanning Tree topologies	302
20.1.6 STP compatibility mode	304
20.1.7 Notes common to Spanning Tree Protocols	305
20.2 Configuration of the Spanning Tree operating mode	306

20.2.1 List of configuration commands	306
20.2.2 Configuring the operating mode	306
20.3 Description of PVST+.....	309
20.3.1 Using PVST+ to balance load.....	309
20.3.2 PVST+ for access ports	309
20.3.3 Notes on PVST+ usage	311
20.4 PVST+ configuration	312
20.4.1 List of configuration commands	312
20.4.2 Configuring PVST+	312
20.4.3 Configuring PVST+ topologies.....	313
20.4.4 Configuring PVST+ parameters.....	315
20.5 PVST+ operation	317
20.5.1 List of operation commands.....	317
20.5.2 Checking PVST+ statuses	317
20.6 Description of Single Spanning Tree	318
20.6.1 Overview	318
20.6.2 Usage with PVST+.....	318
20.6.3 Notes on Single Spanning Tree usage	319
20.7 Configuration of Single Spanning Tree.....	320
20.7.1 List of configuration commands	320
20.7.2 Configuring Single Spanning Tree	320
20.7.3 Configuring topologies for Single Spanning Tree.....	321
20.7.4 Configuring Single Spanning Tree parameters	322
20.8 Operation for Single Spanning Tree	325
20.8.1 List of operation commands.....	325
20.8.2 Checking Single Spanning Tree statuses	325
20.9 Description of Multiple Spanning Tree.....	326
20.9.1 Overview	326
20.9.2 Designing networks for Multiple Spanning Tree.....	328
20.9.3 Compatibility with other Spanning Tree Protocols	330
20.9.4 Notes on Multiple Spanning Tree usage	330
20.10 Configuration of Multiple Spanning Tree	332
20.10.1 List of configuration commands	332
20.10.2 Configuring Multiple Spanning Tree.....	332
20.10.3 Configuring topologies for Multiple Spanning Tree	333
20.10.4 Configuring Multiple Spanning Tree parameters.....	335
20.11 Operation for Multiple Spanning Tree.....	338
20.11.1 List of operation commands	338
20.11.2 Checking Multiple Spanning Tree statuses	338
20.12 Description of common Spanning Tree functionality	340
20.12.1 PortFast.....	340
20.12.2 BPDU filter	341
20.12.3 Loop guards	341
20.12.4 Root guards	344
20.13 Configuration of the common Spanning Tree functionality	346
20.13.1 List of configuration commands	346
20.13.2 Configuring PortFast.....	346
20.13.3 Configuring BPDU filters	347
20.13.4 Configuring loop guards.....	348
20.13.5 Configuring root guards	348
20.13.6 Configuring link types.....	349
20.14 Operation for common Spanning Tree functionality	350
20.14.1 List of operation commands.....	350
20.14.2 Checking the status of common Spanning Tree functionality	350
21. Description of the Ring Protocol	353
21.1 Overview of the Ring Protocol.....	354
21.1.1 Overview	354

21.1.2 Features	354
21.1.3 Supported specifications	356
21.2 Basic Ring Protocol principles.....	358
21.2.1 Network configuration	358
21.2.2 Control VLAN	360
21.2.3 Fault monitoring methods	360
21.2.4 Switching communication paths.....	360
21.3 Overview of single ring operation	363
21.3.1 Normal ring operation	363
21.3.2 Operation when a fault is detected	363
21.3.3 Operation when recovery is detected	365
21.3.4 Operation when path switch-back is suppressed and cleared	366
21.4 Overview of multi-ring operation	368
21.4.1 Normal ring operation	368
21.4.2 Operation for shared link faults and restoration	371
21.4.3 Operation for faults and restoration other than for shared links in a shared link non-monitoring ring	372
21.4.4 Faults and restoration other than for shared links in a shared link monitoring ring	374
21.4.5 Operation when path switch-back is suppressed and cleared	376
21.5 Multi-fault monitoring functionality for the Ring Protocol.....	377
21.5.1 Overview	377
21.5.2 Basic configuration for the multi-fault monitoring functionality.....	378
21.5.3 Overview of operation for multi-fault monitoring	378
21.5.4 Operation when multi-faults occur	379
21.5.5 Operation during multi-fault recovery.....	382
21.6 Ring Protocol network design	386
21.6.1 Using VLAN mappings.....	386
21.6.2 Using forwarding-delay-time for control VLANs.....	386
21.6.3 Automatic primary port determination	387
21.6.4 Configurations with mixed node types within the same device	388
21.6.5 Configurations with mixed node types for shared nodes.....	388
21.6.6 Setting fault monitoring times when link aggregation is used	388
21.6.7 Usage with IEEE 802.3ah/UDLD functionality	389
21.6.8 Usage with link-down detection timers and link-up detection timers	389
21.6.9 Prohibited Ring Protocol configurations.....	390
21.6.10 Prohibited configurations for the multi-fault monitoring functionality	391
21.6.11 Configurations in which both ring ports of a master node are shared links	393
21.7 Notes on Ring Protocol usage	395
22. Settings and Operation for Ring Protocol	399
22.1 Configuration	400
22.1.1 List of configuration commands	400
22.1.2 Flow of Ring Protocol settings	401
22.1.3 Configuring ring IDs	401
22.1.4 Configuring control VLANs.....	402
22.1.5 Configuring VLAN mappings	402
22.1.6 Configuring a VLAN group	403
22.1.7 Configuring modes and ring ports (for single rings and multi-ring configurations without shared links)	403
22.1.8 Configuring modes and ring ports (for multi-ring configurations with shared links)	406
22.1.9 Configuring various parameters.....	410
22.1.10 Configuring the multi-fault monitoring functionality.....	412
22.1.11 Configuring flush control frames for neighboring rings	413
22.2 Operation.....	415
22.2.1 List of operation commands.....	415
22.2.2 Checking Ring Protocol statuses	415

23. Using the Ring Protocol with Spanning Tree Protocols/GSRP	419
23.1 Using the Ring Protocol with Spanning Tree Protocols.....	420
23.1.1 Overview	420
23.1.2 Operating specifications.....	421
23.1.3 Compatibility with various Spanning Tree Protocols	424
23.1.4 Prohibited configurations	428
23.1.5 Notes on using the Ring Protocol and Spanning Tree Protocols together	429
23.2 Using the Ring Protocol with GSRP.....	431
23.2.1 Operational overview	431
23.3 Virtual link configuration	433
23.3.1 List of configuration commands	433
23.3.2 Configuring virtual links.....	433
23.3.3 Configuring the Ring Protocol and PVST+ together	433
23.3.4 Configuring the Ring Protocol and Multiple Spanning Tree together.....	434
23.4 Virtual link operation.....	435
23.4.1 List of operation commands.....	435
23.4.2 Checking the status of virtual links	435
24. Description of IGMP Snooping and MLD Snooping	437
24.1 Overview of IGMP snooping and MLD snooping	438
24.1.1 Overview of multicast.....	438
24.1.2 Overview of IGMP snooping and MLD snooping.....	439
24.2 Functionality supported for IGMP snooping and MLD snooping	440
24.3 IGMP snooping.....	441
24.3.1 MAC address control method	441
24.3.2 Connections with multicast routers	442
24.3.3 IGMP querier functionality.....	443
24.3.4 IGMP instant leave	444
24.4 MLD snooping	445
24.4.1 MAC address control method	445
24.4.2 Connections with multicast routers	446
24.4.3 MLD querier functionality	447
24.5 Notes on IGMP snooping and MLD snooping usage	448
25. Settings and Operation for IGMP Snooping and MLD Snooping	451
25.1 Configuration of IGMP snooping	452
25.1.1 List of configuration commands	452
25.1.2 Configuring IGMP snooping.....	452
25.1.3 Configuring the IGMP querier functionality	452
25.1.4 Configuring multicast router ports	453
25.2 IGMP snooping operation	454
25.2.1 List of operation commands.....	454
25.2.2 Checking IGMP snooping	454
25.3 Configuration of MLD snooping.....	456
25.3.1 List of configuration commands	456
25.3.2 Configuring MLD snooping	456
25.3.3 Configuring MLD querier functionality.....	456
25.3.4 Configuring multicast router ports	457
25.3.5 Configuring the source IP address for MLD Query messages	457
25.4 MLD snooping operation	458
25.4.1 List of operation commands.....	458
25.4.2 Checking MLD snooping.....	458
26. IPv4 Interfaces	461
26.1 Description	462
26.2 Configuration	463
26.2.1 List of configuration commands	463
26.2.2 Configuring an interface.....	463
26.2.3 Configuring multihoming	463

26.2.4 Configuring static routes	464
26.2.5 Configuring static ARP	464
26.3 Operation.....	465
26.3.1 List of operation commands.....	465
26.3.2 Checking the up/down status of the IPv4 interface.....	465
26.3.3 Checking the availability of communication with a destination address	465
26.3.4 Checking the route to a destination address	466
26.3.5 Checking ARP information	466
26.3.6 Checking the route table	467
27. IPv6 Interfaces	469
27.1 Description	470
27.2 Configuration	471
27.2.1 List of configuration commands	471
27.2.2 Configuring an interface.....	471
27.2.3 Configuring the default route.....	471
27.2.4 Configuring a static NDP entry.....	472
27.2.5 Configuring settings for automatically generating an IPv6 address by receiving a router advertisement.....	472
27.3 Operation.....	473
27.3.1 List of operation commands.....	473
27.3.2 Checking the up/down status of the IPv6 interface.....	473
27.3.3 Checking the availability of communication with a destination address	473
27.3.4 Checking the route to a destination address	474
27.3.5 Checking NDP information.....	474
28. DHCP Server Functionality.....	475
28.1 Description	476
28.1.1 Supported specifications.....	476
28.1.2 Information distributed to clients	476
28.1.3 Preventing duplicate distribution of IP addresses.....	477
28.1.4 Notes on using the DHCP server functionality.....	477
28.2 Configuration	478
28.2.1 List of configuration commands	478
28.2.2 Settings for distributing IP addresses to clients	478
28.2.3 Settings for distributing static IPs to clients	480
28.3 Operation.....	482
28.3.1 List of operation commands.....	482
28.3.2 Checking the DHCP server	482
A. Supported Standards.....	486
A.1 TELNET/FTP/TFTP	486
A.2 RADIUS	486
A.3 NTP.....	486
A.4 DNS	486
A.5 Ethernet	487
A.6 Link aggregation	487
A.7 VLANs.....	487
A.8 Spanning Tree Protocols.....	487
A.9 IGMP snooping and MLD snooping.....	488
A.10 IPv4 interfaces	488
A.11 IPv6 interfaces	488
A.12 DHCP server functionality.....	489
Index	491

Part 1: Overview and Capacity Limits of the Switch

1 . Overview of the Switch

This chapter describes the features of the Switch.

1.1 Overview of the Switch

1.2 Switch features

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.

The Switches provide flexible options for building a highly reliable, available, and scalable information network infrastructure through their applicability to mission-critical fields.

Product concept

The Switches support gigabit Ethernet and inherit a variety of functionality, such as authentication functionality and power saving functionality from AX1200S series Layer 2 switches that support Fast Ethernet as edge switches.

As a goal, ALAXALA Networks Corporation has continued to develop platforms that embody the concept of a guaranteed network. For example, we have developed platforms for SD card maintenance and power redundancy in Layer 2 switches. The switches described are small box-type LAN switches that not only inherit these platforms with improved performance and extended capacity limits, but also provide extended redundancy and power saving functionality in distribution switches. The switches are products that have been designed with the functionality, switching capability, and cost performance required by corporate networks in mind.

The Switches provide the following functionality:

- Fanless design that reduces operating noise and provides greater resistance to dust. [24T] [24TD]
- Support various types of network redundancy for highly reliable and highly available networking.
- Feature link aggregation and 10 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.

1.2 Switch features

(1) Fanless design [24T] [24TD]

- Fanless design in a gigabit Ethernet Layer 2 switch
- Achieves a quiet office environment with fewer problems caused by dust being taken into the switch

Note that AX2530S-48T and AX2530S-48TD switches are semi-fanless models with fans that operate only when the temperature inside the device rises.

(2) High reliability for configuring mission-critical networks

- High-quality devices
 - High reliability through carefully selected parts and strict design and inspection requirements
 - The power supply system can be made redundant with the use of an external power unit.
- Variety of redundant network configurations
 - SML (Split Multi Link) for low-cost redundancy with a box-type switch.
 - Standard functionality: Link aggregation (IEEE 802.3ad) and rapid Spanning Tree Protocols (IEEE 802.1w and IEEE 802.1s)
 - Proprietary functionality: GSRP aware capability and the Autonomous Extensible Ring Protocol^{#1} (abbreviated hereafter to the Ring Protocol), SML (split multi-link)^{#2}, and uplink redundancy^{#3}

#1

For details about the Ring Protocol, see *21 Description of the Ring Protocol*.

#2

A distribution switch is made redundant to configure link aggregation as a single switch. For details about SML, see *18 SML (Split Multi Link) [OS-L2A]* in the manual *Configuration Guide Vol. 2*.

Use of this functionality requires a separately purchased license.

#3

A redundant configuration can be created without using a Spanning Tree Protocol. For details about uplink redundancy, see *17 Uplink Redundancy* in the manual *Configuration Guide Vol. 2*.

- Layer 2 loop avoidance
 - The UDLD functionality prevents loops at the Spanning Tree Protocol or frame loss at link aggregation.
 - The Layer 2 loop detection functionality detects improperly connected devices on the network, which helps prevent loops.

(3) Power saving

- Scheduling functionality
 - The Switch can automatically switch to and wake up from a sleep state in accordance with schedule settings for long holidays, Saturdays, Sundays, public holidays, and evenings.
 - The LED operation described below and port power saving can be combined by using schedule settings.
 - Even when the Switch is in the sleep state, it can be re-activated remotely by

using functionality that detects WOL packets received from a specific port and functionality that detects the link-up state of a specific port.

- Three different levels of LED control
 - Three different levels of LED brightness control: normal brightness, power saving brightness, (lower brightness than normal), and OFF
 - LEDs can be set to blink or turn on at normal brightness when consoles are connected to a Switch, ports are in the link-up state, and SD memory cards are inserted. The settings can be also changed so that LEDs automatically turn off after the operations are completed.
 - Port power saving
 - Power saving by powering down a port detected to be in a link-down state or configured to be blocked (using the `shutdown` configuration command)[#]
- #
- For SFP ports and shared SFP/SFP+ ports [10G models], only the turning off of the power when the ports are blocked is supported.
- Visualization of power saving information
 - Consumed power and total consumption are displayed with operation commands and MIBs

(4) Network authentication

- Exclusion of unauthorized users
 - Keeping personal PCs, which have no security management, from connecting to a network.
 - Keeping third parties from accessing a network.
- Protecting server information
 - Department servers and other servers that are installed without permission are prohibited from connecting to the network because appropriate access restrictions such as password protection are not in effect on these servers in most cases.
 - Because continuous use of a server that does not restrict access appropriately could lead to information leakage, measures to protect information leakage are implemented on the network side.
 - Users without access permissions are prohibited from accessing a server.

Authentication in dynamic VLAN mode is used.
- Protecting client PCs
 - Client PCs, which tend to be vulnerable to illegal access, are protected from illegal access, which prevents information leaks.
- Traceability in the case of problems
 - The ability to investigate when and where unauthorized access occurred, based on a log of failed authentications.
 - If a network is used improperly, the ability to investigate when and where such improper use occurred, based on a log of successful authentications.
- Authentication in heterogeneous environments with different terminal types
 - Allows network authentication even in heterogeneous environments with different terminal types by supporting three different authentication functionality (IEEE 802.1X authentication, Web authentication, and MAC-based authentication).
 - Support for multistep authentication that only allows network use when a

combination of terminal authentication and user authentication is passed.

- Drastic reduction of total cost
 - Network authentication is possible even when connection occurs via an intermediate hub.

User capacity can be increased at low cost by using intermediate hubs rather than connecting terminals directly to the floor switch.
- One-time password authentication
 - Web authentication by using the RSA SecurID one-time password authentication functionality can improve network access security. PIN code initial registration and token code re-entry are also supported.[#]

#

Use of this functionality requires a separately purchased license.

(5) Quarantine network

- Security checking
 - Information leaks are prevented by isolating PCs that violate security policies, such as PCs on which Winny or other inappropriate software is installed and PCs on which patches have not been installed.
 - The network prohibits access from infected PCs that may compromise information systems on business networks.
 - Operating cost is reduced through central management of terminal security policies on a quarantine server.
- Linkage with several quarantine systems is possible.
 - Microsoft NAP
 - NOSiDE (NTT Data)
 - JP1 (Hitachi, Ltd.)
 - CapsSuite (NEC)

(6) Robust security

- Finely tuned high-performance packet filtering
 - Hardware-based high-performance filtering processes
 - Layer 2, 3, and 4 headers specifiable
 - Scalability accommodating a variety of conditions
- Support for various VLAN types (Tag-VLANs, port VLANs, MAC VLANs, and protocol VLANs)
- Layer 2 - Virtual Private Network (L2-VPN) using VLAN tunneling
- Login and password authentication for the switch are possible via RADIUS
- Exclusion of unauthorized DHCP servers and terminals with fixed IP addresses
 - Robust security measures such as DHCP snooping, which excludes unauthorized DHCP servers and terminals with fixed IP addresses.

(7) Hardware-based, advanced QoS delivered via Ethernet

- High-performance hardware-based QoS processing
- Fine-grain parameter specification as part of layer 2, 3, and 4 headers
- High-precision QoS control
- Wide range of QoS control functionality

L2-QoS (including IEEE 802.1p, bandwidth controls, and priority controls), and IP-QoS (including Diff-Serv[#], and priority controls)

#

Only the marking functionality is supported.

- Wealth of the hierarchical shaper functionality for an integrated voice and data network
 - Clear audio in which VoIP packets are preferentially transmitted.

(8) High-performance, high-density, compact, and environmentally-friendly devices

- Excellent performance
 - Floor edge switches and server farm Layer 2 switches
- Compact chassis
 - Compact chassis with a 1U height
 - High port density of up to 48 10BASE-T/100BASE-TX/1000BASE-T ports.
- RoHS is applied, and the environmental impact is reduced.

(9) User-friendly interface (configuration commands)

- Industry-standard command line interface
 - Use of the same format for input commands and configuration information improves operability.
 - Copy-and-paste operations are supported for configuration information.

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

- CFM (Connectivity Fault Management) (Ether OAM)
Connectivity monitoring and failure management are available at the Layer 2 level by performing continuity checks (CC), loopbacks, and link traces.
- Offers IPv4/IPv6 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 RMON and a new IPv6-compliant ip MIB (RFC 4293).
- 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
- Support for SD memory cards[#]
 - Users can easily back up the configuration and save error information.
 - Maintenance tasks are simplified.

#

In the manuals of this series, an SD memory card is called an MC.

- The Ethernet ports, console port, and the memory card slot are all on the front panel.
- Device cooling method ensuring stable operation
 - Front-side air intake and rear-side air exhaust cooling reduces the impact of other devices on the switch when it is installed in a rack, ensuring stable operation.

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

- More efficient operation 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 the *AX-Config-Master* part in the *OAN User's Guide*.

(12) Excellent cost performance

- Switching capacity sufficient for an enterprise network provides superior performance.
- Low power consumption-oriented architecture design and part selection. This helps to reduce the total cost of ownership (TCO) after implementation.

(13) 10G uplink support [10G models]

- A high-performance 10G LAN can be configured by combining AX2500S series switches with AX7800S, AX6700S, AX6600S, AX6300S, AX3800S, or AX3600S series switches.
- SFP+ is used as an optical transceiver for 10G Ethernet. 1G Ethernet can be changed to 10G Ethernet smoothly by using shared SFP/SFP+ ports.

1 Overview of the Switch

2. Switch Configuration

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

2.1 Switch model range

2.2 Switch components

2.1 Switch model range

The Switches are box-type, 1U-high gigabit Ethernet switches, equipped with a maximum of 48 10BASE-T, 100BASE-TX, and 1000BASE-TX ports.

Each model provides link aggregation, VLAN, Spanning Tree Protocols, DHCP snooping, IGMP snooping, and MLD snooping, and the Layer 2 authentication functionality. In addition, the switch supports advanced filters and QoS functionality, and either wire-rate or non-blocking switching.

The following table matches switch models to maximum number of ports.

Table 2-1 Maximum number of ports and model

Maximum number of ports	Model
24 ports (10BASE-T/100BASE-TX/1000BASE-T) 4 ports (1000BASE-X)	AX2530S-24T (AC model) AX2530S-24TD (DC model)
24 ports (10BASE-T/100BASE-TX/1000BASE-T) 4 ports (1000BASE-X/10GBASE-R)	AX2530S-24T4X (AC model)
48 ports (10BASE-T/100BASE-TX/1000BASE-T) 4 ports (1000BASE-X)	AX2530S-48T (AC model) AX2530S-48TD (DC model)
48 ports (10BASE-T/100BASE-TX/1000BASE-T) 2 ports (1000BASE-X) 2 ports (1000BASE-X/10GBASE-R)	AX2530S-48T2X (AC model)
24 ports (1000BASE-X) 4 ports (1000BASE-X/10GBASE-R)	AX2530S-24S4X (AC model) AX2530S-24S4XD (DC model)

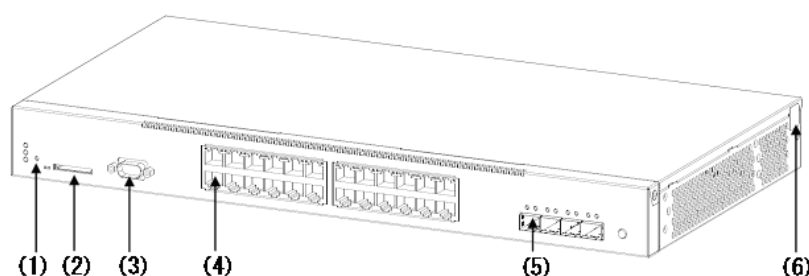
#

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 AX2530S-24T and AX2530S-24TD models

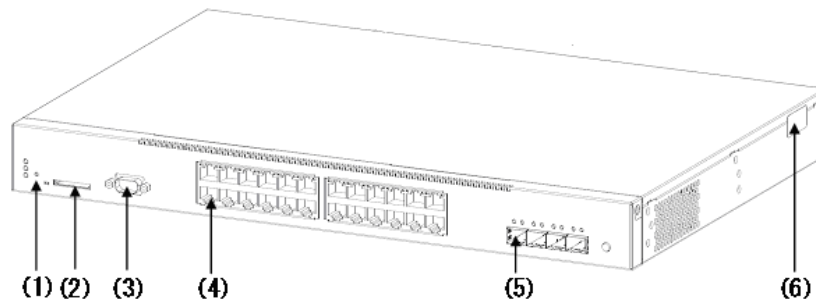


- (1) RESET button
- (2) Memory card slot
- (3) CONSOLE port
- (4) 10BASE-T/100BASE-TX/1000BASE-T Ethernet ports
- (5) SFP slots

(6) Security tape

For details about each component, see the *Hardware Instruction Manual*.

Figure 2-2 AX2530S-24T4X model



(1) RESET button

(2) Memory card slot

(3) CONSOLE port

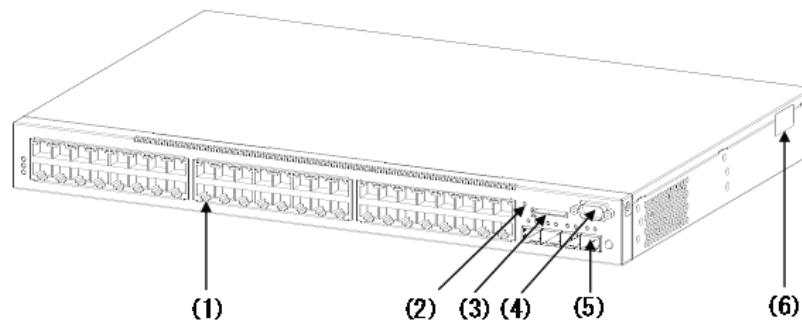
(4) 10BASE-T/100BASE-TX/1000BASE-T Ethernet ports

(5) SFP+ slots

(6) Security tape

For details about each component, see the *Hardware Instruction Manual*.

Figure 2-3 AX2530S-48T and AX2530S-48TD models



(1) 10BASE-T/100BASE-TX/1000BASE-T Ethernet ports

(2) RESET button

(3) Memory card slot

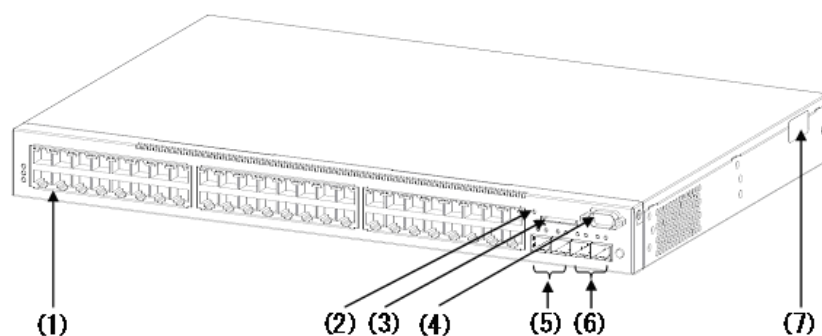
(4) CONSOLE port

(5) SFP slots

(6) Security tape

For details about each component, see the *Hardware Instruction Manual*.

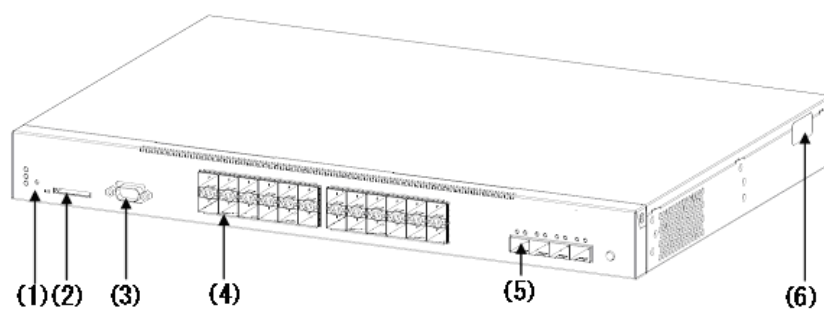
Figure 2-4 AX2530S-48T2X model



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

For details about each component, see the *Hardware Instruction Manual*.

Figure 2-5 AX2530S-24S4X and AX2530S-24S4XD models



- (1) RESET button
- (2) Memory card slot
- (3) CONSOLE port
- (4) SFP slots
- (5) SFP+ slots
- (6) Security tape

For details about each component, see the *Hardware Instruction Manual*.

2.2 Switch components

2.2.1 Hardware

Each Switch model has the same architecture design.

The models that use AC power supplies provide power redundancy through an external redundant power unit (EPU-A).

The models that use DC power supplies have two DC power supply units which can be connected to different sources for power redundancy. The models that use DC power supplies also can provide power redundancy through an external redundant power unit (EPU-D).

The following figures show the hardware configuration.

Figure 2-6 Hardware configuration (AX2530S-24T model)

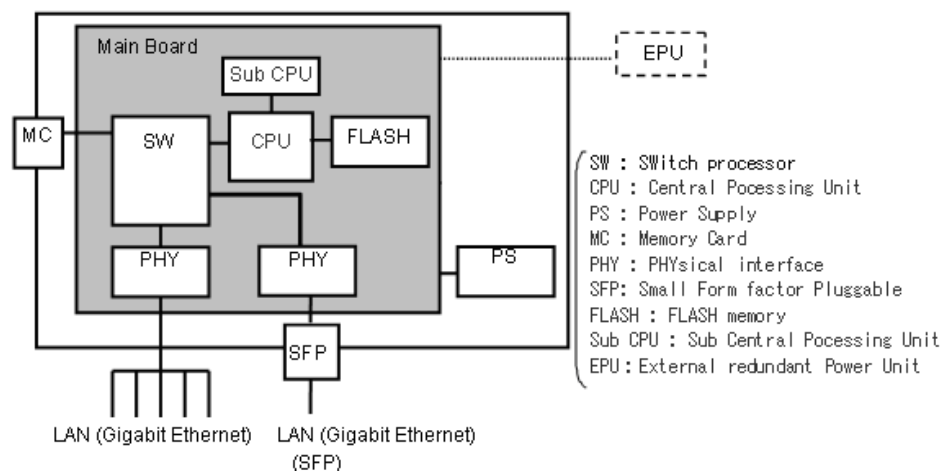
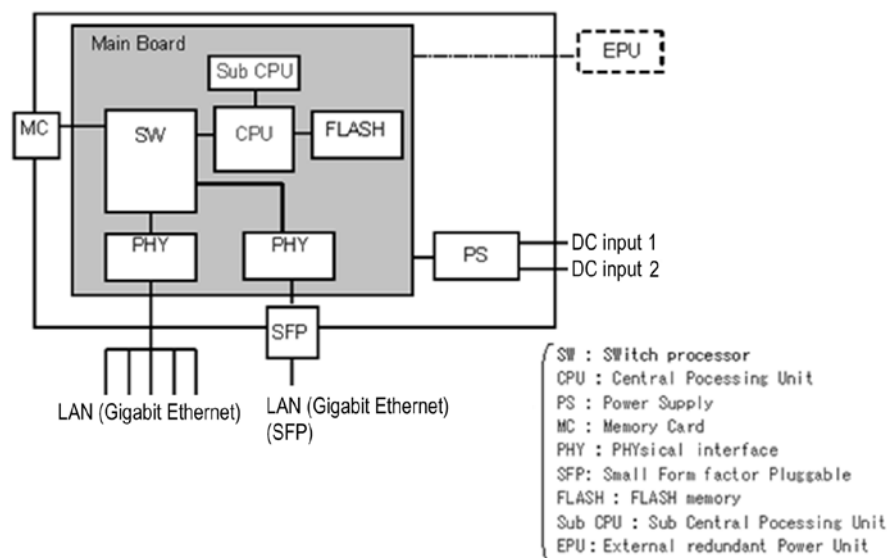


Figure 2-7 Hardware configuration (AX2530S-24TD model)



2 Switch Configuration

Figure 2-8 Hardware configuration (AX2530S-24T4X and AX2530S-48T2X models)

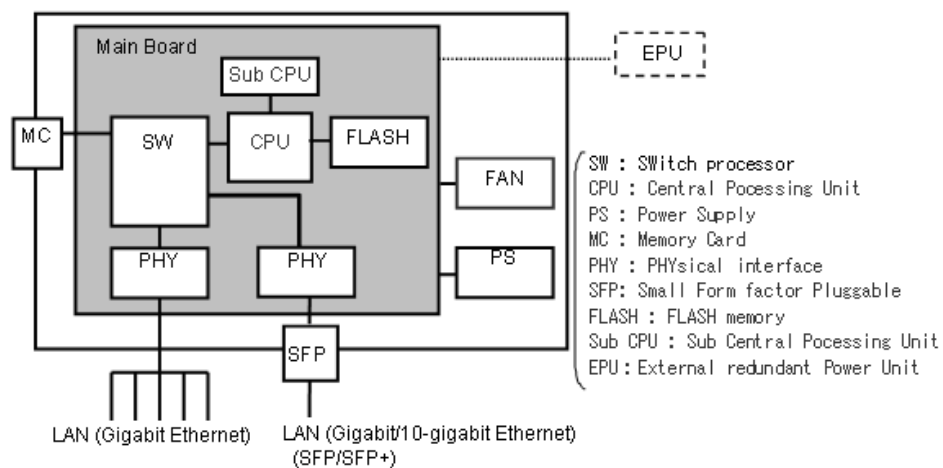


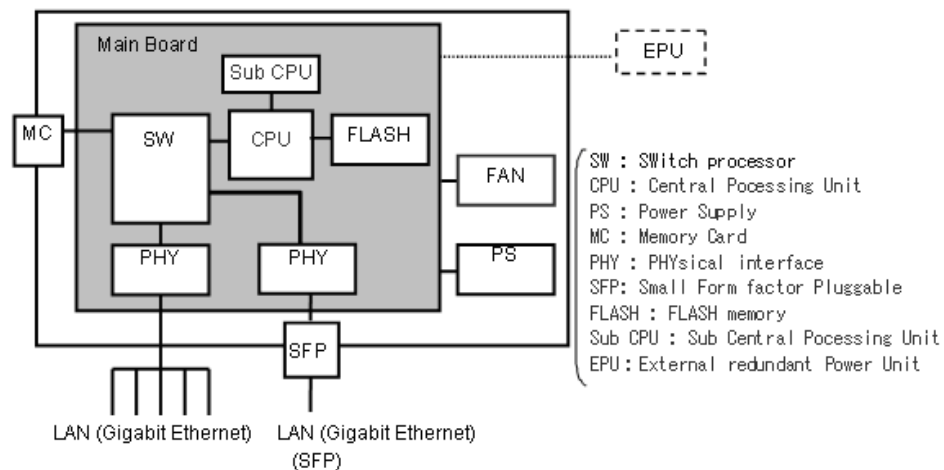
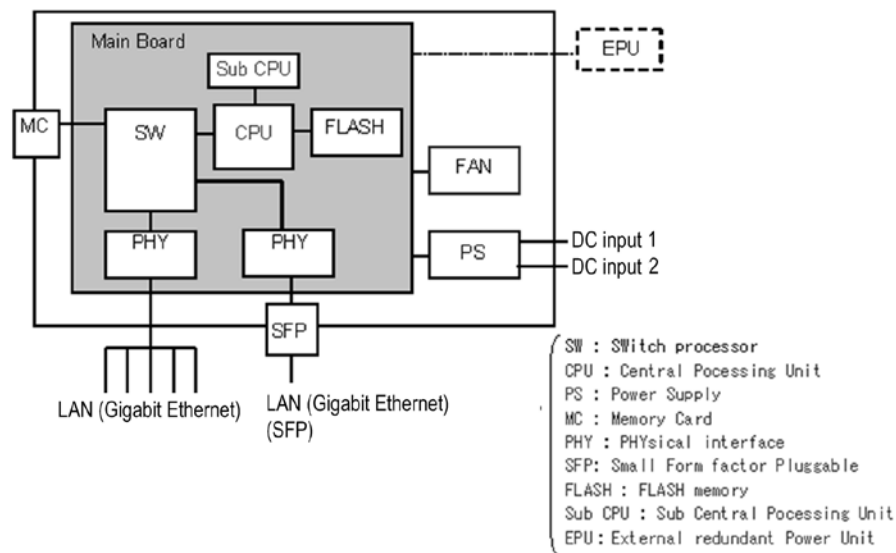
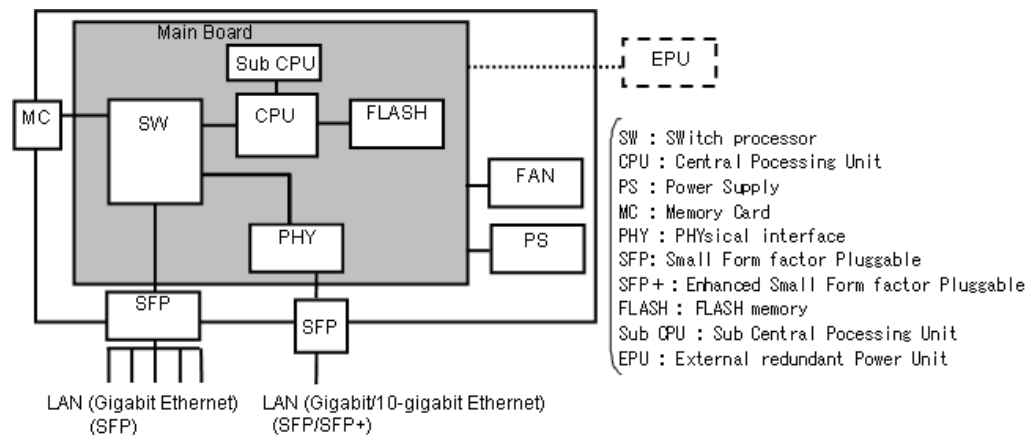
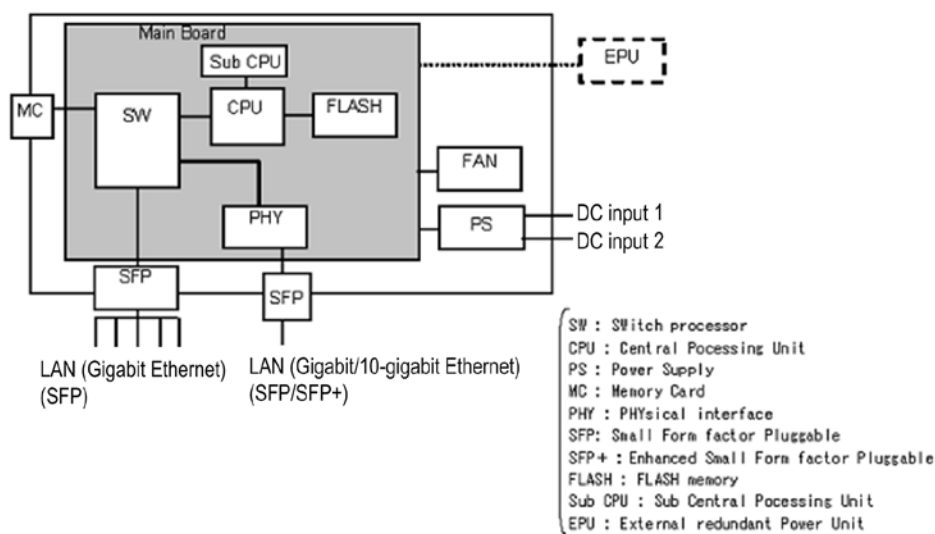
Figure 2-9 Hardware configuration (AX2530S-48T model)**Figure 2-10** Hardware configuration (AX2530S-48TD model)**Figure 2-11** Hardware configuration (AX2530S-24S4X model)

Figure 2-12 Hardware configuration (AX2530S-24S4XD model)



(1) Device chassis

The main board, a power supply (PS) unit and fan are enclosed within the device chassis.

(2) Main board

The main board consists of CPU, SW, MC, Flash, PHY, and Sub-CPU subunits.

- CPU (central processing unit)
 Manages all the hardware, controls PHY subunit, and performs protocol processing via software.
 The software is stored in the Flash subunit's internal flash memory.
- SW (switch processor)
 Handles Layer 2 frame switching. The SW subunit learns hardware MAC addresses, and performs aging, link aggregation, filters, QoS table searches, and DMA forwarding of frames addressed to or originated by the Switch. These functions together enable high-speed frame switching.
- MC (memory card)
 MC slot. An SD card is used as a memory card for storing configuration files and failure information.
- Flash (flash memory)
 Stores software, configuration files, and log data.
- PHY (physical interface)
 An interface subunit supporting various kinds of media.
- Sub-CPU (secondary central processing unit)
 Monitors temperature sensors and fans.

(3) PS (power supply)

A PS converts power from an external source to DC power that can be used inside the Switch. Power supply can be made redundant by connecting an optional EPU. This redundant configuration allows the Switch to continue operating without interruption even if the PS fails. Note that if you need to replace a failed PS, you will have to shut down the Switch, and replace the Switch itself.

For details about how to configure a redundant power supply, see the *Hardware Instruction Manual*.

(4) Fan (for models other than AX2530S-24T and AX2530S-24TD)

Except for some models, the Switch is equipped with fans that cool the inside of the Switch.

- The 48T and 48TD models are semi-fanless models whose fans do not operate at normal temperature (when the cooling fan controller is enabled). These models can be set to ensure that fans will always operate if cooling is critical.
- The fans of models 24T4X, 48T2X, 24S4X, and 24S4XD always operate.

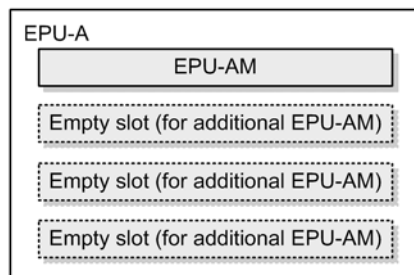
(5) EPU (external redundant power unit)

An EPU is a spare external power supply unit and an optional device for making the Switch power redundant. An EPU-A is provided for AC power supplies, and an EPU-D is provided for DC power supplies. A single power module is installed in one of the EPU slots, and additional power modules can be installed in remaining slots.

An EPU is connected to the Switch with a dedicated cable. An EPU generates the DC power required for the Switch. One EPU can supply power to multiple switches. The EPU has a failure notification function that enables the Switch to monitor the EPU.

The following figure shows an overview of the EPU-A. (EPU-D has the same configuration.)

Figure 2-13 Overview of the EPU-A



2.2.2 Software

The following tables describe the software used for the Switches.

Table 2-2 Software used for the Switch

Abbreviated name	Model name	Description
OS-L2A-A/ OS-L2A	Switching software (advanced L2 version)	Software derived from OS-L2B-A/OS-L2B by applying OS-L2A-U (see <i>Table 2-3</i>). Uses: L2 switch forwarding, VLAN, Spanning Tree Protocols, SNMP, LLDP, Secure Wake-on-LAN, one-time password authentication, and SML, among other uses.
OS-L2B-A/ OS-L2B	Switching software (basic L2 version)	Uses: L2 switch forwarding, VLAN, Spanning Tree Protocols, SNMP, and LLDP, among other uses. Note: Secure Wake-on-LAN, one-time password authentication, and SML are disabled.

Table 2-3 Software (license) used for Switches

Abbreviated name	Model name	Description
OS-L2A-U	Advanced software upgrade license for AX2500S series switches	Enables the following functionality: <ul style="list-style-type: none">● Secure Wake-on-LAN● One-time password authentication (RSA SecurID linkage)● SML (split multi-link)

3. Capacity Limit

This chapter describes the capacity limits for the Switch.

3.1 Line and module capacities

3.2 Capacity limit

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			
	10/100/1000BASE-T	1000BASE-X 1000BASE-T [#]	1000BASE-X 100BASE-FX 10/100/1000BASE-T	10GBASE-R 1000BASE-X 1000BASE-T [#]
	RJ45	SFP	SFP	Shared SFP/SFP+
AX2530S-24T AX2530S-24TD	24	4	--	--
AX2530S-24T4X	24	--	--	4
AX2530S-48T AX2530S-48TD	48	4	--	--
AX2530S-48T2X	48	2	--	2
AX2530S-24S4X AX2530S-24S4XD	--	--	24	4

Legend: --: Not applicable

#

If 10BASE-T, 100BASE-TX, and 1000BASE-T (SFP) lines are connected, 1000BASE-T applies.

3.1.2 Mounted power supply unit

(1) AC models

The AC models contain a power supply unit. In addition, the AC models can provide power redundancy by connecting a spare external power supply unit (an EPU-A).

- AX2530S-24T
- AX2530S-24T4X
- AX2530S-48T
- AX2530S-48T2X
- AX2530S-24S4X

(2) DC models

The DC models contain a power supply unit. In addition, the DC models can provide power redundancy by connecting a spare external power supply unit (an EPU-D).

- AX2530S-24TD
- AX2530S-48TD
- AX2530S-24S4XD

3.1.3 Amount of installed memory

The table below describes the amount of memory installed on the main board and the amount of space available on the memory card. Note that the amount of memory installed on the Switch cannot be increased.

Table 3-2 Amount of memory on the main board, and amount of internal flash memory

Item	AX2530S series switches
Amount of memory on the main board (including the RAMDISK)	512 MB (30 MB is on the RAMDISK.)
Amount of internal flash memory	64 MB

(1) RAMDISK

The RAMDISK can be used as a temporary storage area when data is copied from the Switch to the memory card or a file on the memory card is registered on the Switch.

For example, before you perform the following operations, you can temporarily copy the file to the RAMDISK:

- Example 1: Copy a configuration file from the Switch to the memory card.
- Example 2: After you have created a Web authentication page replacement file on a PC, register the file on the Switch.

After a file has been copied to the memory card or registered on the Switch, the file on the RAMDISK is no longer necessary. Use an operation command to delete the file from the RAMDISK.

Note that restarting the Switch deletes the file on the RAMDISK.

3.2 Capacity limit

3.2.1 Login security and RADIUS

The following table describes the maximum number of logins that are possible from remote operation terminals to a Switch and the maximum number of RADIUS server information entries that can be registered.

Table 3-3 Maximum number of logins that are possible from remote operation terminals to a Switch

Model	Telnet	FTP
All models	16	1

Table 3-4 Maximum number of RADIUS server entries that can be registered

Model	RADIUS server information type	Maximum number of entries that can be registered	Whether the entry can be quoted in the RADIUS server group information	Number of groups that can be registered	Number of servers that can be registered in a RADIUS server group
All models	Information about general-use RADIUS servers	20	Quotable	4/switch	4/group
	Information about RADIUS servers using IEEE 802.1X authentication only	4	Not quotable	--	--
	Information about RADIUS servers using Web authentication only	4	Not quotable	--	--
	Information about RADIUS servers using MAC-based authentication only	4	Not quotable	--	--

Legend: --: Not supported

3.2.2 Link aggregation

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

Table 3-5 Capacity limits for link aggregation

Model	Maximum number of ports per channel group	Maximum number of channel groups per switch
All models	8	64 [#]

#

A physical port cannot be assigned to multiple channel groups. The recommended maximum number of channel groups is 51. Creating more than 51 channel groups might affect device operation.

3.2.3 Layer 2 switch functionality

(1) MAC address table

The Layer 2 switch functionality allows the MAC addresses of any connected hosts to be dynamically learned and registered in the MAC address table. The functionality can also perform static registration in the MAC address table.

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

Table 3-6 Maximum number of entries in the MAC address table

Model	Per switch	
	Maximum number of entries	Number of static entries
All models	32768 [#]	256

#

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, frames 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 3-7 Number of VLANs supported

Model	VLANs per port	VLANs per switch	Total per-port VLANs per switch
AX2530S-24T AX2530S-24TD AX2530S-24T4X AX2530S-24S4X AX2530S-24S4XD	4094	4094	28672
AX2530S-48T AX2530S-48TD AX2530S-48T2X	4094	4094	53248

Notes

We recommend that you configure no more than 1024 VLANs.

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 200 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 2014. 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.

Although a maximum of 4094 VLANs can be configured on a Switch, the maximum number of VLANs (VLAN interfaces) for which an IP address can be set is 128.

(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 number of protocol types that can be configured.

Table 3-8 Number of types of protocols for protocol VLANs

Model	Per port	Per switch
All models	16	16

Table 3-9 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 3-10 Maximum number of MAC addresses in a MAC VLAN

Model	Maximum number of MAC addresses registered by the configuration	Maximum number of MAC addresses registered by Layer 2 authentication functionality	Maximum number of MAC addresses that can be registered concurrently
All models	64	1000	1000 [#]

#

The number of MAC addresses registered by a configuration command is included in the maximum number of MAC addresses registered by Layer 2 authentication functionality.

(c) VLAN tunneling

The following table describes the maximum number of VLANs that can be configured for a trunk port of the switch for which VLAN tunneling is enabled.

Table 3-11 Maximum number of VLAN tunnels

Model	Per switch
All models	4094

(d) Tag translation

The following table describes the number of tag translation entries that can be set by the configuration.

Table 3-12 Maximum number of tag translation entries

Model	Per switch
All models	768 [#]

#

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

(3) Spanning Tree Protocols

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

Table 3-13 Capacity limits for PVST+

Model	Compatible with the Ring Protocol	Number of applicable VLANs	Number of 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 $100 \times 2 = 200$.

#2

Excludes ports that have PortFast enabled.

Table 3-14 Capacity limits for Single Spanning Tree

Model	Compatible with Ring Protocol	Number of applicable VLANs	Number of VLAN ports ^{#1}	Number of VLAN ports ^{#1} (when PVST+ is also used ^{#2})
All models	No	256 ^{#3}	1024	256
	Yes	256 ^{#3}	768	200

#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 $100 \times 2 = 200$.

#2

The total maximum value when PVST+ target ports are included is 256.

#3

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

Table 3-15 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 target VLANs in each MST instance ^{#2}
All models	No	256	1024	16	200
	Yes	256	768	16	200

#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 $100 \times 2 = 200$.

#2

Excludes MST instance 0. The number of target VLANs in MST instance 0 is 256.

(4) Ring Protocol

(a) Ring Protocol

The following table describes the capacity limits for the Ring Protocol.

Table 3-16 Capacity limits for the Ring Protocol

Model	Item	Per ring	Per switch
All models	Number of rings	--	51 ^{#1}
	Number of VLAN mappings	--	128
	Number of VLAN groups	2	102 ^{#2}
	Number of VLANs in a VLAN group	1023 ^{#3, #4}	1023 ^{#3, #4}
	Number of ring ports ^{#5}	2	52

Legend: --: Not applicable

#1

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

#2

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

#3

The maximum number of VLANs that is recommended for the switch.

Although the maximum number of VLANs recommended for the Switch is 1024, one VLAN is always needed as the control VLAN. Therefore, the maximum number of VLANs that can be used for VLAN groups is 1023. As the number of rings increases, the number available for VLAN groups decreases.

#4

Because the multi-fault monitoring functionality uses one VLAN per ring as a multi-fault monitoring VLAN, the maximum number of VLANs that can be used for VLAN groups decreases.

#5

Each channel group is counted as one port.

(b) Virtual links

The following table describes the capacity limits for virtual links.

Table 3-17 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 3-18 Capacity limits for the multi-fault monitoring functionality

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

(5) IGMP snooping and MLD snooping

The tables below show the capacity limits for IGMP snooping and MLD snooping. Multicast MAC addresses learned in IGMP snooping and MLD snooping are registered in the MAC address table. The following table describes the number of multicast MAC addresses that can be registered.

Table 3-19 Capacity limits for IGMP snooping

Model	Item	Maximum number
All models	Number of configurable VLANs	32
	Number of VLAN ports ^{#1}	512
	Number of registered entries ^{#2, #3}	1000

#1

The total number of ports in which IGMP snooping is active (sum of the ports within

3 Capacity Limit

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 sum of the number of multicast MAC addresses learned in each VLAN.

#3

The total number of entries used by IGMP snooping and MLD snooping.

Table 3-20 Capacity limits for MLD snooping

Model	Item	Maximum number
All models	Number of configurable VLANs	32
	Number of VLAN ports ^{#1}	512
	Number of registered entries ^{#2, #3}	1000

#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 sum of the number of multicast MAC addresses learned in each VLAN.

#3

The total number of entries used by IGMP snooping and MLD snooping.

3.2.4 IP interface

On a Switch, an IP address is assigned to a VLAN. This subsection 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 with which the Switch can communicate. It also explains the number of dynamic entries, the number of static entries, and the capacity limit of the DHCP server.

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

The table below shows the maximum number of interfaces supported by the Switch. The values described here are the total for IPv4 and IPv6. IPv4 and IPv6 can be assigned to the same interface, or to separate interfaces.

Table 3-21 Maximum number of interfaces to which IP addresses can be assigned

Model	Maximum number of interfaces to which IP addresses can be assigned (per switch)
All models	128

(2) Maximum number of interfaces that allow VLAN-based reception control to work

The table below shows the maximum number of interfaces that allow VLAN-based reception control to work. When the number of interfaces to which IP addresses have been assigned is less than this maximum number, packets whose destination address is the MAC address of the Switch can be forwarded for VLANs for which IP addresses are not assigned.

If the SML functionality is enabled on the Switch, packets whose destination address is the MAC address of the Switch are not forwarded.

Table 3-22 Maximum number of interfaces that allow VLAN-based reception control to work

Model	Maximum number of interfaces that allow VLAN-based reception control to work (per switch)
All models	32

(3) Maximum number of multihomed subnets

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

(a) IPv4 address

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

Table 3-23 Maximum number of multihomed subnets (IPv4)

Model	Maximum number of multihomed subnets for IPv4 (per interface)
All models	128

(b) IPv6 address

The following table describes the maximum number of multihomed subnets for IPv6. The value does not include the number of default link-local addresses and the number of IPv6 addresses that are automatically generated when receiving router advertisements.

Table 3-24 Maximum number of multihomed subnets (IPv6)

Model	Maximum number of multihomed subnets for IPv6 (per interface)
All models	7

(4) Maximum number of IP addresses**(a) IPv4 address**

The table below describes the maximum number of IPv4 addresses that can be set per switch using a configuration command.

Table 3-25 Maximum number of IPv4 addresses that can be assigned on a switch using a configuration command

Model	Maximum number of IPv4 addresses that can be assigned using a configuration command (per switch)
All models	128

(b) IPv6 address

The table below describes the maximum number of IPv6 addresses that can be set per switch by the configuration. This value indicates the maximum number of IPv6 addresses that can be configured for communication interfaces. The value does not include the number of default link-local addresses and the number of IPv6 addresses that are automatically generated when receiving router advertisements.

Table 3-26 Maximum number of IPv6 addresses that can be set for a switch by the configuration

Model	Maximum number of IPv6 addresses that can be set by the configuration (per switch)
All models	128

(5) Maximum number of IPv6 addresses and IPv6 default gateways automatically generated when receiving router advertisements

The table below shows the maximum number of IPv6 addresses and IPv6 default gateways that are automatically generated when receiving router advertisements in the IPv6 environment.

Table 3-27 Maximum number of IPv6 addresses and IPv6 default gateways automatically generated when receiving router advertisements

Model	IPv6 prefixes (per interface)	IPv6 default gateways (per switch)
All models	2	2

(6) Maximum number of remote devices

The maximum number of remote devices with which a Switch can communicate through the connected LAN is described below. Remote devices include not only routers, but also terminals.

(a) Number of ARP entries

For IPv4 in a LAN, ARP determines a hardware address that corresponds to the destination address of a frame being sent. Therefore, the maximum number of remote devices for this media depends on the number of ARP entries. The following table describes the maximum number of ARP entries supported by a Switch.

Table 3-28 Maximum number of ARP entries

Model	Number of ARP entries	
	Per interface	Per switch
All models	2048	2048

Notes

The number of static ARPs is 128.

(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. The following table describes the maximum number of NDP entries supported by the Switch.

Table 3-29 Maximum number of NDP entries

Model	Number of NDP entries	
	Per interface	Per switch
All models	256	256

Notes

The number of static NDP entries is 128.

(7) Maximum number of dynamic entries and static entries

The table below shows the maximum number of dynamic entries and static entries.

Note that a Switch supports only static routing, and does not support RIP/RIPng, OSPF/OSPFv3, and other routing protocols.

Table 3-30 Maximum number of dynamic entries and static entries

Category	Item	Maximum number of entries per switch	Maximum number of dynamic entries	Maximum number of static entries
IPv4	Unicast path entry	128 [#]	--	128 [#]
IPv6	Unicast path entry	1 [#]	--	1 [#]

Legend: --: Not supported

#: Does not include the number of direct routes.

(8) DHCP server

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

Table 3-31 Capacity limits for the DHCP server

Model	Item	Maximum number
All models	Number of DHCP server interfaces	64
	Number of subnets managed on the DHCP server	64
	Number of IP addresses that can be distributed	1024
	Number of fixed IP addresses that can be distributed	80
	Number of addresses that are not subject to distribution	1024

#

Includes the number of fixed IP addresses that can be distributed.

3.2.5 Filters and QoS

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 filters and QoS. Select a flow detection mode to determine resource allocation based on the detection conditions for filters and QoS. 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.

- **flow detection mode** configuration command: Sets the receiving-side flow detection mode.
- **flow detection out mode** configuration command: Sets the sending-side flow detection mode.

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

(1) Number of filter entries on the receiving side

The table below describes the maximum number of filter entries on the receiving side that can be set when you select **layer2-1**, **layer2-2**, or **layer2-3** as the receiving-side flow detection mode. The flow detection conditions that can be used depend on the selected mode. If **layer2-1** is selected, MAC conditions can be used. If **layer2-2** is selected, IPv4 conditions can be used. If **layer2-3** is selected, IPv4 conditions and IPv6 conditions can be used.

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

Model	Receiving-side flow detection mode	Interface type	Maximum number of filter entries on the receiving side [#]					
			Per interface			Per switch		
			MAC conditions	IPv4 conditions	IPv6 conditions	MAC conditions	IPv4 conditions	IPv6 conditions
All models	layer2-1	Ethernet	256	--	--	256	--	--
		VLAN	256	--	--	256	--	--
	layer2-2	Ethernet	--	256	--	--	256	--
		VLAN	--	256	--	--	256	--
	layer2-3	Ethernet	--	256	128	--	256	128
		VLAN						

Legend: --: Not applicable

[#]

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: One entry is set for Ethernet interface 0/1.

Number of entries: Two entries (the entry to be set and the discard entry for

Ethernet interface 0/1) are used.

Number of remaining entries:

$$\text{maximum-number-of-filter-entries-on-the-receiving-side} - \text{number-of-entries}$$

Example 2:

Entry condition: Two entries are set for Ethernet interface 0/1, and three entries are set for Ethernet interface 0/2.

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

Number of remaining entries:

$$\text{maximum-number-of-filter-entries-on-the-receiving-side} - \text{number-of-entries}$$

(2) Number of QoS entries on the receiving side

The table below describes the maximum number of receiving-side QoS entries that can be set when you select **layer2-1**, **layer2-2**, or **layer2-3** as the receiving-side flow detection mode. The flow detection conditions that can be used depend on the selected mode. If **layer2-1** is selected, MAC conditions can be used. If **layer2-2** is selected, IPv4 conditions can be used. If **layer2-3** is selected, IPv4 conditions and IPv6 conditions can be used.

Table 3-33 Maximum number of receiving-side QoS entries

Model	Receiving-side flow detection mode	Interface type	Maximum number of QoS entries on the receiving side					
			Per interface			Per switch		
			MAC conditions	IPv4 conditions	IPv6 conditions	MAC conditions	IPv4 conditions	IPv6 conditions
All models	layer2-1	Ethernet	128	--	--	128	--	--
		VLAN	128	--	--	128	--	--
	layer2-2	Ethernet	--	128	--	--	128	--
		VLAN	--	128	--	--	128	--
	layer2-3	Ethernet	--	128	64	--	128	64
		VLAN	--	128	64	--	128	64

Legend: --: Not applicable

(3) Number of filter entries on the sending side

The table below describes the maximum number of sending-side filter entries that can be set when you select **layer2-1-out**, **layer2-2-out**, or **layer2-3-out** as the sending-side flow detection mode. The flow detection conditions that can be used depend on the selected mode. If **layer2-1-out** is selected, MAC conditions can be used. If **layer2-2-out** is selected, IPv4 conditions can be used. If **layer2-3-out** is selected, MAC conditions, IPv4 conditions, and IPv6 conditions can be used.

Table 3-34 Maximum number of sending-side filter entries

Model	Receiving-side flow detection mode	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
All models	layer2-1-out	Ethernet	128	--	--	128	--	--
		VLAN	128	--	--	128	--	--
	layer2-2-out	Ethernet	--	128	--	--	128	--
		VLAN	--	128	--	--	128	--
	layer2-3-out	Ethernet	128	128	128	128	128	128
		VLAN						

Legend: --: Not applicable

(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 and QoS flow detection conditions. These patterns refer to hardware resources that are used with the port settings in a flow detection condition.

Table 3-35 Capacity limits for the TCP/UDP port number detection patterns

Model	Receiving-side flow detection mode	Maximum number per switch
All models	layer2-1	--
	layer2-2	16
	layer2-3	16

Legend

--: Receiving-side flow detection mode that does not use TCP/UDP port number detection patterns

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 3-36 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	
		layer 2-1	layer 2-2 layer 2-3	layer 2-1-out	layer 2-2-out layer 2-3-out
Source port number	Single specification (eq)	Not specifiable	--	Not specifiable	--
	Range specification (range)	Not specifiable	Y	Not specifiable	Not specifiable
Destination port number	Single specification (eq)	Not specifiable	--	Not specifiable	--
	Range specification (range)	Not specifiable	Y	Not specifiable	Not specifiable

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. Patterns are shared between multiple filter entries and multiple QoS entries.
2. Patterns are shared between TCP and UDP in the flow detection conditions.
3. Patterns are not shared between source and destination port numbers in the flow detection conditions.
4. Patterns are shared between IPv4- and IPv6-based flow detection conditions.

The following table describes examples of using TCP/UDP port number detection patterns. These examples assume [layer 2-2](#) as the receiving-side flow detection mode.

Table 3-37 Usage examples of the TCP/UDP port number detection patterns

Pattern usage example [#]	Number of patterns used
Filter entry: <ul style="list-style-type: none"> ● Source port range (10 to 30) Filter entry: <ul style="list-style-type: none"> ● Source port range (10 to 40) 	Because a different range is specified in the two entries, the following two patterns are used: <ul style="list-style-type: none"> ● Source port range(10 to 30) ● Source port range (10 to 40)
Filter entry: <ul style="list-style-type: none"> ● No source port number specified ● Destination port range (10 to 20) Filter entry: <ul style="list-style-type: none"> ● No source port number specified ● Destination port range (10 to 20) QoS entry: <ul style="list-style-type: none"> ● No source port number specified ● Destination port range (10 to 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 one following pattern is used: <ul style="list-style-type: none"> ● Destination port range (10 to 20)

Pattern usage example [#]	Number of patterns used
QoS entry: <ul style="list-style-type: none"> ● TCP specified ● Source port range (10 to 30) ● No source port number specified QoS entry: <ul style="list-style-type: none"> ● UDP specified ● Source port range (10 to 30) ● No source 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 to 30). Therefore, the following one pattern is used: <ul style="list-style-type: none"> ● Source port range (10 to 30)
QoS entry: <ul style="list-style-type: none"> ● Source port range (10 to 20) ● Destination port range (10 to 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: <ul style="list-style-type: none"> ● Source port range (10 to 20) ● Destination port range (10 to 20)

Legend

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 functionality

(1) Common to Layer 2 authentication types

The following table describes the maximum number of authenticated terminals allowed on an entire switch.

Table 3-38 Number of authenticated terminates allowed on an entire switch

Authentication mode	Authentication functionality	Number of terminals per authentication functionality ^{#1}	Number of terminals allowed on the switch ^{#1}	Limit on the number of terminals that can be authenticated			
				Per port	Per switch		
Fixed VLAN mode	IEEE 802.1X	1024	1024	1024 ^{#3}	1024 ^{#4}		
	Web authentication	1024					
	MAC-based authentication	1024					
Dynamic VLAN mode	IEEE 802.1X	1000	1000 ^{#2}				
	Web authentication	1000					
	MAC-based authentication	1000					
Maximum total number of terminals for all authentication functionality and modes within the entire switch			1024				

^{#1}

If the DHCP snooping functionality is also used, the maximum becomes 500.

#2

If the limit on the number of terminals that can be authenticated is set to 1000 or a greater value, in dynamic VLAN mode, no more than 1000 terminals can be authenticated.

#3

The limit applies to the total number of terminals that can be authenticated in fixed VLAN mode and dynamic VLAN mode for all authentication functionality (IEEE 802.1X, Web authentication, and MAC-based authentication) on the port.

#4

The limit applies to the total number of terminals that can be authenticated in fixed VLAN mode and dynamic VLAN mode for all authentication functionality (IEEE 802.1X, Web authentication, and MAC-based authentication) on the entire switch.

Table 3-39 Other capacity limits common to Layer 2 authentication types

Item	Maximum number
Number of general-use RADIUS servers that can be registered	20 ^{#1}
Access list name that can be specified for the IPv4 access list used for authentication	1
Number of filter conditions that can be specified for the IPv4 access list used for authentication	250 ^{#2}
Maximum number of authentication-failed terminals that can be registered	256 ^{#3}

#1

The number of registrations indicates the number for the entire switch, which includes the login security functionality.

#2

If the specified number of filter entries exceeds the capacity limit, only those entries that are within the capacity limit are applied.

#3

When the number of authentication-failed terminals exceeds the maximum number, the terminal with the oldest update date is deleted so that the new failed terminal can be registered.

(2) IEEE 802.1X

The tables below describe the capacity limits for IEEE 802.1X authentication.

Table 3-40 Maximum number of terminals that can be authenticated by IEEE 802.1X authentication[#]

Authentication mode		Per port	Entire switch
Port-based authentication	(static)	1024	1024
	(dynamic)	1000	1000
Maximum number of terminals in all IEEE 802.1X authentication modes		1024	1024

#

The limit on the number of terminals that can be authenticated applies to all Layer 2 authentication types. Also see *Table 3-38 Number of authenticated terminates*

3 Capacity Limit

allowed on an entire switch.

Note that if the DHCP snooping functionality is also used, the maximum becomes 500.

Table 3-41 Capacity limits for IEEE 802.1X authentication

Item		Maximum number
Number of registered authentication method groups	Device default	1
	Authentication method list	4
Number of registered RADIUS servers using IEEE 802.1X authentication only ^{#1}		4
Maximum number of physical ports for IEEE 802.1X	All models	Maximum number of physical ports on the switch
Maximum number of exempted terminals for the authentication-exempted terminal option	MAC address table static registration	256/switch ^{#2}
	MAC address static registration in MAC VLAN	64/switch ^{#3}

#1

For RADIUS accounting servers, the capacity limits for authentication RADIUS servers (RADIUS servers using IEEE 802.1X authentication only or general-use RADIUS servers) applies.

#2

Number of static entries in the MAC address table

#3

Maximum number of MAC addresses registered by the configuration for MAC VLAN capacity limits

(3) Web authentication

The following tables describe the capacity limits for Web authentication.

Table 3-42 Maximum number of users that can be authenticated by Web authentication[#]

Authentication mode	Per port	Entire switch
Fixed VLAN mode	1024	1024
Dynamic VLAN mode	1000	1000
Maximum number of users that can be authenticated in all Web authentication modes	1024	1024

#

The limit on the number of terminals that can be authenticated applies to all Layer 2 authentication types. Also see *Table 3-38 Number of authenticated terminals allowed on an entire switch.*

Note that if the DHCP snooping functionality is also used, the maximum becomes 500.

Table 3-43 Capacity limits for Web authentication

Item		Maximum number
Number of registered authentication method groups	Device default	1
	Authentication method list	4
Number of registered RADIUS servers using Web authentication only ^{#1}		4
Number of users registered in the internal Web authentication DB		300 ^{#2}
Total size of files that can be specified for the replaceable Web authentication page		1024 KB/switch ^{#3}
	Number of registered custom file sets ^{#4} for the Web authentication page	5/switch Breakdown One for the basic Web authentication page Four for individual Web authentication pages
	Number of files per file set	100

#1

For RADIUS accounting servers, the capacity limits for authentication RADIUS servers (RADIUS servers using Web authentication only or general-use RADIUS servers) applies.

#2

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 user authentications can be authenticated. If, however, the number of user IDs to be authenticated is larger than that of the maximum number of registered user IDs in the internal Web authentication DB, use RADIUS authentication that uses a RADIUS server.

#3

This value is the total size of the file for the basic Web authentication page and the files for the individual Web authentication pages. Because the file area includes a management area, the actual available size is less than 1024 KB.

#4

For details about custom file sets, see *8 Description of Web Authentication* in the manual *Configuration Guide Vol. 2*.

(4) MAC-based authentication

The following tables describe the capacity limits for MAC-based authentication.

Table 3-44 Maximum number of terminals that can be authenticated by MAC-based authentication[#]

Authentication mode	Per port	Entire switch
Fixed VLAN mode	1024	1024

3 Capacity Limit

Authentication mode	Per port	Entire switch
Dynamic VLAN mode	1000	1000
Maximum number of terminals in all MAC-based authentication modes	1024	1024

#

The limit on the number of terminals that can be authenticated applies to all Layer 2 authentication types. Also see *Table 3-38 Number of authenticated terminates allowed on an entire switch*.

Note that if the DHCP snooping functionality is also used, the maximum becomes 500.

Table 3-45 Capacity limits for MAC-based authentication

Item		Maximum number
Number of registered authentication method groups	Device default	1
	Authentication method list	4
Number of registered RADIUS servers using MAC-based authentication only [#]		4
Number of MAC addresses registered in the internal MAC-based authentication DB		1024

#

For RADIUS accounting servers, the capacity limits for authentication RADIUS servers (RADIUS servers using MAC-based authentication only or general-use RADIUS servers) applies.

(5) Secure Wake-on-LAN [OS-L2A]

The following table describes the capacity limits for the Secure Wake-on-LAN functionality.

Table 3-46 Capacity limits for the Secure Wake-on-LAN functionality

Item	Maximum number
Number of concurrent users	32 ^{#1}
Number of terminals that can be registered in the internal DB used to register terminals from which the activation command can be sent	300
Number of terminals that can be registered in the internal DB for user authentication	300
Number of combinations of users and terminals	300 ^{#2}

#1

The time during which a Secure Wake-on-LAN user is managed is the period of time from the time the user is authenticated to the time terminal startup is confirmed.

Therefore, if the timeout value for confirming startup of the internal DB of terminals from which the activation command can be sent is too long, the entries that manage

the number of concurrent users might reach saturation. In that case, the Secure Wake-on-LAN functionality can no longer be used.

#2

The upper limit on the number of combinations of users and terminals is 300. For example, if you allowed one user to access 300 terminals, then no more access rights to other terminals can be set for the user. The settings of [any](#) and [manual](#) are excluded from this limit.

3.2.7 DHCP snooping

The following table describes the capacity limits for DHCP snooping.

Table 3-47 Capacity limits for DHCP snooping

Item	Maximum number
Number of configurable VLANs	64
Total number of entries in the binding database	500
Number of static entries in the binding database	128 [#]

#

The number of static entries is included in the total number of entries in the binding database.

3.2.8 High reliability function based on redundant configurations

(1) Uplink redundancy

The following tables describe the capacity limits for uplink redundancy.

Table 3-48 Capacity limits for uplink redundancy

Model	Number of uplink ports	Number of interfaces allowed per up-link port
AX2530S-24T AX2530S-24TD AX2530S-24T4X AX2530S-24S4X AX2530S-24S4XD	14	2
AX2530S-48T AX2530S-48TD AX2530S-48T2X	26	2

Table 3-49 Capacity limits for the MAC address update functionality

Model	Maximum number of outgoing MAC address entries
All models	1024

(2) SML [OS-L2A]

The following tables describe the capacity limits for SML.

Table 3-50 Capacity limits for the peer link

Model	Maximum number of ports that can be specified for the peer link	Combinations of ports that can be specified for the peer link
AX2530S-24T AX2530S-24TD AX2530S-24T4X AX2530S-24S4X AX2530S-24S4XD	2	Ports 0/25 to 0/26 or ports 0/27 to 0/28
AX2530S-48T AX2530S-48TD AX2530S-48T2X	2	Ports 0/49 to 0/50 or ports 0/51 to 0/52

Table 3-51 Capacity limits for SML ChGrS

Model	Limit per SML switch		Limit for two SML pseudo-switches	
	Maximum number of ports per channel group	Maximum number of channel groups per switch	Maximum number of ports that can belong to the same channel group number across two SML pseudo-switches	Maximum number of channel groups that can have the same channel group number across two SML pseudo-switches
All models	8	64 ^{#1}	8 ^{#2}	64 ^{#3}

#1

A physical port cannot be assigned to multiple channel groups. The recommended maximum number of channel groups is 51. Creating more than 51 channel groups might affect switch operation.

#2

A maximum of eight ports can belong to one SML ChGr across two SML switches.

For example, the number of ports on the two devices does not need to be the same, as shown below.

- One port on SML switch A + seven ports on SML switch B = eight ports across two switches
- Three ports on SML switch A + five ports on SML switch B = eight ports across two switches

#3

All of the 64 channel groups that can be set per SML switch can be used as SML ChGrS that have the same channel group number across two SML switches.

3.2.9 High reliability function based on network failure detection

(1) IEEE 802.3ah/UDLD

The following table describes the capacity limits for IEEE 802.3ah/UDLD.

Table 3-52 Capacity limits for IEEE 802.3ah/UDLD

Model	Maximum number of link monitoring information items
All models	Maximum number of physical ports on the switch

(2) L2 loop detection

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

Table 3-53 L2 loop detection frame transmission rate

Model	L2 loop detection frame transmission rate (per switch)
All models	20 (packets/sec.) ^{#1}

Formula for calculating the number of ports and VLANs from which L2 loop detection frames can be sent:

$$\frac{\text{total-number-of-L2-loop-detection-frame-destinations}^{\#2}}{\text{L2-loop-detection-frame-transmission-rate-(packets/sec.)} \leq \text{transmission-interval-(sec.)}}$$

#1

Frames whose transmission rate exceeds 20 (packets/sec.) will not be sent. Loop failures cannot be detected on target ports or VLANs from which frames have not been sent.

#2

$$\frac{\text{number-of-ports-that-send-L2-loop-detection-frames} \times \text{number-of-VLANs-that-send-L2-loop-detection-frames}}{\text{transmission-interval-(sec.)}}$$

(3) CFM

The following tables describe the capacity limits for CFM.

Table 3-54 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

For channel groups, one ring port is counted per channel group. 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. These maximums change if you change the CCM sending interval. The following table describes the

3 Capacity Limit

capacity limits for total CFM ports and total remote MEPs according to the set CCM sending interval.

Table 3-55 Capacity limits based on different CCM sending intervals

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	100/switch	640/switch
	1 second	50/switch	64/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 3-56 Capacity limits of physical ports and channel groups for CFM

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 3-57 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 256/route

#

Information for a maximum of 256 devices can be retained per route. 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 Neighboring device information (LLDP)

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

Table 3-58 Capacity limits for storing neighboring device information (LLDP)

Item	Maximum capacity
LLDP neighboring device information	52

4. Login Procedures

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

4.1 Operation terminal-based management

4.2 Starting the switch

4.3 Login and logout

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 an RS232C port, and a remote operation terminal is a terminal connected via an IP network. The Switch also supports network management by an SNMP manager via 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

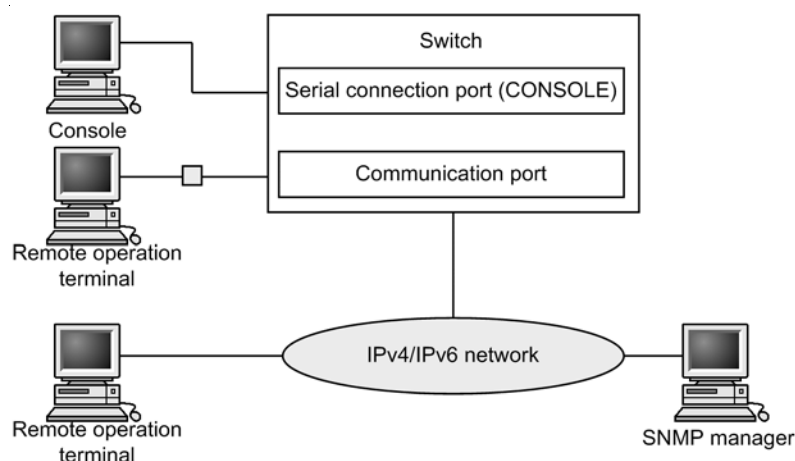


Table 4-1 Functional requirements of operation terminals

Terminal type	Connection method	Required specifications
Console	Serial port (RS232C)	RS232C port (line speed: 19200, 9600, 4800, 2400, or 1200)
Remote operation terminal	Communication port	TCP/IP Telnet FTP

Note The Switch recognizes **CR** as the line feed code. Note, however, that some terminals send **CR** and **LF** as the line feed code. If such terminal connects to the Switch, unnecessary blank lines might be displayed on a terminal. In this case, check the terminal settings.

(1) Console

The console connects via an RS232C port 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 length: 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. Then, in the terminal software, change the communication speed to the same speed you set on the Switch side.

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

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

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. Make sure you use the console terminal in VT-100 mode.
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 to perform command operations. Any terminal that has Telnet client functionality can be used as a remote operation terminal.

Note

If the Telnet connection is closed on the terminal side when, for example, settings are changed or a link-down state on the connected port is detected, the terminal might be unable to reconnect for about 10 minutes.

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

Operation functionality	Serial	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

Operation functionality	Serial	Communication port
Access control	None	Yes
Command input	Supported	Supported
File transfer protocol	None	FTP
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

Operation functionality	Description
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 via Telnet login.
Logs and statistics	Shows information such as past failures and statistics about the packet counter.
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.

Operation functionality	Description
Memory card tools	Perform tasks such as formatting memory cards.

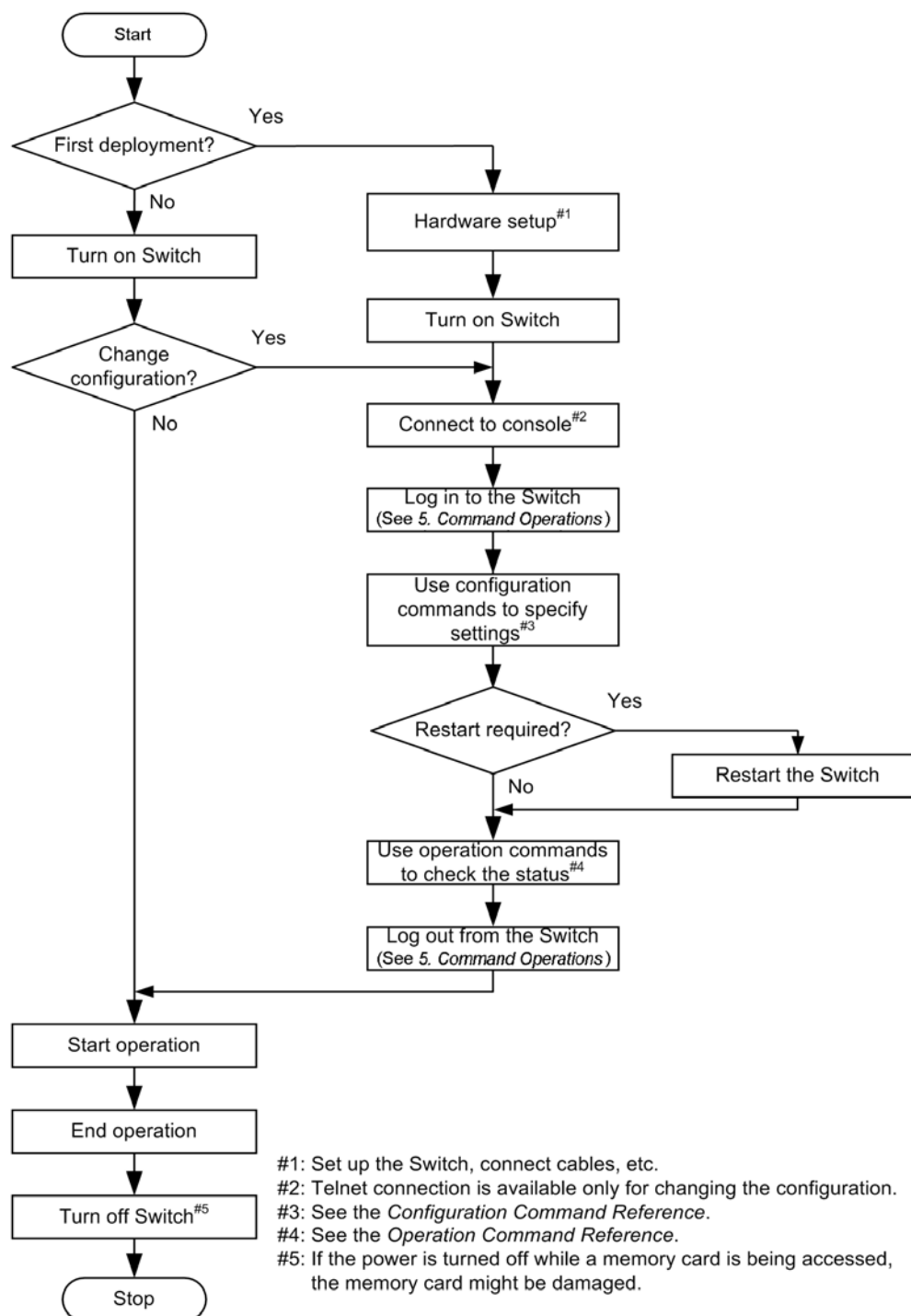
4.2 Starting the switch

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 operation command.

[#]

Press the RESET button of the Switch even when the Switch power supply has been made redundant with the connection of an external redundant power unit (EPU).

If the ST1 LED 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*.

If you start the Switch when a memory card that contains a software image file [k.img](#) is inserted in the memory card slot, the Switch boots from the memory card.

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.

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 ID 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 using the user ID **operator**, without needing a password.

Figure 4-4 Login page

```
login: operator
Password:                                     ... 1

Copyright (c) 2010-2011 ALAXALA Networks Corporation. All rights reserved.

>                                           ... 2
```

1. The **Password:** line is displayed only if a password has been set.
The characters typed following **Password:** are not displayed.
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 specified period (default: 60 minutes). You can change the auto-logout time by using the **set exec-timeout** operation command.

5. Command Operations

This chapter describes how to specify commands on the Switch.

5.1 Command input mode

5.2 CLI operations

5.3 Notes on CLI

5.1 Command input mode

5.1.1 List of operation commands

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

Table 5-1 List of operation commands

Command name	Description
<code>enable</code>	Changes the command input mode from user mode to administrator mode.
<code>disable</code>	Changes the command input mode from administrator mode to user mode.
<code>exit</code>	Ends the current command input mode.
<code>logout</code>	Logs out from the device.
<code>configure(configure terminal)</code>	Changes the command input mode from administrator mode to configuration command mode, and starts configuration editing.
<code>end</code>	Ends configuration command mode, and returns to administrator mode.

5.1.2 Command input mode

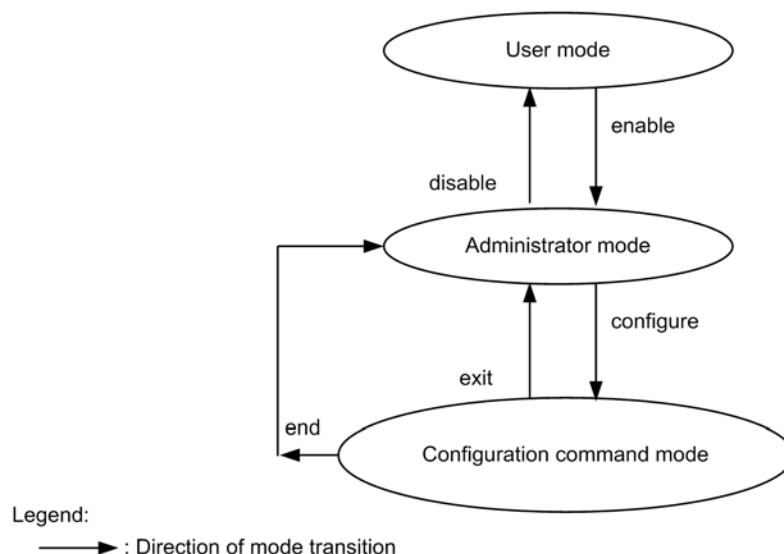
To change the configuration or check the status of the Switch, you must move to the appropriate command input mode, and then enter a configuration command or operation command. From the CLI prompt, you can tell which command input mode you are in.

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 <code>configure</code> , can only be executed in administrator mode.)	>
Administrator mode		#
Configuration command mode	Configuration commands	(config) #

The following figure shows an overview of mode transitions.

Figure 5-1 Overview of mode transitions

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

1. If you set a host name using the `hostname` configuration command, that host name precedes the prompt.
2. If you edit the running configuration but do not save it in the startup configuration file, an exclamation mark (!) appears in front of the prompt.

The following figure shows an example of displaying prompts in these two cases.

Figure 5-2 Example of displaying prompts

```

> enable
# configure
(config)# hostname "OFFICE1"
!OFFICE1(config)# end
!OFFICE1# copy running-config startup-config
Do you wish to copy from running-config to startup-config? (y/n): y
OFFICE1#
  
```

After the configuration has been edited or saved, if a Switch restart is required, an at mark (@) appears at the beginning of the prompt line. If an at mark appears, enter the `reload` operation command to restart the switch.

Figure 5-3 Example of displaying prompts (with @ displayed)

```

OFFICE1# configure
OFFICE1(config)# limit-queue-length 728
Please execute the reload command after save,
because this command becomes effective after reboot.
!OFFICE1(config)# end
!OFFICE1# copy running-config startup-config
Do you wish to copy from running-config to startup-config? (y/n): y
@OFFICE1# reload
Restart OK? (y/n): y
  
```

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 5-4 Simplified command input using command line completion

```
(config)# in[Tab]
(config)# i nterface
```

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

```
(config)# interface [Tab]
gigabitethernet      port-channel      range      vlan
(config)# i nterface
```

Notes

Items that cannot be entered might be displayed. For the items that can be entered for a command, see the input format and the specifiable range for the command in the manual *Configuration Command Reference* and in the manual *Operation Command Reference*.

5.2.2 Help

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 5-5 Example of Help display by entering a question mark

```
> show vlan ?
<VLAN ID list>      - [1-4094] ex. "5", "10-20" or "30,40"
<Display option>    - {detail | list | summary}
channel-group-number - Display the VLAN information specified by channel-group-number
id                  - A part of VLAN ID
mac-vlan            - Display the MAC VLAN information
port                - Display the VLAN information specified by port number

<cr>
> show vlan
```

Notes

1. Items that are not enclosed in angle brackets (<>) might be displayed as parameter names.
2. Items that cannot be entered might be displayed. For the items that can be entered for a command, see the input format and the specifiable range for the command in the manual *Configuration Command Reference* and in the manual *Operation Command Reference*.

If you type a question mark in a parameter without entering a preceding space, command line completion will activate.

5.2.3 Entry-error location detection functionality

If you enter a command or parameter incorrectly, an error message is displayed on the next line. For details on error messages, see *42 Error Messages Displayed When Editing the*

Configuration in the manual *Configuration Command Reference*. This functionality also works when the **Tab** key is pressed or a question mark (?) is typed.

Check and re-enter the command or parameter, referring to the error message. *Figure 5-6 Display example when a parameter (gigabitethernet) is misspelled* and *Figure 5-7 Display example when a parameter (duplex) is missing* show display examples of entry errors.

Figure 5-6 Display example when a parameter (gigabitethernet) is misspelled

```
(config)# interface gigabtiethernet 0/1 [Enter]
                ^
Error: Invalid parameter.
(config)#
```

Figure 5-7 Display example when a parameter (duplex) is missing

```
(config)# interface gigabitethernet 0/1
(config-if)# duplex [Enter]
                ^
Error: Missing parameter.
(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 5-8 Example of abbreviated-command execution (show ip arp command)

```
> sh ip ar [Enter]

Date 2010/09/14 20:04:23 UTC
Total: 2

```

IP Address	Link layer Address	Interface	Expi re	Type
10.0.0.55	0013.20ad.0155	VLAN2048	20mi n	arpa
10.0.0.56	0013.20ad.0156	VLAN2048	20mi n	arpa

```
>
```

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 5-9 Simplified command input using the history functionality

```
> ping 192.168.100.2 interval 2 count 1 packet size 120 ... 1
PING 192.168.100.2 (192.168.100.2): 120 data bytes
128 bytes from 192.168.100.2: icmp_seq=0 ttl=128 time=0 ms

---- 192.168.100.2 PING Statistics ----
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max = 0/0/0 ms
> ... 2
> ping 192.168.100.2 interval 2 count 1 packet size 120 ... 3
PING 192.168.100.2 (192.168.100.2): 120 data bytes
128 bytes from 192.168.100.2: icmp_seq=0 ttl=128 time=0 ms

---- 192.168.100.2 PING Statistics ----
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max = 0/0/0 ms
> ... 4
> ping 192.168.100.3 interval 2 count 1 packet size 120 ... 5
```

5 Command Operations

```
PING 192.168.100.3 (192.168.100.3): 120 data bytes
128 bytes from 192.168.100.3: icmp_seq=0 ttl=128 time=0 ms
```

```
----192.168.100.3 PING Statistics----
1 packets transmitted, 0 packets received, 100.0% packet loss
>
```

1. Execute the **ping** command on 192.168.100.2.
2. Press the up arrow key to call the preceding command.

In this example, pressing the up arrow key once displays the line **ping 192.168.100.2 interval 2 count 1 packet size 120**. Simply press the **Enter** key to re-execute this command.

3. Execute the **ping** command on 192.168.100.2.
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 arrow key once displays the line **ping 192.168.100.2 interval 2 count 1 packet size 120**. Change **2** in the IP address to **3**, and then press the **Enter** key.

5. Execute the **ping** command on 192.168.100.3.

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 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 can be enabled or disabled by executing the **set terminal pager** operation command.

5.2.7 Keyboard command functionality

The keys available with the keyboard command functionality differ according to the terminal application and the terminal settings. For each Switch, we recommend that you use only the following key combinations whose specifications have been clarified by the VT-100 standard.

Table 5-3 Recommended keyboard commands

Key	Switch behavior
Backspace	Deletes the character to the left of the cursor. Note that this key command does not work if there are no characters preceding the cursor on the line.
Ctrl + A	Moves the cursor to the beginning of the command line.
Ctrl + B	Moves the cursor one character left. Note that this key command does not work if there are no characters preceding the cursor on the line.
Ctrl + C	Cancels command execution.
Ctrl + D	Deletes the character to the right of the cursor.
Ctrl + E	Moves the cursor to the end of the command line.
Ctrl + F	Moves the cursor one character right. Note that this key command does not work if there are no characters following the cursor on the line.

Key	Switch behavior
Ctrl + L	Refreshes the console screen so that everything other than the command line is deleted.
Ctrl + N	Shows the next character string in the history (up to the current command).
Ctrl + P	Shows the previous character string in the history.
Ctrl + U	Deletes the text on the line on which the cursor is positioned.
Ctrl + W	Deletes all characters in a word from the beginning of the word to the cursor position. Example: <code>!> show sysversion</code> : For the above entry, if you position the cursor before the character <code>v</code> , and press Ctrl + W , the characters <code>sys</code> preceding the cursor are deleted, as shown below. <code>!> show version</code>
Ctrl + Z	Configuration command mode ends, and you are returned to administrator mode.
Ctrl + K	Deletes the text following the cursor.
Ctrl + T	Replaces the current character with the previous character.
Esc + B	Moves the cursor one word left.
Esc + F	Moves the cursor one word right.
Esc + D	Deletes all characters in a word from the cursor position to the end of the word.

5.2.8 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 functionality 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

This CLI environment information can be set by executing the following operation commands.

- `set exec-timeout`
- `set terminal pager`

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. To check the settings, use the `show users` operation command.

5 Command Operations

When a user restarts the Switch by using an account added by the `adduser` operation command with the `no-flash` parameter specified, the CLI environment information for the user is reset to the defaults for an initial installation.

5.3 Notes on CLI operation

(1) Restrictions that apply after login

If an operation terminal crashes, the user's login status is sometimes retained in the Switch. If this occurs, wait for the user to be automatically logged out.

(2) Display restrictions applying to command line completion and Help functionality

For some commands, display restrictions apply to command line completion and Help functionality.

If an error occurs when one of these commands is entered, see either the manual *Configuration Command Reference* or the manual *Operation Command Reference*, and re-enter the command correctly.

The explanation in this section uses the following terms:

- Variable: Parameter that is an arbitrary number or character string
- Literal: Parameter that is a fixed character string

(a) When a variable is followed by a literal

Input format: *command* *<variable>* *literal*

Following *<variable>*, it might be possible to enter a literal that is not allowed or the command line completion functionality might generate a literal that is not allowed. In either case, an error occurs when the **Enter** key is pressed.

Figure 5-10 Example when a literal that cannot be entered is displayed

```
(config)# spanning-tree mst 5 [?]
configuration          - Configure the common information used by each MST instance of multiple spanning tree, and enter MST configuration mode
forward-time          - Specify the time which state changes take to a bridge interface
hello-time            - Specify a BPDU transmitting interval
max-age               - Specify the maximum time holding the received protocol information
max-hops                 - Specify the maximum number of hop about BPDU
root                     - Specify a root
transmission-limit    - Specify the maximum number of BPDU which can be transmitted for one second
```

```
(config)# spanning-tree mst 5
```

Normally, when you enter *spanning-tree mst 5* and press the **?** key, the Help functionality displays literals and parameters that can be entered. In actuality, however, the functionality also displays literals that are not allowed (underlined bold strings), as shown above.

Accordingly, an error occurs if you press the **Enter** key after entering *spanning-tree mst 5 configuration*.

(b) When a command takes multiple variables but no literals

Input format: *command* [*<variable>*] [*<variable>*]...

For a command that takes multiple parameters enclosed in square brackets (**[]**) but no literals, parameters that are not allowed might be included in the parameter list displayed by Help or pressing the **Tab** key.

Figure 5-11 Example when the command takes multiple variables enclosed in square brackets but no literals

```
(dhcp-config) # lease 360 [?]
<Time hour>          - [0-23]
<Time min>           - [0-59]
<Time sec>           - [0-59]
<cr>
```

```
(dhcp-config) # lease 360 [Tab]
```

```
<cr>                <Time hour>      <Time min>      <Time sec>
```

Normally, when you enter `lease 360` (the `lease` command with the number of days specified) and press the `?` key, the Help functionality displays parameters that can be entered. In actuality, however, the functionality also displays a parameter that is not always enterable (underlined bold string), as shown above.

(c) When a variable and a literal can be entered at the same position

When a variable and a literal can be entered at the same position, the command assumes a string rather than a literal. Therefore, when you want to enter a variable, if the first characters you type are identical to the first characters of a literal that the command can take, the command line completion functionality produces the literal.

The examples below show when a parameter is recognized as a literal and when a parameter is recognized as a variable.

Figure 5-12 When command line completion treats a variable as a literal

```
(config) # aaa authentication mac-authentication
<List name>          - Specify the RADIUS server list name 1 to 32 character
                      s
default              - Specify default mac authentication mechanism
(config) # aaa authentication mac-authentication de ("de" is recognized as a literal.)
group                - Specify mac authentication mechanism using RADIUS pro
                      tocol
local                - Specify mac authentication mechanism using local pass
                      word
```

In the above example, `de` is entered as the `<List name>` variable. However, because `de` is the same as the first two characters of the literal `default`, which can occupy the same position as `<List name>`, the command line completion functionality assumes `default`, and displays a list of items that can be entered following `default`.

Figure 5-13 Example when a variable is treated as a variable

```
(config) # aaa authentication mac-authentication device ("device" is recognized as a variable.)
group                - group <Group name>: Specify mac authentication mechan
                      ism using RADIUS protocol
(config) # aaa authentication mac-authentication device
```

In the above example, `device` is entered as the `<List name>` variable. In this case, because `device` is not the same as the first six characters of literal `default`, which can occupy the same position as `<List name>`, the command line completion functionality assumes `device`, and displays a list of items that can be entered following `<List name>`.

(d) Limit on the number of characters in commands and parameters displayed in Help

For commands and parameters that are 24 or more characters, the 24th and subsequent characters are not displayed in Help.

Figure 5-14 Example when the limit on the number of characters that can be displayed in Help applies

```
(config) # switchport-backup
startup-active-port-sel - Specify the mode of active port selection pattern at
```


startup

(config) #

In the above example, `startup-active-port-sel`, which is displayed as Help information for `switchport-backup`, is actually `startup-active-port-selection`. Because the actual form has 24 or more characters, only the first 23 characters are displayed.

(e) When only some literals, one of which is to be selected, take an additional parameter

If only some literals, one of which is to be selected, take an additional parameter, items that are not always enterable might be displayed as Help information or as candidates for entry. If you enter a candidate that is not allowed for the selected literal, an error occurs when you press the **Enter** key.

Figure 5-15 Example when only some literals, one of which is selected, take an additional parameter

```
(config) # snmp-server host 10.0.0.1 traps ABC
version                - version {1 | 2c | 3}: Specifies SNMP trap version
security level       - {noauth | auth | priv}: Specify SNMP Security Level
snmp                   - SNMP traps send
rmon                   - RMON traps send
air-fan                - Air fan stop traps send
power                  - Power failure traps send
login                  - Login traps send
temperature            - Temperature trap sends
storm-control          - Storm-control trap sends
efmoam                 - IEEE802.3ah/UDLD trap sends
dot1x                  - 802.1X traps send
web-authentication     - Web authentication traps send
mac-authentication     - MAC authentication traps send
loop-detection         - L2 loop detection trap sends
switchport-backup     - Uplink-redundant traps send
cfm                    - CFM traps send
<cr>
```

Normally, when you enter `snmp-server host 10.10.0.1 traps ABC` and press the ? key, the Help functionality displays literals and parameters that can be entered. In actuality, however, the functionality also displays a parameter that is not always enterable (underlined bold string), as shown above. (The `security level` parameter can be specified only when `3` is selected for `version`.)

In this case, an error occurs when you press the **Enter** key after entering `snmp-server host 10.10.0.1 traps ABC auth`.

(f) Restrictions on Help display and command line completion for the deny, permit, and qos configuration commands

The following restrictions apply to the Help display and command line completion for the configuration command `deny` or `permit` (except for `ip access-list standard`) and the configuration command `qos`.

- Display of the command input format as Help information

If the `<source ipv4>`, `<source ipv6>`, or `<source mac>` parameter is specified, the command input format is displayed as Help information for all subsequent parameters as shown in the following figure.

Figure 5-16 Example when the input format is displayed as Help information (for ip access-list extended)

```
(config-ext-nacl) # permit
<protocol>          - 0-255, ah, esp, gre, icmp, igmp, ip, ipinip, ospf, pcp, pim, sctp, tcp, tunnel, udp, vrrp
(config-ext-nacl) # permit ip
```

```
<PARAMs: input format> - permit <protocol> {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} [*1] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [*2][*3][*4] {[tos <tos>] [precedence <precedence>] | dscp <dscp>} [vlan <vlan id>] [user-priority <priority>] NOTE: *1: (TCP/UDP)- {eq <source port> | range <source port start> <source port end>} *2: (TCP/UDP)- {eq <destination port> | range <destination port start> <destination port end>} *3: (ICMP)- [{<icmp type> [<icmp code>] | <icmp message>}] *4: (TCP)- [ack][fin][psh][rst][syn][urg]
```

- When <cr> is displayed in the Help information

Normally, the Help functionality displays <cr> when entry reaches the end. However, for the **deny**, **permit**, and **qos** configuration commands, <cr> might also be displayed before entry is complete. If you press the **Enter** key when <cr> appears, but command entry is incomplete, an error occurs. If this type of error occurs, see either the *Configuration Command Reference* or the *Operation Command Reference*, and re-enter the command correctly.

Figure 5-17 Example when <cr> is displayed although command entry is incomplete (for ip access-list extended)

```
config-ext-nacl)# permit ip any host
<PARAMs: input format> - permit <protocol> {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} [*1] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [*2][*3][*4] {[tos <tos>] [precedence <precedence>] | dscp <dscp>} [vlan <vlan id>] [user-priority <priority>] NOTE: *1: (TCP/UDP)- {eq <source port> | range <source port start> <source port end>} *2: (TCP/UDP)- {eq <destination port> | range <destination port start> <destination port end>} *3: (ICMP)- [{<icmp type> [<icmp code>] | <icmp message>}] *4: (TCP)- [ack][fin][psh][rst][syn][urg]

<cr>
```

- Restrictions on command line completion

If the <source ipv4>, <source ipv6>, or <source mac> parameter appears, command line completion has no effect on the subsequent items.

Figure 5-18 Example when command line completion has no effect (for ip access-list extended)

```
(config-ext-nacl)# permit i
icmp                igmp                ip                ipinip

(config-ext-nacl)# permit ip a => "a" is not converted to "any".
```

(g) Input format when the command contains multiple instances of the <interface id list> variable

Input format: **monitor session** <session no.> **source interface** <interface id list> [{rx | tx | both}] **destination interface** <interface id list>

For commands that contain multiple instances of the <interface id list> variable (as shown above), regardless of whether a delimiter (a comma) is entered after the port number specified for the second and subsequent instances of the <interface id list> variable, you can set an interface type or you can end the command without setting anything, which is not what is supposed to happen.

Figure 5-19 Help display that should be displayed and possible operations when the first instance of the <interface id list> variable is entered

```
(config) # monitor session 1 source interface gigabitethernet 0/1
<monitor frames>          - {rx | tx | both}: Set monitor of receiving frames / mon
                           itor of transmitting frames / monitor of receiving and
                           transmitting frames
destination                - Specify a mirrored port

(config) # monitor session 1 source interface gigabitethernet 0/1,
gigabitethernet            - gigabitethernet <interface no. list> : The type of a
                           port is specified in 10BASE-T/100BASE-TX/100BASE-FX/1
                           00BASE-T/1000BASE-X line ex. "0/1", "0/2-4"
tengigabitethernet         - tengigabitethernet <interface no. list> : The type of
                           a port is specified in 1000BASE-T/1000BASE-X/10GBASE
                           -R line ex. "0/25-26", "0/25"
```

In the above example, the parameter to be specified next is displayed in the help message when no comma is entered for the delimiter after the port number. The interface types (gigabitethernet and tengigabitethernet) that can be specified next are displayed in the help message when a comma is entered for the delimiter after the port number.

Figure 5-20 Help display that should not be displayed and possible operations when the second instance of the <interface id list> variable is entered (without a comma after the port number)

```
(config) # monitor session 1 source interface gigabitethernet 0/1, gigabitethernet 0/3
rx destination interface gigabitethernet 0/11
gigabitethernet          - The type of a port is specified in 10BASE-T/100BASE-TX/
                           100BASE-FX/1000BASE-T/1000BASE-X line
tengigabitethernet       - The type of a port is specified in 1000BASE-T/1000BASE-
                           X/10GBASE-R line
<cr>
```

Figure 5-21 Help display that should not be displayed and possible operations when the second instance of the <interface id list> variable is entered (with a comma after the port number)

```
(config) # monitor session 1 source interface gigabitethernet 0/1, gigabitethernet 0/3
rx destination interface gigabitethernet 0/11,
gigabitethernet          - The type of a port is specified in 10BASE-T/100BASE-TX/
                           100BASE-FX/1000BASE-T/1000BASE-X line
tengigabitethernet        - The type of a port is specified in 1000BASE-T/1000BASE-
                           X/10GBASE-R line
<cr>
```

When no comma is entered for the second instance of the <interface id list> variable, only <cr> (which indicates that no more information can be entered) should be displayed for the help display. However, the interface types (gigabitethernet and tengigabitethernet) are also displayed in the help message and can be specified as shown in the bold and underlined text in the above figure.

When a comma is entered after the port number, <cr> (which indicates that no more information can be entered) should not be displayed. However, <cr> is also displayed in the help message and can be specified as shown in bold and underlined text the above figure.

The following figures show the execution results of the show command in these situations.

Figure 5-22 Execution results of the show command when a comma is entered for the second instance of the <interface id list> variable

```
(config) # monitor session 1 source interface gigabitethernet 0/1, gigabitethernet 0/3
rx destination interface gigabitethernet 0/11,
```

```
(config) # show
monitor session 1 source interface gigabitethernet 0/1, gigabitethernet 0/3 rx
destination interface gigabitethernet 0/11 ⇒ Displayed without any comma
```

Figure 5-23 Execution results of the show command when no comma is entered for the second instance of the <interface id list> variable

```
(config) # monitor session 1 source interface gigabitethernet 0/1, gigabitethernet 0/3
rx destination interface gigabitethernet 0/11 interface gigabitethernet 0/13
(config) # show
monitor session 1 source interface gigabitethernet 0/1, gigabitethernet 0/3 rx
destination interface gigabitethernet 0/11, interface gigabitethernet 0/13 ⇒
Displayed with a comma
```

(h) Restrictions when an omissible parameter is specified when deleting a configuration setting

Input format: *command* <parameter> [*optional parameters*]

If you specify an omissible parameter in a command for deleting a configuration and the parameter value is outside the valid range, parameters that cannot currently be entered are shown in the Help display or in the command list displayed when you press the **Tab** key.

Figure 5-24 Example of displaying parameters that cannot be entered

```
(config) # no ip dhcp excluded-address 192.168.0.1 127.0.0.1 ⇒ Out of range
<High address> - Last address of an excluded range ⇒ Parameter that cannot
be input
<cr>
```

In this state, if you press the **Enter** key, deletion is executed, ignoring the omissible parameter.

In the above example, the **no ip dhcp excluded-address 192.168.0.1** command is executed, so the setting of **ip dhcp excluded-address 192.168.0.1** is deleted.

(i) Command line completion and the Help display for "no"

Keyword **no**, which can be used to negate a setting, among other things, is not included in the Help information displayed by pressing the **?** key or in the command list displayed by pressing the **Tab** key. Command line completion performed by pressing the **Tab** key does not support **no**.

(3) Entry in configuration mode

In a level-2 configuration mode, you will not be able to enter global configuration mode (level-1 configuration mode) commands. Before entering these commands, enter the **exit** command to return to global configuration mode.

(4) Console (RS232C) settings

Make sure you use the console terminal in VT-100 mode, the screen size (terminal size) of which is 80 (columns) x 24 (rows).

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

6.2 Overview of editing a running configuration

6.3 Mode transitions when entering configuration commands

6.4 Configuration editing procedures

6.5 Configuration operations

6.1 Configuration

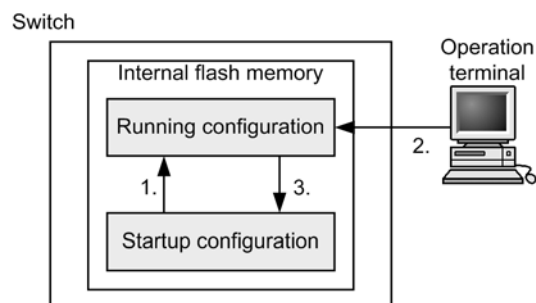
Both at deployment and during operation, the administrator will need to perform configuration settings relating to the connected network and the operating conditions of the Switch. The switch configuration is not predefined at initial deployment.

6.1.1 Configuration at startup

When you power on the Switch, the startup configuration file in internal flash 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 file. It is updated automatically when you edit the running configuration and then execute the **save (write)** configuration command or the **copy** operation command. The following figure shows 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 of the Switch, the startup configuration file of the internal flash memory is read and the operation starts.
2. Any changes to the configuration are reflected in the running configuration.
3. The new running configuration is saved in the startup configuration file.

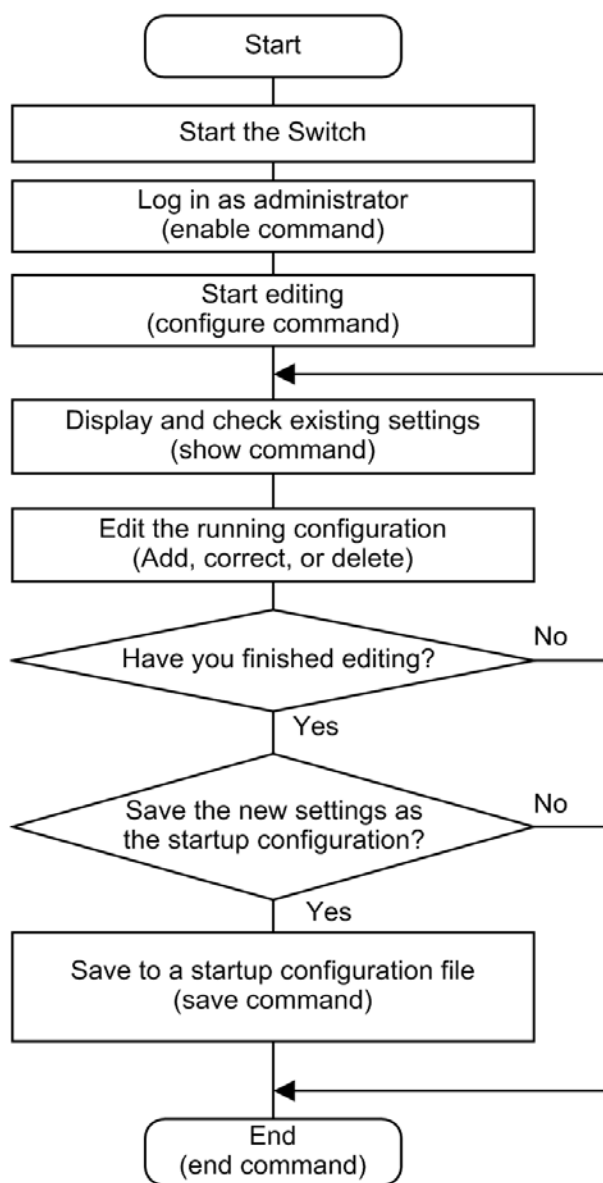
6.1.2 Configuration during operation

When you edit a configuration during operation, the edited contents are immediately applied as the running configuration. By executing the **save (write)** configuration command or the **copy** operation command, you can save the running configuration as the startup configuration file in the switch's internal flash memory. Note that the edited contents will be lost if you restart the 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 shows an overview of transition between configuration modes.

Figure 6-3 Overview of configuration mode transition

Global configuration mode (Level-1)	Mode transition commands	Configuration mode (Level-2)
config	interface gigabitethernet	config-if
	interface range gigabitethernet	config-if-range
	interface tengigabitethernet	config-if
	interface range tengigabitethernet	config-if-range
	interface port-channel	config-if
	interface range port-channel	config-if-range
	interface vlan	config-if
	interface range vlan	config-if-range
	vlan	config-vlan
	axrp	config-axrp
	spanning-tree mst configuration	config-mst
	ip access-list standard	config-std-nacl
	ip access-list extended	config-ext-nacl
	ipv6 access-list	config-ipv6-acl
	mac access-list extended	config-ext-macl
	ip qos-flow-list	config-ip-qos
	ipv6 qos-flow-list	config-ipv6-qos
	mac qos-flow-list	config-mac-qos
	ip dhcp pool	dhcp-config
	aaa group server radius	config-group
	ethernet cfm domain	config-ether-cfm
	line console	config-line
	line vty	config-line
	auto-config	config-auto-cf
	netconf	config-netconf

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
<code>end</code>	Ends configuration command mode, and returns you to administrator mode.
<code>exit</code>	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.
<code>save (write)</code>	Saves the edited configuration in the startup configuration file.
<code>show</code>	Shows the configuration being edited.
<code>top</code>	After a switch to configuration command mode, enter this command restores level-1 global configuration mode.

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

Table 6-2 List of operation commands

Command name	Description
<code>show running-config</code>	Shows the running configuration.
<code>show startup-config</code>	Shows the startup configuration file.
<code>copy</code>	Copies the specified file or directory.
<code>erase startup-config</code>	Deletes the contents of the startup configuration file.
<code>rename</code>	Renames a file.
<code>del</code>	Deletes a specified file.
<code>mkdir</code>	Creates a new directory.
<code>rmdir</code>	Deletes a specified directory.

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 the startup configuration file

You can display and check the running configuration or the startup configuration file by using the **show running-config** operation command or the **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

```
# show running-config ... 1
#configuration list for XXXXX-XXX
!
vlan 1
    name "VLAN0001"
!
vlan 100
    state active
!
vlan 200
    state active
!
spanning-tree mode pvst
!
interface gigabitethernet 0/1
    switchport mode access
    switchport access vlan 100
!
interface gigabitethernet 0/2
    switchport mode access
    switchport access vlan 200
!
:
:
#
```

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.

Notes

1. In global configuration mode, parameters can be specified only for a command that switches to a level-2 configuration mode. The command line completion, Help, and abbreviated-command execution functionality can also be used.
2. In a level-2 configuration mode, parameters can be specified only for a command that switches modes, as in global configuration mode. In this case, however, the command line completion functionality and Help functionality cannot be used.

Figure 6-6 Displaying all configuration entries

```
(config) # show ... 1
#configuration list for XXXXXX-XXX
!
vlan 1
    name "VLAN0001"
!
vlan 100
    state active
!
vlan 200
    state active
!
spanning-tree mode pvst
!
interface gigabitethernet 0/1
    switchport mode access
    switchport access vlan 100
!
interface gigabitethernet 0/2
    switchport mode access
    switchport access vlan 200
!
:
:
(config) #
```

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

Figure 6-7 Displaying gigabitethernet interface information

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

1. Display all the **gi gabi tethernet** interface information in the running configuration.

Figure 6-8 Displaying information for a specified interface

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

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

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

```
(config) # interface gigabitethernet 0/1 ... 1
```

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

1. Display interface 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 the disabling and reinstating functionality* shows an example of disabling functionality and later re-enabling it.

Figure 6-10 Example of editing a configuration

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

1. Configure VLAN 100 as a port VLAN.
2. Activate VLAN 100.
3. Move to Ethernet interface 0/1 configuration mode.
4. Set the access mode for Ethernet interface 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 0/1 configuration mode.
9. Remove VLAN ID 100 from the defined accessed VLANs.

Figure 6-11 Example of the disabling and reinstating functionality

```
(config)# interface gigabitethernet 0/1
!(config-if)# shutdown ... 1
!(config-if)# speed 100 ... 2
!(config-if)# duplex full ... 3
!(config-if)# no shutdown ... 4
!(config-if)#
```

1. Disable the interface.
2. Set the transmission speed to 100 Mbit/s.

3. Set full duplex mode.
4. Enable the interface.

(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 0/1
!(config-if) # description TokyoOsaka
!(config-if) #
```

Figure 6-13 Error message output for an incorrect configuration

```
(config) # interface gigabitEthernet 0/1
!(config-if) # description
                        ^
Error: Missing parameter.
!(config-if) #
```

6.4.5 Saving configuration entries to a file

Using the **save** (**wri te**) configuration command or the **copy** operation command, you can save the edited running configuration to the startup configuration file. The following figure shows an example of saving a configuration.

Figure 6-14 Example of saving a configuration (save command)

```
# 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.

Figure 6-15 Example of saving a configuration (copy command)

```
# configure ... 1
(config) #
:
: ... 2
:
!(config) # end ... 3
!# copy running-config startup-config ... 4
Do you wish to copy from running-config to startup-config? (y/n) :y
#
```

1. Start editing the running configuration.
2. Change the configuration.
3. Use the **end** command to return to administrator mode.

4. Save to the startup configuration file.

6.4.6 Ending configuration editing (exit command)

When you have finished editing the running configuration, execute the `exit` command in global configuration mode.

6.4.7 Notes on configuration editing

(1) Limits on the number of configuration commands

If the number of entries you have edited exceeds the limit, a message to that effect appears. (For example: `Maximum number of entries are already defined.`). If such a message appears, check whether any unnecessary entries exist.

(2) Copying and pasting configuration entries

When you copy and paste configuration entries, you can copy and paste no more than 1000 characters (including spaces and line feed codes) per operation.

If the total size of the configuration entries you want to copy and paste exceeds 1000 characters, copy and paste them in multiple operations, each time keeping the number of characters to 1000 or less.

6.5 Configuration operations

This section describes operations such as configuration backups and file transfers.

6.5.1 Transferring files using the ftp command

Use the FTP protocol to transfer files between the Switch and a remote operation terminal.

(1) Transferring a backup configuration file to the Switch

To use the contents of a backup configuration file saved on a PC, first transfer the file to the Switch via FTP, and then use the `copy` operation command to copy the file to the startup configuration file.

On your PC, open the Command Prompt window. (If your PC's OS is the standard edition of Windows XP, from the **Start** menu, choose **All Programs**, choose **Accessories**, and then choose **Command Prompt**.)

Change the current directory to the directory that contains the backup configuration file, and then log in to the Switch via FTP. Transfer the file to the RAMDISK on the Switch in ASCII mode.

Make sure a VLAN and an IP address are set for the port to which you connect via FTP.

The following shows a sample command execution when a backup configuration file named `backup.cnf` has been saved in `C:\TEMP`.

Figure 6-16 Operation in the Command Prompt window: Transferring a backup configuration file to the PC

```
C:\TEMP>ftp 192.168.0.1
Connected to 192.168.0.1
220 AX2530S-24T FTP server ready
User (192.168.0.1: (none)): operator
331 Password required
Password:
230 User logged in
ftp> asc
200 Type set to A, ASCII mode
ftp>
ftp> put backup.cnf
200 Port set okay
150 Opening ASCII mode data connection
226 Transfer complete
ftp: xxxxxx bytes sent in xx.x Seconds (xx.xx Kbytes/sec)
ftp> bye
221 Bye...see you later
C:\TEMP>
```

Log in to the console, and then use the `copy` operation command to copy the target file from the RAMDISK to the startup configuration file.

Figure 6-17 Operation on the console: Copying the transferred file on the Switch (copy command)

```
> enable
# copy ramdisk backup.cnf startup-config
Do you wish to copy from RAMDISK to startup-config? (y/n): y
#
```

(2) Transferring a backup configuration file to a remote operation terminal

The following figure shows an example of transferring a backup configuration file stored on the RAMDISK on the Switch to a remote operation terminal.

Log in to the console, and then use the **copy** operation command to copy the startup configuration file to the RAMDISK.

Figure 6-18 Operation on the console: Copying the startup configuration file to the RAMDISK (copy command)

```
> enable
# copy startup-config ramdisk backup.cnf
#
```

On your PC, open the Command Prompt window.

Change the current directory to the directory that contains the backup configuration file, and then log in to the Switch via FTP. Transfer the file from the RAMDISK on the Switch to the PC in ASCII mode.

Figure 6-19 Operation in the Command Prompt window: Transferring a backup configuration file to the PC

```
C:\TEMP>ftp 192.168.0.1
Connected to 192.168.0.1
220 AX2530S-24T FTP server ready
User (192.168.0.1: (none)): operator
331 Password required
Password:
230 User logged in
ftp> asc
200 Type set to A, ASCII mode
ftp>
ftp> get backup.cnf
200 Port set okay
150 Opening ASCII mode data connection
226 Transfer complete
ftp: xxxxxx bytes sent in xx.x Seconds (xx.xx Kbytes/sec)
ftp> bye
221 Bye...see you later
C:\TEMP>
```

6.5.2 Transferring files using a memory card

Use the **copy** operation command to transfer files to a memory card.

(1) Transferring a backup configuration file to the Switch

Insert a memory card that contains a backup configuration file into the memory card slot. Use the **copy** operation command to copy the backup configuration file on the memory card to the RAMDISK on the Switch. Then use the **copy** operation command to copy the backup configuration file on the RAMDISK to the startup configuration file. The following figure shows an example of performing these operations.

Figure 6-20 Example of transferring a backup configuration file on a memory card to the Switch (copy command)

```
> enable
# copy mc backup.cnf ramdisk backup.cnf          ... 1
# copy ramdisk backup.cnf startup-config          ... 2
Do you wish to copy from RAMDISK to startup-config? (y/n): y
#
```

1. Copy the backup configuration file from the memory card to the RAMDISK.
2. Copy the backup configuration file on the RAMDISK to the startup configuration file.

(2) Transferring a backup configuration file to a memory card

Use the **copy** operation command to copy a backup configuration file to a memory card.

Use the **copy** operation command to copy the startup configuration file to the RAMDISK.

Then use the **copy** operation command to copy the backup configuration file on the RAMDISK to the memory card. The following figure shows an example of performing these operations.

Figure 6-21 Copying a backup configuration file from the Switch to a memory card (copy command)

```
> enable
# copy startup-config ramdisk backup.cnf          ... 1
# copy ramdisk backup.cnf mc backup.cnf          ... 2
#
```

1. Copy the startup configuration file to the RAMDISK.
2. Copy the backup configuration file on the RAMDISK to the memory card.

6.5.3 Notes on applying a backup configuration file

If you use the **copy** operation command to copy a backup configuration file to the startup configuration file, the new settings in the startup configuration file are not applied to the running configuration immediately. To apply the new settings, you need to restart the switch by turning it off and then on again or by executing the **reload** operation command.

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.

7. Remote Login

This chapter describes remote access to the Switch from a remote operation terminal.

7.1 Description

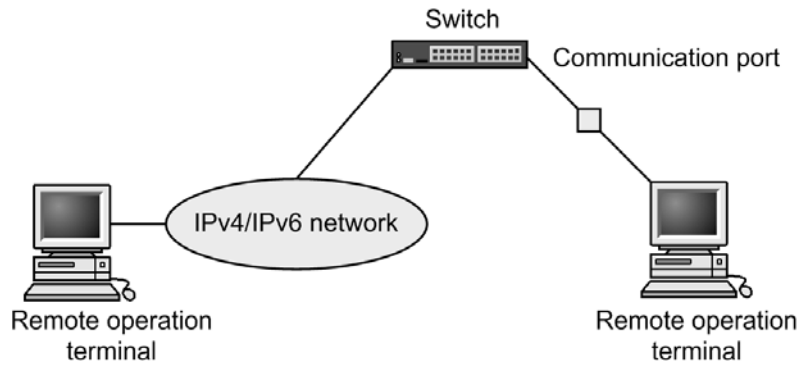
7.2 Configuration

7.3 Operation

7.1 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 configuration.

Figure 7-1 Login to the Switch from a remote operation terminal



7.2 Configuration

7.2.1 List of configuration commands

The following table describes the configuration commands related to operation terminal connections and remote operations.

Table 7-1 List of configuration commands

Command name	Description
<code>ftp-server</code>	Permits access from remote operation terminals using FTP.
<code>line console</code>	Sets parameters for the RS232C port.
<code>line vty</code>	Permits Telnet remote access to the switch.
<code>speed</code>	Sets the communication speed of the RS232C port.
<code>transport input</code>	Regulates access from a remote operation terminal using the various protocols.

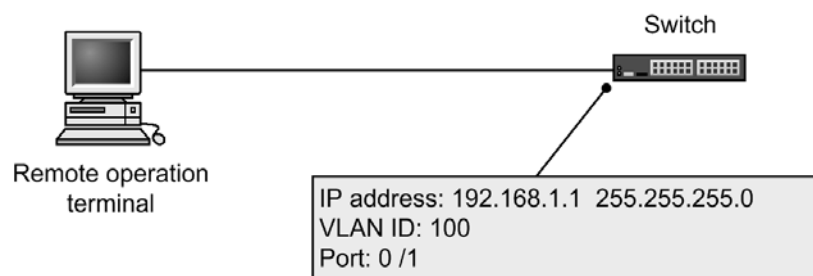
For details about the configuration commands related to setting up VLANs and IPv4/IPv6 interfaces, see *18 VLAN*, and *26 IPv4 Interfaces* or *27 IPv6 Interfaces*.

7.2.2 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 7-2 Example of connecting with a remote operation terminal



Command examples

- ```
(config)# vlan 100
(config-vlan)# exit
```

Creates a port VLAN with an ID of 100.
- ```
(config)# interface gigabitethernet 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 0/1. Sets port 0/1 for the VLAN 100 access port.

7 Remote Login

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 100. Sets IPv4 address 192.168.1.1 and subnet mask 255.255.255.0 for VLAN 100.

7.2.3 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 a configuration that permits a remote operation terminal to remotely log in to the Switch via the Telnet protocol.

If remote login has not been configured, you can log in only from the console.

Command examples

1. `(config)# line vty 0 15`
`(config-line)# exit`

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 16 users.

7.2.4 Permitting login by using FTP

Points to note

The switch's IP address must be assigned before you can use this procedure.

Set a configuration that permits a remote operation terminal to remotely access the Switch 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.

7.3 Operation

7.3.1 List of operation commands

The following table describes the operation commands related to operation terminal connections and remote operations.

Table 7-2 List of operation commands

Command name	Description
<code>set exec-timeout</code>	Specifies the length of time until the user is automatically logged out.
<code>set terminal pager</code>	Enables or disables paging.
<code>telnet</code>	Connects via Telnet to the remote host that has the specified IP address.
<code>ftp</code>	Transfers files between the Switch and a remote operation terminal connected by using TCP/IP.
<code>tftp</code>	Transfers files between the Switch and a remote operation terminal connected by using UDP.

7.3.2 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` operation command. For details, see *26 IPv4 Interfaces* or *27 IPv6 Interfaces*.

8. Login Security and RADIUS

This chapter describes login control, login security, and RADIUS implementations on the Switches.

8.1 Setting login security

8.2 Description of RADIUS

8.3 RADIUS configuration

8.4 RADIUS operation

8.1 Setting login security

8.1.1 Lists of configuration and operation commands

The following table describes the configuration commands for login security.

Table 8-1 List of configuration commands

Command name	Description
<code>aaa authentication login</code>	Specifies the authentication method to be used at remote login.
<code>aaa authentication login end-by-reject</code>	Ends authentication if authentication fails at login. If authentication fails due to an inability to communicate (for example, the RADIUS server does not respond), the next authentication method specified by the <code>aaa authentication login</code> configuration command is used to perform authentication.
<code>ip access-group</code>	Sets an access list that specifies the IPv4 addresses of the remote operation terminals for which remote login to the Switch is permitted or denied.
<code>ipv6 access-class</code>	Sets an access list that specifies the IPv6 addresses of the remote operation terminals for which remote login to the Switch is permitted or denied.

The following table describes the operation commands for login security.

Table 8-2 List of operation commands

Command name	Description
<code>adduser</code>	Adds an account for a new login user.
<code>rmuser</code>	Deletes a user login account registered by the <code>adduser</code> command.
<code>password</code>	Specifies the password of a login user.
<code>clear password</code>	Deletes the password of a login user.
<code>show users</code>	Shows information about valid users set for the Switch.
<code>show sessions (who)</code>	Shows the users currently logged in to the Switch.

8.1.2 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, the user ID and password are checked at login.
2. Users can log in to a Switch concurrently from both local and remote operation 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`, `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. Command execution results appear only on the terminal where the command was executed. Operation messages appear on all login operation terminals.
7. 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.
8. The user is automatically logged out if there is no key input for a specified period (default: 60 minutes). You can change the auto-logout time by using the `set exec-timeout` operation command.
9. Login from a remote operation terminal (via Telnet) also supports one-time password authentication by using the SecurID mechanism engineered by RSA Security. For details about one-time password authentication, see *14 One-Time Password Authentication [OS-L2A]* in the manual *Configuration Guide Vol. 2*.

8.1.3 Creating and deleting user accounts

To create a user account for logging in to the Switch, use the `adduser` operation command. The following figure shows an example.

Figure 8-1 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
# exit
>
```

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 authentication. For configuration examples, see *8.3.2 Configuring the login authentication method*.

Do not forget your user ID.

8.1.4 Setting the password for switching to 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 8-2 Setting the password for switching to administrator mode immediately after deployment

```
> enable
# password enable-mode
```

```
Changing local password for admin.  
New password:  
Retype new password:  
#
```

8.1.5 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 8-3 Example of configuring permission for remote login

```
(config)# line vty 0 1  
(config-line)# exit
```

To permit access to the Switch from a remote operation terminal using FTP, you need to set the `ftp-server` configuration command. If you omit this setting, users cannot access the Switch by FTP.

Figure 8-4 Example of configuring permission for FTP access

```
(config)# ftp-server  
(config)#
```

8.1.6 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 `<End allocation>` parameter of the `line vty` configuration command limits the number of remote users that can log in concurrently. Regardless of this setting, login from the console is always possible. The following setting example allows no more than 16 users to be logged in concurrently.

Figure 8-5 Example of setting the maximum number of concurrent users

```
(config)# line vty 0 15  
(config-line)# exit
```

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.

8.1.7 Setting the IP addresses of remote operation terminals permitted to log in

By configuring the setting below, 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`, `ip access-group`, or `ipv6 access-class` configuration command. You can register a maximum of 128 lists that contain IPv4 addresses and subnet masks, or IPv6 addresses and prefixes to allow access from the addresses. If you omit this setup, all remote operation terminals will be able to access the Switch.

Command examples (IPv4)

1. `(config)# ip access-list standard REMOTE`

```
(config-std-nacl)# deny host 192.168.0.254
(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 192.168.0.0/24, but denies login from the IPv4 address 192.168.0.254 on that network.

2.

```
(config)# line vty 0 1
(config-line)# ip access-group REMOTE in
(config-line)# exit
```

Moves to line mode, applies the access list **REMOTE**, and permits login only from the remote operation terminals on network IP address 192.168.0.0/24.

Command examples (IPv6)

1.

```
(config)# ipv6 access-list REMOTE6
(config-ipv6-nacl)# deny ipv6 host 3ffe:501:811:ff01::0001
(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 3ffe:501:811:ff01::/64, but denies login from the IPv6 address 3ffe:501:811:ff01::0001 on that network.

2.

```
(config)# line vty 0 1
(config-line)# ipv6 access-class REMOTE6 in
(config-line)# exit
```

Moves to line mode, applies the access list **REMOTE6**, and permits login only from the remote operation terminals on the network 3ffe:501:811:ff01::/64.

Notes

- An access list for use by the Switch does not depend on the settings of the flow detection mode.
- An IP address matching a permit condition will be permitted to log in.
An IP address matching a deny condition will not be permitted to log in.
- An implicit deny condition for all IP addresses is set in the last lists of **ip access-group** and **ipv6 access-class**. For an IP address that does not match any registered group, the Switch assumes that an implicit deny condition exists, and denies remote login from the IP address.
- For an IP access group for which no access list is registered in **ip access-group** and **ipv6 access-class**, the Switch assumes that a permit condition exists.

8.2 Description of RADIUS

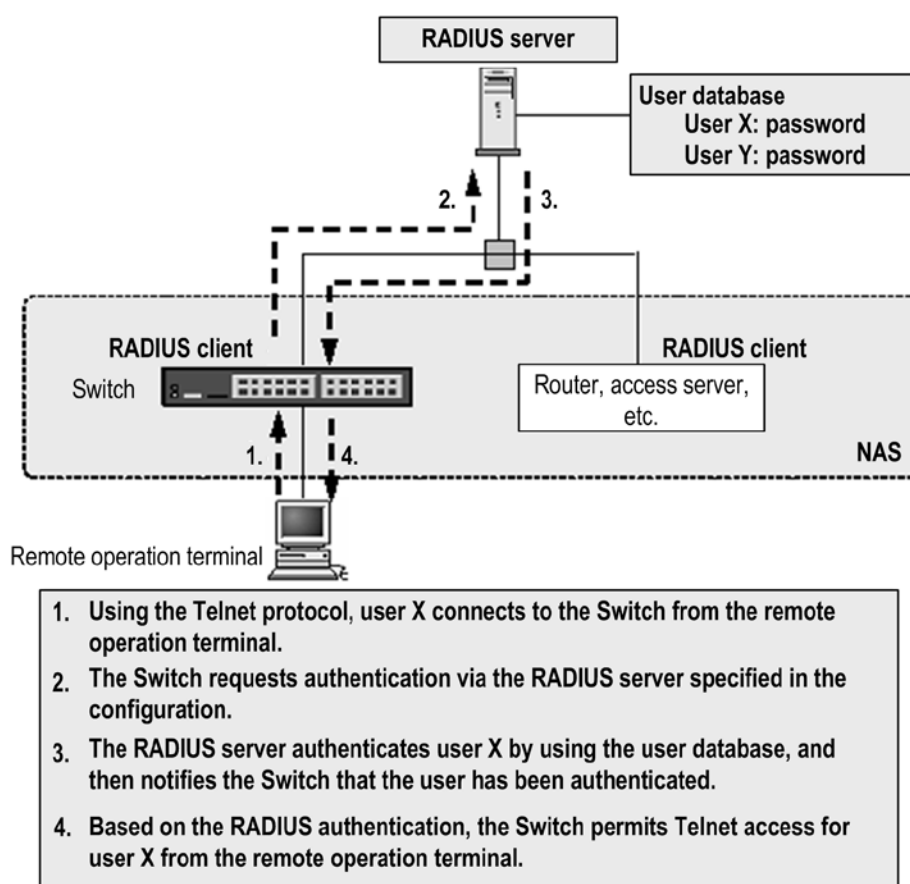
8.2.1 Overview of RADIUS

The Remote Authentication Dial In User Service (RADIUS) is a protocol that provides authentication 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 client. A NAS device requests services such as user authentication and accounting from the configured RADIUS server. The server responds to service requests based on the data in its management information database. The Switch supports NAS functionality.

When RADIUS is implemented, authentication information such as user passwords used by the NAS devices and accounting information can be centrally managed by one RADIUS server. The Switch can request user authentication and accounting services from a RADIUS server.

The following figure shows the flow of RADIUS authentication.

Figure 8-6 Flow of RADIUS authentication



8.2.2 Scope of RADIUS implementation

The Switch can use RADIUS for the following types of authentication:

- User authentication at login from a remote operation terminal (abbreviated hereafter to login authentication)
RADIUS authentication
- Layer 2 authentication functionality (IEEE 802.1X, Web authentication, or MAC-based authentication)

RADIUS authentication and RADIUS accounting

For details about Layer 2 authentication functionality, see the manual *Configuration Guide Vol. 2*.

The scope of RADIUS authentication support covered in this section pertains only to login authentication.

(1) Scope of RADIUS authentication

RADIUS 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)

RADIUS authentication cannot be used for the following operation:

- Login from the console (RS232C)

(2) Scope of RADIUS server support

The Switch supports the following NAS functionality for communication with a RADIUS server:

Table 8-3 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 accounting packet types used in login authentication: <ul style="list-style-type: none"> ● Access-Request (send) ● Access-Accept (receive) ● Access-Reject (receive) ● Access-Challenge (receive)
Attribute	Support for the following attributes used in login authentication: <ul style="list-style-type: none"> ● User-Name ● User-Password ● Service-Type ● NAS-IP-Address ● NAS-IPv6-Address ● Reply-Message ● State ● NAS-Identifier

(a) Description of supported RADIUS attributes

The table below describes the supported RADIUS attributes.

- Access-Request packet
No attributes other than those listed in the table below are attached to Access-Request packets sent by the Switch.
- Access-Accept, Access-Reject, and Access-Challenge packets
Attributes other than those listed below are ignored by the Switch if attached to the packet.

Table 8-4 Supported RADIUS attributes

Attribute name	Attribute value	Packet type	Description
User-Name	1	Access-Request	The name of the user being authenticated.
User-Password	2	Access-Request	The password of the user being authenticated, sent in encrypted form.
Service-Type	6	Access-Request	Login (value = 1). This is ignored when attached to Access-Accept or Access-Reject.
NAS-IP-Address	4	Access-Request	The IPv4 address of the Switch. From among the VLAN interfaces that have an IPv4 address registered, the IPv4 address of the smallest VLAN ID is used.
Reply-Message	18	Access-Challenge Access-Accept ^{#1} Access-Reject ^{#1}	Text character string. A message used for one-time password authentication ^{#2} is displayed in the Telnet window.
State	24	Access-Challenge Access-Request	Text character string. If the Access-Challenge packet used for one-time password authentication ^{#2} contains state information, the Switch holds the state information. When an Access-Request packet is sent in response to an Access-Challenge packet, the state information held on the Switch is added.
NAS-Identifier	32	Access-Request	The device name of the Switch. This is not attached if a device name was not set.
NAS-IPv6-Address	95	Access-Request	The IPv6 address of the Switch. From among the VLAN interfaces that have an IPv6 address registered, the IPv6 address of the smallest VLAN ID is used.

#1

Access-Accept and Access-Reject packets ignore Reply-Message packets.

#2

For details about one-time password authentication, see *14 One-Time Password Authentication [OS-L2A]* in the manual *Configuration Guide Vol. 2*.

8.2.3 Authentication using RADIUS

This section describes RADIUS authentication when used for login authentication.

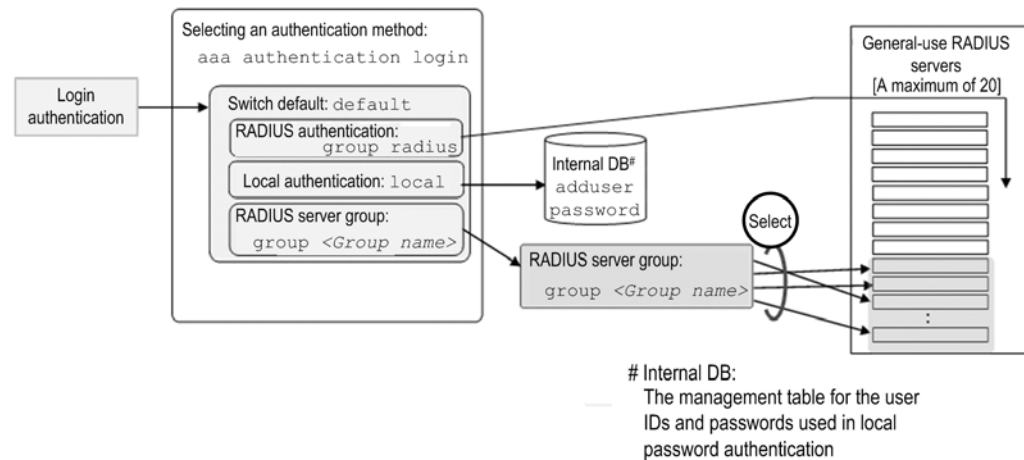
Note that the RADIUS server selection functionality and the automatic-restoration functionality described below can also be used for Layer 2 authentication. For more details, see *5 Overview of Layer 2 Authentication Functionality* in the manual *Configuration Guide Vol. 2*.

(1) Selecting the login authentication service

You can specify multiple services for login authentication. The specifiable services are RADIUS authentication (general-use RADIUS server authentication or RADIUS server group authentication) and local password authentication functionality (the Switch's own authentication functionality implemented by the `adduser/password` command).

The following figure shows a correlation diagram of authentication method settings.

Figure 8-7 Correlation of the authentication method settings



You can specify these authentication methods singly or in combination, which allows the user to be authenticated by the next specified method if authentication by the first specified method fails. You can also change the action taken by the authentication service selection if authentication by the first specified method fails. To change the action, use the [aaa authentication login end-by-reject](#) configuration command.

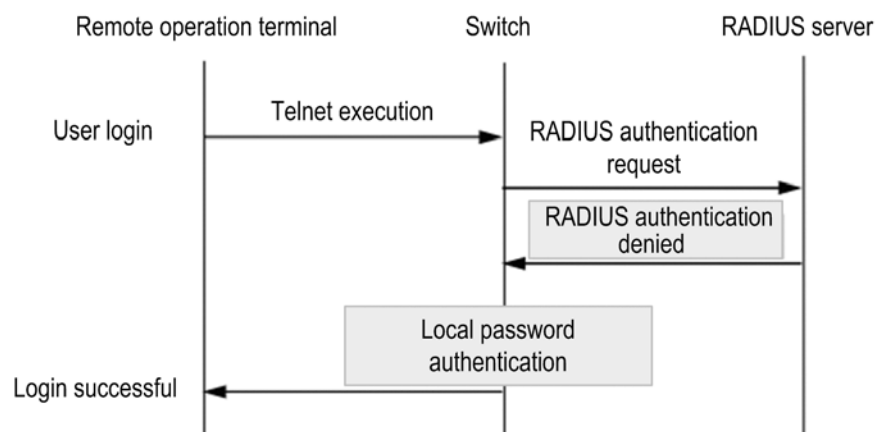
You cannot simultaneously specify both [group radius](#) (general-use RADIUS server authentication) and [group <Group name>](#) (RADIUS server group authentication) in the above figure, because both methods are treated as the RADIUS authentication service. Use either of them in combination with local password authentication.

(a) When end-by-reject is not set

The following explains how an authentication service is selected if [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 authentication and local password authentication are specified and performed in that order. The authentication results are as follows: RADIUS server authentication fails, but local password authentication succeeds.

Figure 8-8 Sequence of authentication (without end-by-reject is specified)



In this figure, the user accesses the Switch via Telnet from a remote operation terminal, and

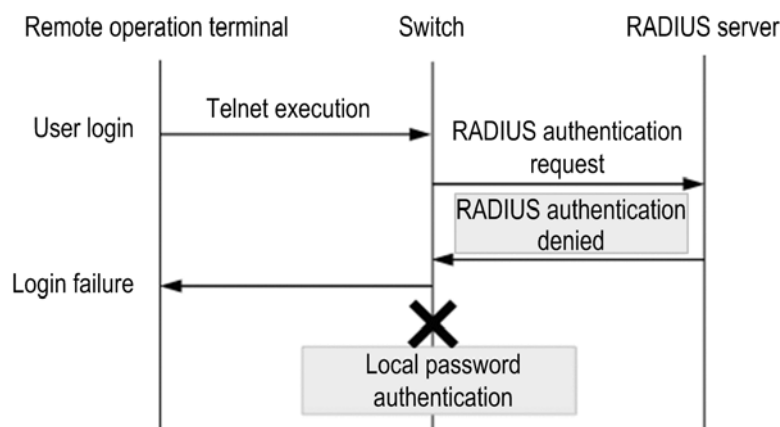
the Switch requests the RADIUS server to perform authentication. However, the RADIUS server rejects the request, and authentication fails. The Switch then performs local password authentication. This authentication succeeds, and the user is able to log in successfully to the Switch.

(b) When end-by-reject is set

The following explains how an authentication service is selected when **end-by-reject** is set. If **end-by-reject** is specified and authentication by the first specified method is denied, the next specified authentication method is not used to issue another authentication request. Authentication processing is ended at this point, and the entire authentication process is assumed to have failed. However, if the authentication failure is due to an inability to communicate (for example, the RADIUS server does not respond), the next specified method is used to issue another authentication request.

As an example, the figure below shows the sequence in which authentication is performed when RADIUS authentication and local password authentication are specified and performed in that order. The authentication results are as follows: RADIUS server authentication fails.

Figure 8-9 Sequence of authentication (with end-by-reject specified)



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. However, the RADIUS server rejects the request, and authentication fails. At this point, the entire authentication process is assumed to have failed, and authentication processing is ended. Local password authentication, which is the next specified authentication method on the Switch, is not used. As a result, the user fails to log in to the Switch.

(2) RADIUS server selection and automatic-restoration (dead-interval)

A maximum of 20 general-use RADIUS servers can be specified for remote login that uses RADIUS authentication. If one server is unreachable and its authentication service is unavailable, the Switch tries each of the other servers in turn.

- RADIUS server selection (timeout period for determining whether communication is possible)

You can configure a response timeout period to determine whether communication with a RADIUS server is possible. The default is five seconds. If a RADIUS server times out, the Switch keeps trying to connect with it. You can set the maximum number of connection retries that the server makes with each server (three by default). Accordingly, the maximum time before the system decides that RADIUS server login is unavailable is as follows: *response-timeout-period* x (*first-try* + *number-of-retries*) x *number-of-RADIUS-servers-configured*

- Automatic-restoration (dead-interval) functionality

RADIUS authentication used by the Switch detects the RADIUS server in effect when the Switch detects a RADIUS authentication request by receiving a frame from a terminal subject to authentication. The following terminals always use the RADIUS server in effect. In this method, time to authentication is reduced, but it cannot be automatically restored to a load-distributed state when a RADIUS server is used in a load-distributed structure and a failure occurs on a RADIUS server. The Switch supports the automatic-restoration (dead-interval) functionality provided by the monitoring timer as a method of auto-recovery for the first valid RADIUS server (primary RADIUS server). The default monitoring timer value is 10 minutes.

(3) Registering information with a RADIUS server

Register the user ID and password with the RADIUS server. A user ID can be registered in either of two ways:

- User ID already registered in the Switch by the `adduser` operation command
Login processing is based on the user information registered in the Switch.
- Unregistered user ID
Login processing is performed with user ID `operator`, which is the initial user ID.

Note that the user ID and password you register on the RADIUS server must meet the following requirements:

- User ID: The character string must consist of 1 to 16 alphanumeric characters and must begin with an alphabetic character.
- Password: The character string must consist of 6 to 128 alphanumeric characters.

8.2.4 Connecting with a RADIUS server

(1) Switch identification on the RADIUS server side

The RADIUS server uses the source IP address of the request packet as the key for identifying the RADIUS client. The Switch uses the IP address of the source VLAN interface.

(2) 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 use port 1645, not 1812. 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.

(3) RADIUS server information configurable on the Switch

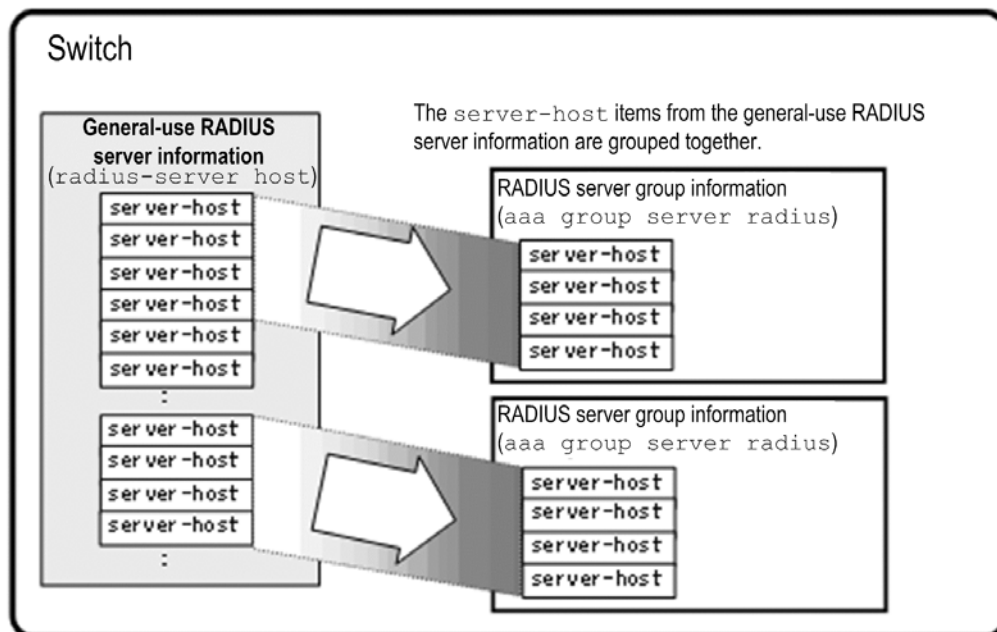
The following RADIUS server information can be configured on the Switch.

- General-use RADIUS server information
Used for both login authentication and Layer 2 authentication functionality.
- Authentication RADIUS server information (IEEE 802.1X, Web authentication, and MAC-based authentication)
Used only for each Layer 2 authentication functionality.
- RADIUS server group information
Information about grouped general-use RADIUS servers, which is used for both login authentication and the Layer 2 authentication functionality.

For details about the setup and use of the Layer 2 authentication functionality and the relevant information for each RADIUS server, see *5 Overview of Layer 2 Authentication Functionality* in the manual *Configuration Guide Vol. 2*.

The RADIUS server group information is assigned from the general-use RADIUS server information that has been configured. The following table describes the relationship between the general-use RADIUS server group information and general-use RADIUS server information.

Figure 8-10 Relationship between the RADIUS server group information and the general-use RADIUS server information



The IP address, the port number for authentication, and the port number for accounting to be set for a RADIUS server group must be the same as the values in the general-use RADIUS server information (`radius-server host` configuration command).

Note that for the RADIUS servers in a RADIUS server group, the selection processing is the same as that for other RADIUS servers. However, the automatic-restoration time follows the setting of the `radius-server dead-interval` configuration command.

For details about the capacity limits for a RADIUS server group, see *3.2 Capacity limit*.

RADIUS server groups are also used for the port-based authentication method in Layer 2 authentication functionality or the user ID-based authentication method in Web authentication. For more details, see *5 Overview of Layer 2 Authentication Functionality* in the manual *Configuration Guide Vol. 2*.

8.3 RADIUS configuration

8.3.1 List of configuration commands

The following table describes the configuration commands for RADIUS.

Table 8-5 List of configuration commands (RADIUS)

Command name	Description
<code>aaa group server radius</code>	Sets a RADIUS server group.
<code>server</code>	Sets a RADIUS server host in the RADIUS server group.
<code>radius-server dead-interval</code>	Sets the monitoring timer used to automatically restore the primary RADIUS server.
<code>radius-server host</code>	Sets the general-use RADIUS server information used for authentication.
<code>radius-server key</code>	Sets a RADIUS server key used for authentication.
<code>radius-server retransmit</code>	Sets the maximum number of retransmissions to a RADIUS server used for authentication.
<code>radius-server timeout</code>	Sets a response timeout value for a RADIUS server used for authentication.
<code>radius-server attribute station-id capitalize</code>	Sends the MAC address that is used for sending data to a RADIUS server with the RADIUS attribute in upper case. (These commands are used for the Layer 2 authentication functionality. [#])

#

For the RADIUS attributes for which these commands are used in Layer 2 authentication functionality, see the description of the applicable authentication functionality in the manual *Configuration Guide Vol. 2*.

8.3.2 Configuring the login authentication method

This section uses the following configuration examples to describe how to configure the login authentication method:

- Combining general-use RADIUS server authentication and local password authentication
- Combining RADIUS server group authentication and local password authentication

(1) Configuring general-use RADIUS server authentication and local password authentication

Points to note

In this example, RADIUS authentication and local password authentication are set as the authentication methods that will be used. The settings are specified so that RADIUS authentication is used as the primary method, but if it fails due to an inability to communicate (for example, the RADIUS server does not respond), then local password authentication on the Switch is used.

Note that if the cause of the RADIUS authentication failure is denial of authentication, the Switch ends all authentication processing at this point and does not attempt local password authentication.

The general-use RADIUS server information used for RADIUS authentication is also configured.

Make sure that the normal settings necessary for remote access have already been specified.

Command examples

1. `(config)# aaa authentication login default group radius local`
Specifies RADIUS authentication and local password authentication, in that order, as the login authentication methods to be used.
2. `(config)# aaa authentication login end-by-reject`
Configures the Switch so that if RADIUS authentication is denied, the Switch ends all authentication processing and does not attempt local password authentication.
3. `(config)# radius-server host 192.168.10.1 key "AAAA1234"`
Sets IP address 192.168.10.1 as the general-use RADIUS server to be used for RADIUS authentication and a common key for communication with the server.
4. `(config)# radius-server host 192.168.10.2 key "BBBB1234"`
Sets IP address 192.168.10.2 as the server to be used for RADIUS authentication and a common key for communication with the server.

Notes

1. `group radius` and `group <group-name>` cannot both be specified as authentication methods because they are treated as the same *<Method>* (RADIUS authentication). If you want to specify multiple methods, combine either of them and `local`.

(2) Configuring RADIUS server group authentication and local password authentication

Points to note

In this example, RADIUS server group authentication and local password authentication are set as the authentication methods that will be used. The settings are specified so that RADIUS server group authentication is used as the primary method, but if it fails due to an inability to communicate (for example, the RADIUS server does not respond), then local password authentication on the Switch is used.

Note that if the cause of the RADIUS authentication failure is denial of authentication, the Switch ends all authentication processing at this point and does not attempt local password authentication.

For the RADIUS server group information used for RADIUS server group authentication, see *8.3.3 Configuring a RADIUS server group*.

Make sure that the normal settings necessary for remote access have already been specified.

Command examples

1. `(config)# aaa authentication login default group LOGIN-SEC local`
Specifies the RADIUS server group name and local password authentication, in that order.
2. `(config)# aaa authentication login end-by-reject`
Configures the Switch so that if RADIUS server group authentication is denied, the Switch ends authentication processing and does not attempt local password

authentication.

Notes

1. `group radius` and `group <group-name>` cannot both be specified as authentication methods because they are treated as the same *<Method>* (RADIUS authentication). If you want to specify multiple methods, combine either of them and `local`.

8.3.3 Configuring a RADIUS server group

Points to note

Set a RADIUS server group that is to be used for authentication.

A RADIUS server group consists of RADIUS servers that have been set by using the `radius-server host` (general-use RADIUS server) configuration command. From these RADIUS servers, select the servers you want to include in the RADIUS server group, and set their addresses for the RADIUS server group.

You can set information for a maximum of four RADIUS servers for one group.

Command examples (IPv4)

1.

```
(config) # radius-server host 192.168.10.1 key "AAAA1234"
(config) # radius-server host 192.168.10.2 key "BBBB1234"
(config) # radius-server host 192.168.10.3 key "CCCC1234"
(config) # radius-server host 192.168.10.4 key "DDDD1234"
(config) # radius-server host 192.168.10.5 key "EEEE1234"
(config) # radius-server host 192.168.10.6 key "FFFF1234"
(config) # radius-server host 192.168.10.7 key "GGGG1234"
(config) # radius-server host 192.168.10.8 key "HHHH1234"
```

Sets the IPv4 addresses and common keys of general-use RADIUS servers.

2.

```
(config) # aaa group server radius LOGIN-SEC
```

Sets the RADIUS server group name, and switches to RADIUS server group configuration mode.

3.

```
(config-group) # server 192.168.10.1
(config-group) # server 192.168.10.2
(config-group) # server 192.168.10.7
(config-group) # server 192.168.10.8
(config-group) # exit
```

Sets, for the RADIUS server group, the addresses of RADIUS servers selected from the RADIUS servers that were set by using the `radius-server host` configuration command.

In this example, the port number for authentication and the port number for accounting are omitted. Therefore, by default, port 1812 is used for authentication and port 1813 is used for accounting.

Command examples (IPv6)

1.

```
(config) # radius-server host 3ffe:501:811:ff03::c7c0 key "AAAA1234"
(config) # radius-server host 3ffe:501:811:ff03::c7c1 key "BBBB1234"
```



```
(config) # radius-server host 3ffe:501:811:ff03::c7d0 key "CCCC1234"
(config) # radius-server host 3ffe:501:811:ff03::c7d1 key "DDDD1234"
(config) # radius-server host 3ffe:501:811:ff03::c7e0 key "EEEE1234"
(config) # radius-server host 3ffe:501:811:ff03::c7e1 key "FFFF1234"
(config) # radius-server host 3ffe:501:811:ff03::c7f0 key "GGGG1234"
(config) # radius-server host 3ffe:501:811:ff03::c7f1 key "HHHH1234"
```

Sets the IPv6 addresses and common keys of general-use RADIUS servers.

2. (config) # aaa group server radius LOGIN-SEC-IPv6

Sets the RADIUS server group name, and switches to RADIUS server group configuration mode.

3. (config-group) # server 3ffe:501:811:ff03::c7c1
(config-group) # server 3ffe:501:811:ff03::c7d1
(config-group) # server 3ffe:501:811:ff03::c7e1
(config-group) # server 3ffe:501:811:ff03::c7f1
(config-group) # exit

Sets, for the RADIUS server group, the addresses of RADIUS servers selected from the general-use RADIUS servers that were set by using the [radius-server host](#) configuration command.

In this example, the port number for authentication and the port number for accounting are omitted. Therefore, by default, port 1812 is used for authentication and port 1813 is used for accounting.

Notes

1. We recommend that the group names you set by using the [aaa group server radius](#) configuration command begin with an upper-case letter.
2. The settings specified by the [server](#) configuration command take effect when all of the following conditions are met:
 - The values of the settings are the same as the values set by using the [radius-server host](#) configuration command (IP address, port number for authentication, and port number for accounting).
 - The [radius-server host](#) settings whose values are the same values as the settings specified by the [server](#) command are enabled (the [key](#) parameter has been set or [radius-server key](#) has been configured).

8.4 RADIUS operation

8.4.1 List of operation commands

The following table describes the operation commands for RADIUS.

Table 8-6 List of operation commands

Command name	Description
<code>show radius-server</code>	Shows information about the RADIUS servers that were set for the Switch and that are in effect.
<code>clear radius-server</code>	Resets the authentication RADIUS server to the first set RADIUS server.
<code>show radius-server statistics</code>	Shows statistics about the RADIUS servers that were set for the Switch and that are in effect.
<code>clear radius-server statistics</code>	Clears the statistics about the RADIUS servers that were set for the Switch and that are in effect.

8.4.2 Displaying information about the RADIUS servers in effect

(1) Displaying the RADIUS servers that are in effect

You can use the `show radius-server` operation command to display the RADIUS server information set on the Switch. If there are no usable RADIUS servers, `* hold down` is displayed.

Figure 8-11 Results of executing show radius-server (the servers running as effective RADIUS servers)

```
> show radius-server

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

```

        IP address: 2000::fe
        Port: 1812 Timeout: 5 Retry: 3 Remain: -
* hold down 591
[Accounting]
* IP address: 192.168.101.254
  Port: 1813 Timeout: 5 Retry: 3 Remain: -
  IP address: 2000::fe
  Port: 1813 Timeout: 5 Retry: 3 Remain: -
<web-auth>
[Authentication]
* IP address: 192.168.100.254
  Port: 1812 Timeout: 5 Retry: 3 Remain: -
  IP address: 2001::fe
  Port: 1812 Timeout: 5 Retry: 3 Remain: -
[Accounting]
* IP address: 192.168.100.254
  Port: 1813 Timeout: 5 Retry: 3 Remain: -
  IP address: 2001::fe
  Port: 1813 Timeout: 5 Retry: 3 Remain: -
<Group1>
[Authentication]
* IP address: 192.168.100.254
  Port: 1812 Timeout: 5 Retry: 3 Remain: -
  IP address: 2001::fe
  Port: 1812 Timeout: 5 Retry: 3 Remain: -
>

```

Note: The IP addresses indicated by an asterisk (*) are the IP addresses of the RADIUS servers that are currently in use.

(2) Displaying statistics about the RADIUS servers in effect

You can display statistics about the RADIUS servers that are set for the Switch and that are in effect.

- The `show radius-statistics summary` operation command displays summary information.
- The `show radius-server statistics` operation command displays normal statistics.

Figure 8-12 Results of executing show radius-server statistics summary

```

> show radius-server statistics summary

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

```

Figure 8-13 Results of executing show radius-server statistics

```

> show radius-server statistics

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

```

```

        Retry      :          0 Timeout:          0
[Rx] Responses:          0
        Mal formed:          0 BadAuth:          0 UnknownType:          0
IP address: 192.168.101.254
[Authentication]      Current Request:          0
[Tx] Request  :          1 Error  :          0
    Retry      :          3 Timeout:          4
[Rx] Accept   :          0 Reject :          0 Challenge :          0
    Mal formed:          0 BadAuth:          0 UnknownType:          0
[Accounting]          Current Request:          0
[Tx] Request  :          0 Error  :          0
    Retry      :          0 Timeout:          0
[Rx] Responses:          0
    Mal formed:          0 BadAuth:          0 UnknownType:          0
IP address: 2000::fe
[Authentication]      Current Request:          0
[Tx] Request  :          1 Error  :          0
    Retry      :          3 Timeout:          4
[Rx] Accept   :          0 Reject :          0 Challenge :          0
    Mal formed:          0 BadAuth:          0 UnknownType:          0
[Accounting]          Current Request:          0
[Tx] Request  :          0 Error  :          0
    Retry      :          0 Timeout:          0
[Rx] Responses:          0
    Mal formed:          0 BadAuth:          0 UnknownType:          0
IP address: 2001::fe
[Authentication]      Current Request:          0
[Tx] Request  :          2 Error  :          0
    Retry      :          0 Timeout:          0
[Rx] Accept   :          1 Reject :          0 Challenge :          1
    Mal formed:          0 BadAuth:          0 UnknownType:          0
[Accounting]          Current Request:          0
[Tx] Request  :          0 Error  :          0
    Retry      :          0 Timeout:          0
[Rx] Responses:          0
    Mal formed:          0 BadAuth:          0 UnknownType:          0

```

>

9. Time Settings and NTP

This chapter describes the time settings and NTP.

9.1 Setting and checking the time

9.2 Configuration

9.3 Operation

9.1 Setting and checking the time

9.1.1 Supported specifications

Set the clock time when you first install the Switch. Time information is used in a 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 following table describes the NTP client functionality supported by Switches.

Table 9-1 NTP client functionality supported by Switches

Functionality	Description
Unicast mode	In this mode, the Switch periodically retrieves the time from the NTP server.
Multicast mode	Not supported
Broadcast mode	In this mode, the Switch receives the time broadcast by the NTP server.
Manual time acquisition functionality	The <code>set clock ntp</code> operation command is used to acquire the time from the NTP server. (Unicast mode)
Distributor limitation functionality	Not supported
Host name specification (using DNS) functionality	Not supported
Authentication functionality	Not supported
Time adjustment functionality	Not supported

If periodic time reception has been enabled by setting of a configuration command, the Switch acquires the time from the NTP server whenever it starts up.

Although multiple modes can be set, only one mode can be in effect. Manual time reception can be performed any time regardless of the mode in effect as described in the following table:

Table 9-2 Mode that is in effect when multiple modes are set (Y: Set, --: Not set)

Unicast	Broadcast	Mode in effect
Y	N	Unicast
Y	Y	Unicast
N	Y	Broadcast

(1) Acquiring the time periodically from the specified NTP server (unicast mode)

If the address of the NTP server from which the time is to be received is set, the Switch periodically requests the time from the NTP server, and updates the internal clock time. (The interval at which the request is issued can be set by using a configuration command.)

A maximum of two NTP server addresses can be registered. The first registered address is called the primary address, and the second registered address is called the secondary address. If the time cannot be acquired from the primary NTP server address, the Switch requests the time from the secondary NTP server address.

Figure 9-1 Overview of acquiring time information in unicast mode (when only the primary address is set)

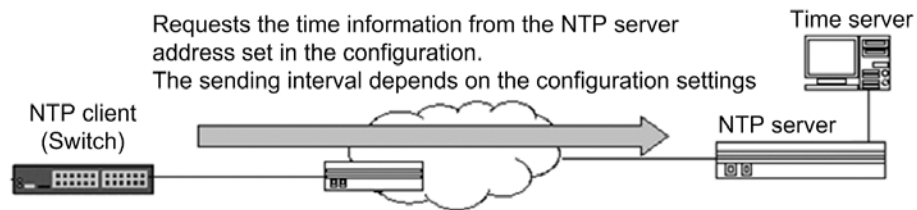
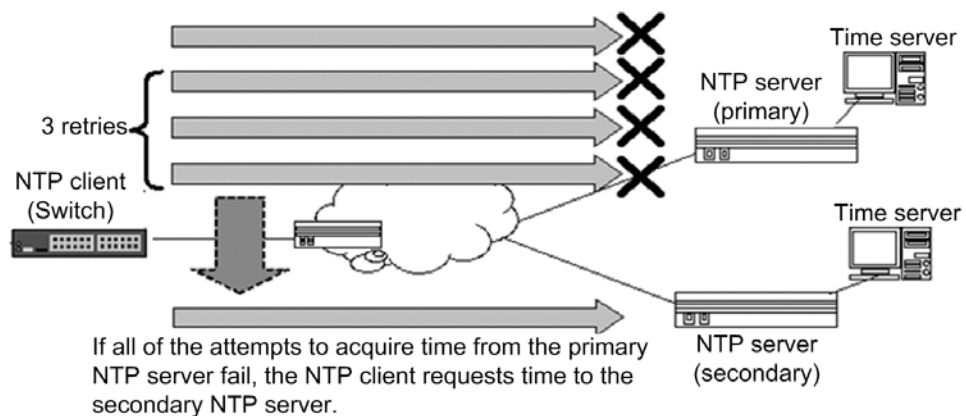


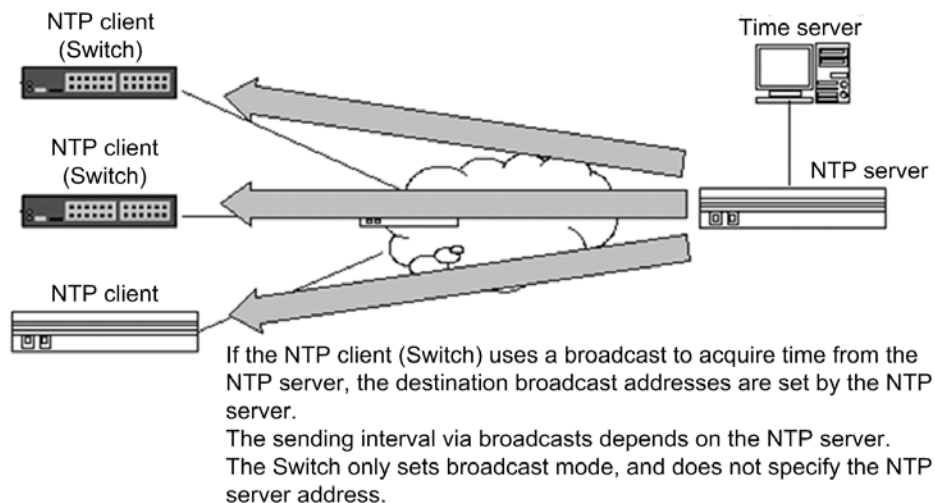
Figure 9-2 Overview of acquiring time information in unicast mode (when primary and secondary addresses are set)



(2) Acquiring the time information sent by broadcast (broadcast mode)

In broadcast mode, the Switch receives the time broadcast by the NTP server, and updates the internal clock time.

Figure 9-3 Overview of acquiring the time in broadcast mode



(3) Manual acquisition

The Switch internal clock time can be updated by executing an operation command set with an NTP server address to request the time from the NTP server. If an NTP server address is not specified, the Switch uses the address of the NTP server that has been set as the NTP server from which the time is to be requested periodically.

9.1.2 Notes on changing the time

The statistics on CPU usage collected by the Switch will be cleared to zero by any of the following operations:

- The Switch is restarted or the Switch is placed in sleep mode according to the schedule of the power saving functionality.
- The `clock timezone` configuration command is used to change the time zone.
- The time is changed by executing the `set clock` operation command or is changed on the NTP client (in this case, only the seconds digit is cleared to zero).

9.2 Configuration

9.2.1 Configuration commands

The following table describes the configuration commands related to time settings and NTP.

Table 9-3 List of configuration commands

Command name	Description
<code>clock timezone</code>	Sets the time zone.
<code>ntp broadcast client</code>	Sets acceptance of time information broadcast from an NTP server.
<code>ntp interval</code>	Sets the interval for regularly obtaining time information from an NTP server.
<code>ntp server</code>	Sets the address of the NTP server from which time information can be obtained.

9.2.2 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)# exit`
`# copy running-config startup-config`
`Do you wish to copy from running-config to startup-config? (y/n): y`
Moves from configuration mode to administrator mode, and saves the settings.
3. `# set clock 1102221530`
`Tue Feb 22 15:30:17 JST 2011`
`#`
Sets the date and time as 15:30 on February 22, 2011.

9.2.3 Acquiring the time periodically from the NTP server

The NTP client functionality can be used to acquire the time periodically from the NTP server.

Points to note

Set the address of the NTP server from which the time will be requested. The request interval can be set by using the `ntp interval` configuration command.

Command examples

1. `(config)# ntp server 192.168.1.100`
Sets the address of the NTP server from which the time will be requested.
2. `(config)# ntp interval 7200`

9 Time Settings and NTP

Sets the interval for requesting the time from the NTP server. If the `ntp interval` configuration command is not set, by default, the Switch issues a request every 3600 seconds (one hour).

9.3 Operation

9.3.1 List of operation commands

The following table describes the operation commands related to time settings and NTP.

Table 9-4 List of operation commands

Command name	Description
<code>set clock</code>	Shows and sets the date and time.
<code>set clock ntp</code>	Manually obtains the time from the NTP server.
<code>show clock</code>	Shows the current date and time.
<code>show ntp-client</code>	Shows the NTP client information.

9.3.2 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 9-4 Checking the time

```
> show clock
Tue Feb 22 15:30:24 JST 2011
>
```

9.3.3 Displaying the NTP client information

If the time is being acquired from the NTP server, the `show ntp-client` operation command can be used to display information about the NTP client. The following figures show examples.

Figure 9-5 Displaying the NTP client information

```
> show ntp-client
```

```
Date 2010/08/03 19:52:48 UTC
```

```
Last NTP Status
```

```
NTP-Server : 192.1.0.254, Source-Address : ---
```

```
Mode : Unicast, Lapsed time : 104(s), Offset : 1(s)
```

```
Activate NTP Client
```

```
NTP-Server : 192.1.0.254, Source-Address : ---
```

```
Mode : Unicast, Interval : 120(s)
```

```
NTP Execute History(Max 10 entry)
```

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

>

10. Host Names and DNS

This chapter explains host names and describes the Domain Name Service and its operation.

10.1 Description
10.2 Configuration

10.1 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 by using the operation commands `telnet`, `ftp` and `tftp`. 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.

10.2 Configuration

10.2.1 List of configuration commands

The following table describes the configuration commands for host names and the DNS.

Table 10-1 List of configuration commands

Command name	Description
<code>ip domain lookup</code>	Disables the DNS resolver functionality when <code>no ip domain lookup</code> is set.
<code>ip domain name</code>	Sets the domain name to be used by the DNS resolver.
<code>ip domain reverse-lookup</code>	Disables the reverse lookup functionality of the DNS resolver when <code>no ip domain reverse-lookup</code> is set.
<code>ip host</code>	Sets host name information mapped to an IPv4 address.
<code>ip name-server</code>	Sets the name server referenced by the DNS resolver.
<code>ipv6 host</code>	Sets host name information mapped to an IPv6 address.

10.2.2 Configuring host names

(1) Mapping a host name to an IPv4 address

Points to note

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

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.

10.2.3 Configuring DNS settings

(1) DNS resolver setting

Points to note

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 domainserver.example.com`

Sets the domain name as `domainserver.example.com`.

2. `(config)# ip name-server 192.168.0.1`

Sets the name server as 192.168.0.1.

(2) Disabling the DNS resolver

Points to note

Disable the DNS resolver functionality.

Command examples

1. `(config)# no ip domain lookup`

Disables the DNS resolver functionality.

11 . Device Management

This chapter describes the tasks involved in deploying and managing the Switch.

11.1 Settings related to status display and system operation

11.2 Backing up and restoring switch information

11.3 Failure recovery

11.1 Settings related to status display and system operation

11.1.1 List of configuration commands and operation commands

The following tables describe the configuration commands and operation commands needed to manage the switch.

Table 11-1 List of configuration commands

Command name	Description
<code>system fan mode</code>	Sets the operating mode of the fan.
<code>system l2-table mode</code>	Sets the search method for the Layer 2 hardware table.
<code>system memory-soft-error</code>	Sets output of a log message if a soft error occurs in SW (switch processor) subunit memory.
<code>system recovery</code>	Determines whether to restart the Switch if the Switch fails. If the <code>no system recovery</code> command is set, the Switch is not restarted and remains in the failure state.
<code>system temperature-warning-level</code>	Outputs an operation message if the intake temperature exceeds the specified temperature.
<code>system temperature-warning-level average</code>	Outputs an operation message if the average device temperature for the specified period exceeds the specified temperature.

Table 11-2 List of operation commands (software version and switch status check)

Command name	Description
<code>show version</code>	Shows information about the Switch software and the board installed.
<code>show system</code>	Shows the Switch's operating status.
<code>show environment</code>	Shows the fan status, the power unit status, the temperature status, and the cumulative operating time of the device.
<code>reload</code>	Restarts the switch.
<code>show tech-support</code>	Collects information, required for technical support, that shows the hardware and software status.

Table 11-3 List of operation commands (memory card and RAMDISK)

Command name	Description
<code>show mc</code>	Shows the memory card format and card usage.
<code>show mc-file</code>	Shows the names and sizes of the files on the memory card.
<code>show ramdisk</code>	Shows the RAMDISK format and usage.

Command name	Description
<code>show ramdisk-file</code>	Shows the names and sizes of the files on the RAMDISK.
<code>format flash</code>	Formats the internal flash memory file system.
<code>format mc</code>	Formats the memory card for use by the Switch.

Table 11-4 List of operation commands (logging control)

Command name	Description
<code>show logging</code>	Shows the log entries recorded by the Switch.
<code>clear logging</code>	Erases the log entries recorded by the Switch.
<code>show logging console</code>	Shows the contents set by the <code>set logging console</code> command.
<code>set logging console</code>	Controls the logging of operation messages by event level.
<code>show critical-logging</code>	Shows the detailed information regarding device fault log entries as log records.
<code>show critical-logging summary</code>	Shows a list of device fault log entries in reference code format.
<code>clear critical-logging</code>	Clears the device fault log entries recorded by the Switch.

Table 11-5 List of operation commands (resource information)

Command name	Description
<code>show cpu</code>	Shows CPU usage.
<code>show memory summary</code>	Shows the installed capacity, used capacity, and free capacity of the device's physical memory.

11.1.2 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 11-1 Checking the software version

```
> show version

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

>
```

11.1.3 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 11-2 Checking the switch status

```

> show system

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

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

File System
  < RAMDISK information >
    used      168,960 byte
    free      31,288,320 byte
    total     31,457,280 byte
  < RAMDISK files >
  File Date           Size Name
  2012/07/08 03:06    1,024 Config_File/
  2012/07/08 03:02    4,648 Test_Config.txt
  2012/07/08 03:06    6,196 Config_File/12Floor_Config.txt
  2012/07/08 03:02   14,964 Config_File/11Floor_Config.txt
  < MC information >
  MC : enable
  Manufacture ID : 00000003
    used      9,108,992 byte
    free      116,801,536 byte
    total     125,910,528 byte
  < MC files >
  File Date           Size Name
  2012/07/06 18:12    8,990,720 K.IMG
  2012/07/08 03:05    16,384 Config_File/
  2012/06/20 12:08    4,648 Test_Config.txt
  2012/05/04 10:30    6,196 Config_File/12Floor_Config.txt
  2012/07/05 20:17   14,964 Config_File/11Floor_Config.txt

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

  System Layer2 Table Mode : 1
  Flow detection mode : layer2-2

```

```

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

```

>

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 11-3 Checking the device environment

```
> show environment
```

```
Date 2012/07/27 18:12:36 UTC
```

```
Fan environment
```

```

Fan      : active
Speed    : normal
Mode     : 1 (silent)
EPU Fan  : -

```

```
Power environment
```

```

PS       : active
EPU      : notconnect

```

```
Temperature environment
```

```

Main      : 29 degrees C
Warning level : normal

```

```
Temperature-warning-level current status : 29/32 degrees C
```

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

```
Accumulated running time
```

```

total      : 320 days and 15 hours
critical   : 219 days and 6 hours

```

>

The `temperature-logging` parameter of the `show environment` operation command allows you to check the temperature log. An example is shown below:

Figure 11-4 Checking temperature log data

```
> show environment temperature-logging
```

```
Date 2010/12/16 21:54:23 UTC
```

```

Date      0:00  6:00 12:00 18:00
2010/12/16 30.0 30.3 28.0 27.8
2010/12/15 31.0 32.0 29.8 31.1
2010/12/14 -    -    29.2 30.0
2010/12/13 29.0 30.2 28.0 15.0
2010/12/12 28.8 30.0 30.0 28.0
2010/12/11 31.6 32.0 28.0 28.0
2010/12/10 31.0 30.1 28.9 29.8

```

2010/12/09 - - - 30.1

>

(1) Notes on support for Long Life Solution

Note the following when you configure the `system temperature-warning-level` configuration command or check the temperature information in the temperature history:

1. The temperature that is specified in the `system temperature-warning-level` configuration command is the air intake temperature of the switch. Therefore, the internal temperature of the Switch is converted to the air intake temperature, but an error might arise depending on the setting environment of the Switch, or the number of ports or the SFP type being used on the Switch.
2. Functionality supporting Long Life Solution starts monitoring 60 minutes after all configurations are applied at startup.

11.1.4 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, when the Switch is able to resume communication, an operation message reporting this fact is displayed. Similarly, if the Switch is no longer able to communicate, an operation message reporting this fact is displayed.

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 operation terminal.

Figure 11-5 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, the message **WARNING!! There are too many messages to output.** might be displayed on the console or remote operation terminal. This message indicates that some operation messages have not been displayed. Use the `show logging` operation command to check the operation messages.

11.1.5 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:

- User command operations and response messages
- Operation messages

A reference log contains error information and warnings about problems that occurred in the switch. The data is categorized by message ID, and shows for each event the time of the first and last occurrences, and the total number of occurrences.

This data is logged in text format inside the switch. To view the entries, use the `show logging` operation command.

11.2 Backing up and restoring switch information

If you have created a backup file containing switch information, you can restore the switch information from the backup file after a switch failure or replacement of the switch.

For details about the restore operation, see *11.2.2 Information that is backed up or restored*. You can also restore the information manually, but we do not recommend this because the switch handles a wide variety of switch information which is complicated to manage and cannot be fully restored.

11.2.1 List of operation commands

The following table describes the operation commands used for backing up and restoring information.

Table 11-6 List of operation commands

Command name	Description
<code>backup</code>	Saves switch information and information about active applications to a memory card, the RAMDISK, or a remote FTP server.
<code>restore</code>	Restores the switch information saved to a memory card, the RAMDISK, or a remote FTP server to the Switch.

11.2.2 Information that is backed up or restored

(1) Backing up information

Create a backup file by using the `backup` operation command at a time when the switch is running normally. The `backup` operation command places the information (described in the table below) that is required for switch operation in one file, and then saves that file to a memory card, the RAMDISK, or a remote FTP server.

We recommend that you create a backup file before updating any of this information.

Table 11-7 Switch information saved to a backup file

Type of switch information	Remarks
Software that is running	
Startup configuration file	
Login authentication user ID and password	<code>adduser</code> operation command <code>rmuser</code> operation command <code>password</code> operation command
CLI environment information	<code>set exec-timeout</code> operation command <code>set terminal pager</code> operation command
Password for administrator mode	<code>password enable-mode</code> operation command
Web authentication database	Internal Web authentication DB

Type of switch information	Remarks
Registered HTML files for Web authentication pages (Authentication page custom file sets that have been registered)	Custom file set of the basic Web authentication page Custom file set of the individual Web authentication page
Web authentication certificate file	
MAC-based authentication database	Internal MAC-based authentication DB
DHCP snooping binding database	
License information	set license operation command
Secure Wake-on-LAN terminal information database [OS-L2A]	WOL terminal information DB
Secure Wake-on-LAN user authentication database [OS-L2A]	WOL user authentication DB

Note that the [backup](#) operation command does not save the following information:

- Operation log entries and other log entries displayed by the [show logging](#) operation command

(2) Restoring information

To restore information from a backup file created by the [backup](#) operation command, use the [restore](#) operation command.

When you execute the [restore](#) operation command, the switch software is updated automatically from the software update files stored in the backup file. When updating finishes, the switch is automatically restarted. After the restart, the switch will operate in the restored environment.

Note the following when you execute the [restore](#) operation command:

1. When you use the [restore](#) operation command to restore information, always use the backup file that was created on the same switch model as the model of the switch on which the information will be restored.

To check the switch model, execute the [show version](#) operation command. The information displayed for [Model](#) is the model name.

2. Make sure that the version of the software used when the backup file was created is appropriate for the switch on which the information will be restored.
3. (This note applies when the software version of the destination switch is earlier than 3.1.A.) If you restore the operating information from a backup file meeting the following conditions, the login authentication user ID and password^{#1} will be initialized (login authentication user ID: [operator](#), password^{#1}: none).
 - The version of the software being used when the backup file was created was 3.1.A or later.
 - The login authentication user ID saved in the backup file has nine or more characters, or the password^{#1} saved in the backup file have 17 or more characters.

If either of the above conditions exists, log in as [operator](#), and then re-set the login authentication user ID and password^{#1}.

4. Depending on the version of the software used when a backup file is created, you need to set^{#2} an additional tag dedicated to Web authentication to a Web

authentication page replacement file.

#1

Passwords here means the login authentication password and the administrator password.

#2

The following table describes the setting of an additional tag dedicated to Web authentication.

Table 11-8 Setting of an additional tag dedicated to Web authentication

AX2530S version	Setting of an additional tag dedicated to Web authentication
Versions 3.0 to 3.4	Add the tag dedicated to Web authentication (" <code><!-- Original_URL --></code> ") to display the URL requested before authentication, after a successful login.
Versions 3.5 and later	No tag needs to be added.

For details about a Web authentication page replacement file and the tags dedicated to Web authentication, see *8 Description of Web Authentication* in the *Configuration Guide Vol. 2*.

11.3 Failure recovery

11.3.1 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 11-9 Error locations and recovery processing

Error location	Switch response	Recovery processing	Scope of effect	Switch
Main board	Makes six auto-recovery attempts in one hour. If a seventh error occurs after one hour elapses after six auto-recovery attempts, the switch stops. The number of auto-recovery attempts is reset one hour after the last recovery operation.	Restarts the switch. [#]	Communication via all ports on the switch is suspended.	Y
SW subunit	If a parity error occurs in internal memory, the switch attempts auto-recovery. If the same error occurs again after recovery, the switch restarts to initiate recovery.	Correctly reconfigures the affected location. [#]	Communication will be affected.	Y
Port failure	Makes an unlimited number of auto-recovery attempts.	Reconfigures and re-initializes the applicable port.	Communication via the applicable port might be affected.	Y
Power failure	Restarts when the power required to run the switch ceases to be supplied.	Restarts the switch.	Communication via all ports on the device is suspended.	Y
Fan	Performs nothing.	There is no means of auto-recovery.	Nothing is affected.	--

Legend

Y: Restored automatically.

--: Not restored automatically.

#

If you have disabled restoration processing by using the **no system recovery** configuration command, auto-recovery will not be performed even if a critical failure occurs (an E9-level failure is logged).

(1) Disabling auto-recovery

Auto-recovery no longer operates if system recovery is disabled (**no system recovery**). If a critical failure (E9-level failure) occurs, the switch will not be restarted after the failure is logged. In such cases, the ST1 LED lights red, all ports are placed in the link-down state, and communication stops.

If the power saving functionality is scheduled, the schedule is disabled to stop the operation of the scheduled power saving functionality (LED operation, port power saving, or sleep mode).

If a critical failure (E9-level failure) occurs when the Switch is in sleep mode with the

wake-up option enabled, the Switch restarts.

(a) Collection of device status information when auto-recovery is disabled

If auto-recovery has been disabled, execute the `show tech-support` operation command from the console to obtain the device status information in order to restore the Switch.

If the `show tech-support` operation command is executed when auto-recovery is disabled, information can be displayed only on the console. Accordingly, do not specify the `ramdisk` or `page` option when executing the command. If you need to record the information that is displayed on the console by the command, you can use the terminal's capture functionality.

Note the following when auto-recovery of the Switch is disabled:

- Do not update the software version while auto-recovery is disabled. If you need to update the software version, do so after the Switch has been restored.
- Commands might not be executed normally while auto-recovery is disabled.

(b) Switch recovery

Auto-recovery of the Switch will be re-enabled by one of the following operations:

- Restarting the Switch by turning it off and then on again, or pressing the RESET button.
- If the software is not responding when auto-recovery has been disabled, perform a hard reset to restart the Switch.

12. Power Saving Functionality

This chapter describes the power saving functionality provided by Switches, and the Switch settings.

- | |
|--|
| 12.1 Description of the power saving functionality |
| 12.2 Configuration of the power saving functionality |
| 12.3 Operation of the power saving functionality |

12.1 Description of the power saving functionality

The power consumption of a Switch can be reduced by using the power saving functionality to place the Switch in sleep state at night or during vacations according to a schedule.

12.1.1 Supported functionality

The power saving functionality supported by Switches can be enabled either continuously or during specific time ranges according to a schedule. The table below describes the power saving functionality that is available during time ranges that have been scheduled and time ranges that have not been scheduled.

The set time ranges when power saving functionality is enabled are referred to as the scheduled time ranges, and the time ranges when power saving functionality is not enabled are referred to as the normal time ranges.

Table 12-1 Supported power saving functionality

Functionality		Description	Availability during normal time ranges	Availability during scheduled time ranges
LED behavior control	LED brightness setting	Normal brightness, power saving brightness, and OFF	Y	Y
		Trigger for automatic behavior control	Y	N
Port power saving		Power saving functionality for a link-down port [#]	Y	Y
		Port blocking (setting for unused ports)	Y	Y
Sleep mode	Basic operations	Power supply to the Switch (sleep state) When a scheduled time range ends, the Switch automatically wakes.	N	Y
Wake-up option	Detection of an incoming WOL packet	Condition for waking the Switch from a sleep state: A WOL packet is received from the specified port.	N	Y
	Detection of the link-up state on a port	Condition for waking the Switch from a sleep state: The link-up state for the specified port is detected.	N	Y
Cooling fan control functionality (semi-fanless operation) [48T] [48TD]		Turning on or off the cooling fan in response to changes in temperature	Y	N
Power consumption information indication		Displaying power consumption information for the Switch	--	--

Legend

Y: Supported

N: Not supported

--: Not applicable

#

Supported only for 10BASE-T, 100BASE-TX, and 1000BASE-T ports.

SFP ports and shared SFP/SFP+ ports [10G model] do not support the power saving functionality for link-down ports.

12.1.2 LED behavior control

LED behavior can be controlled at three levels by changing configuration entries. The LED behavior can also be changed automatically by configuring triggers for automatic behavior control.

(1) LED behavior details

You can use the [system port - led](#) configuration command to set one of the following levels of LED brightness.

- Normal brightness: Activated LEDs are either on or blinking at normal brightness.
- Power saving brightness: Activated LEDs are either on or blinking at a lower brightness than normal brightness.
- OFF: The LEDs of all ports are turned off. (The ST1, ST2, and ACC LEDs sometimes remain on at a lower brightness.)

The LEDs for which brightness can be controlled are listed below. The behavior of the PWR LED cannot be controlled. When this LED is on, it is always on at normal brightness. For details about the LEDs, see the *Hardware Instruction Manual*.

- ST1
- ST2
- ACC
- LINK
- T/R
- 1 to 24 (for AX2530S-24T, AX2530S-24TD, and AX2530S-24T4X models)
- 1 to 48 (for AX2530S-48T, AX2530S-48TD, and AX2530S-48T2X models)

The following table describes the status of each LED according to the LED behavior setting specified by using the [system port - led](#) configuration command.

Table 12-2 Status of each LED according to the LED behavior setting specified by the configuration command

LED type	Switch status	Setting specified by the system port-led configuration command					
		Normal brightness (enable)		Power saving brightness (economy)		OFF (disable)	
		LED status	Brightness	LED status	Brightness	LED status	Brightness
ST1	Ready	Lit in green	Normal	Lit in green	Low	Slow blinking green	Low
	Not ready	Blinking green	Normal	Blinking green	Normal	Blinking green	Normal
	Initial status	Lit in orange	Normal	Lit in orange	Normal	Lit in orange	Normal
	Partial failure	Blinking red	Normal	Blinking red	Low	Blinking red	Low
	Fatal failure	Lit in red	Normal	Lit in red	Low	Lit in red	Low
	Power off or power failure	Off	--	Off	--	Off	--
ST2	Operating normally	Off	--	Off	--	Off	--
	SML full ^{#1}	Lit in green	Normal	Lit in green	Low	Lit in green	Low
	SML conflict, ^{#1} SML standalone ^{#1}	Blinking green	Normal	Blinking green	Low	Blinking green	Low
	Initial status	Lit in orange	Normal	Lit in orange	Normal	Lit in orange	Normal
ACC	Accessing	Lit in green	Normal	Lit in green	Low	Lit in green	Low
	Idle	Off	--	Off	--	Off	--
LINK ^{#2}	A link has been established.	Lit in green	Normal	Lit in green	Low	Off	--
	A link has not been established.	Off	--	Off	--	Off	--
	Problem	Off	--	Off	--	Off	--

LED type	Switch status	Setting specified by the system port-led configuration command					
		Normal brightness (enable)		Power saving brightness (economy)		OFF (disable)	
		LED status	Brightness	LED status	Brightness	LED status	Brightness
T/R ^{#2}	Sending or receiving	Blinking green	Normal	Blinking green	Low	Off	--
	Problem	Off	--	Off	--	Off	--
1-24 ^{#3}	A link has been established.	Lit in green	Normal	Lit in green	Low	Off	--
1-48 ^{#3}	Sending or receiving	Blinking green	Normal	Blinking green	Low	Off	--
	Problem	Off	--	Off	--	Off	--

#1

For details about SML, see *SML (Split Multi Link) [OS-L2A]* in the manual *Configuration Guide Vol. 2*.

#2

SFP ports or shared SFP/SFP+ ports [10G model]

#3

10BASE-T, 100BASE-TX, or 1000BASE-T ports

(2) Triggers for automatic LED behavior control

LED behavior can be changed automatically if the triggers for automatic behavior control have been set by using the [system port-led trigger](#) configuration command. For details, see *Table 12-3 Triggers for automatic behavior control*. For this operation, make sure you set normal brightness ([enable](#)) for the [system port-led](#) configuration command.

The following table describes the triggers for automatic behavior control.

Table 12-3 Triggers for automatic behavior control

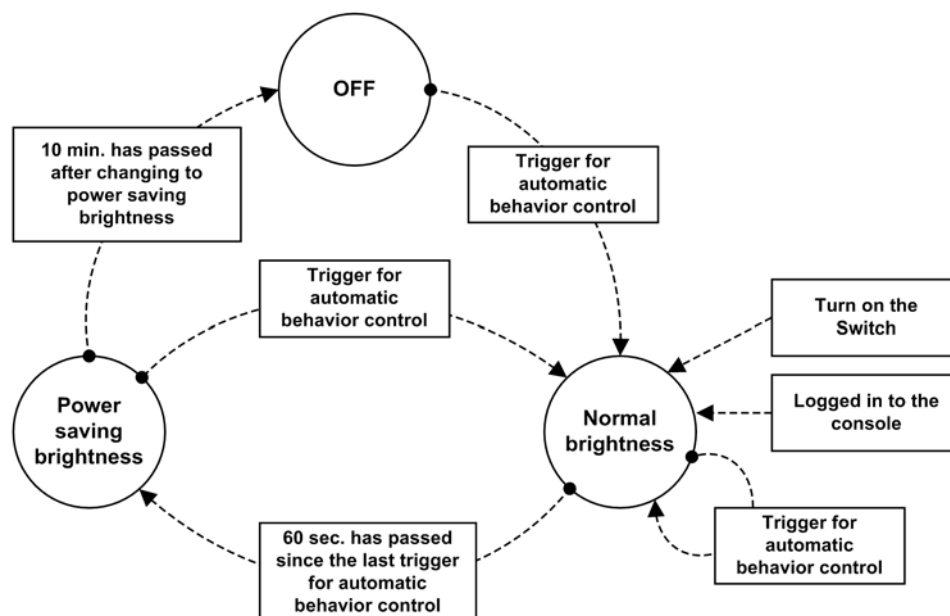
Trigger	Description
Console (RS232C)	When login to the Switch via a console connection is successful, the LED brightness level changes to normal brightness. For the entire login period, timer control stops, and the LED remains at normal brightness. After logout, the brightness level changes to power saving brightness or OFF according to timer control.
Memory card	When a memory card is inserted or removed, the LED brightness level changes to normal brightness. The brightness level changes to power saving brightness or OFF under timer control.
Physical port	When the link-up or link-down state of the specified physical port is detected, the LED brightness level changes to normal brightness.

Trigger	Description
	The brightness level changes to power saving brightness or OFF under timer control.

You can set multiple triggers to perform automatic behavior control.

The following figure shows the transitions for automatic LED behavior control.

Figure 12-1 Transitions for automatic LED brightness control



Note that although the triggers for automatic LED behavior control operate as described in *Table 12-3 Triggers for automatic behavior control*, transitions depend on the specific trigger and the timer.

1. Condition for changing the brightness level to normal brightness

Transition of the brightness level to normal brightness follows *Table 12-3 Triggers for automatic behavior control*.

2. Condition for changing the brightness level to power saving brightness

Transition of the brightness level from normal brightness to power saving brightness is controlled by the timer. When 60 seconds have passed since activation of the last trigger for automatic LED behavior control, the brightness level changes to power saving brightness.

Even when triggers for changing the brightness level to normal brightness occur continuously, the level changes to power saving brightness only after 60 seconds have passed since activation of the last trigger.

3. Condition for changing the brightness level to OFF

Transition of the brightness level to OFF is controlled by the timer. The brightness level changes to OFF when 10 minutes have passed since the last time the level changed to power saving brightness.

Note that the brightness level does not change from normal brightness to OFF.

The table below describes the LEDs whose behavior can be controlled automatically. Note that the brightness of the PWR LED cannot be controlled. When this LED is on, the brightness level is always normal brightness.

Table 12-4 LEDs subject to automatic behavior control and the scope of control

LED type	Type and scope of automatic LED behavior control			Description
	Normal brightness	Power saving brightness	OFF	
ST1	Y	Y	--	When the brightness is set to power saving brightness or OFF, the LED is lit at low-level brightness.
ST2				
ACC				
LINK ^{#1}			Y	The brightness level changes to one of three levels.
T/R ^{#1}				
1-24 ^{#2} 1-48 ^{#2}				

Legend

Y: Controlled

--: Not controlled

#1

LED for an SFP port or a shared SFP/SFP+ port [10G model]

#2

LED for a 10BASE-T, 100BASE-TX, or 1000BASE-T port

12.1.3 Port power saving

The port power saving functionality reduces the power to Ethernet ports that are inactive.

The port power saving functionality is able to perform the following operations:

- Power saving functionality for link-down ports
- Port blocking

(1) Power saving functionality for link-down ports

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 the `power-control port cool-standby` configuration command 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, and 1000BASE-T ports. SFP ports and shared SFP/SFP+ ports [10G model] do not support the power saving functionality for link-down ports.

The following table describes the conditions under which power saving for link-down ports is enabled.

Table 12-5 Conditions under which power saving for link-down ports is enabled

Configuration settings	shutdown [#]		no shutdown	
	Detection of an electrical signal		Detection of an electrical signal	
	None	Yes	None	Yes
power-control port cool-standby	Y (link-down)	Y (link-down)	Y (link-down)	-- (link-up)
no power-control port cool-standby	Y (link-down)	Y (link-down)	-- (link-down)	-- (link-up)

Legend

Y: Power saving functionality for link-down ports is enabled, and ports operate at reduced power.

--: Power saving functionality for link-down ports is disabled, and ports operate at normal power.

#

Applies to the `shutdown` configuration command or the `ifAdminStatus Set` specification in the `SetRequest` operation performed from the SNMP manager.

(2) Port blocking

You can block unused ports to reduce power consumption by using the `shutdown` configuration command to shut down the ports.

You can also use this functionality with the power saving functionality for link-down ports (see (1) *Power saving functionality for link-down ports*).

12.1.4 Sleep mode

Switches enter or exit sleep mode by scheduling the power saving functionality. For details about the schedule, see 12.1.6 *Scheduling power saving functionality*.

In principle, the sleep functionality turns a Switch off or on at a specific time. While the Switch is in sleep mode, the PWR LED blinks green slowly, and all Switch functionality, including switching (frame forwarding) and remote access, is disabled.

In addition to schedule-based wake-up, the sleep functionality also provides the administrator with the following means for intentionally waking the Switch:

- Forced cancellation of sleep mode: Holding down the RESET button on the front of the Switch wakes the Switch.
- Wake-up option: option that wakes the Switch when a WOL packet bound to the Switch from a specific port is detected
- Wake-up option: option that wakes the Switch when a link-up state for a specified port is detected

If you want to forcibly cancel sleep mode, you must manually operate the Switch. However, wake-up options can be enabled remotely by configuration.

(1) Forced cancellation of sleep mode

When the Switch is in sleep mode, hold down the RESET button on the Switch for at least three seconds until all LEDs on the front of the Switch turn on. This operation cancels sleep mode. The Switch wakes in schedule-disabled mode.

Note that if a wake-up option described below is set, the Switch attempts the wake-up even when the RESET button is not held down. However, if the attempt is made while the Switch

is scheduled to sleep, the Switch stops the wake-up.

(2) Wake-up option: option that wakes the Switch when an incoming WOL packet is detected

When the option that wakes the Switch on detection of an incoming WOL packet is enabled and such a packet is detected, the Switch wakes. However, when the time scheduled for enabling the power saving functionality arrives, the Switch returns to sleep mode in accordance with the basic principle.

The ports set as monitoring ports for incoming WOL packets discard all incoming packets other than WOL packets, and do not forward any packets to other ports.

When one of the monitoring ports detects a WOL packet, the Switch wakes.

If the Switch wakes when an incoming WOL packet is detected, the Switch starts in schedule-disabled mode.

(a) Combinations of ports that can be set as monitoring ports for incoming WOL packets

The ports that can monitor for incoming WOL packets when the Switch is in sleep mode and the option that wakes the Switch when an incoming WOL packet is detected is enabled differ depending on the model as described in *Table 12-6 Combinations of ports that can be set as ports to monitor for incoming WOL packets*.

As the ports to monitor for incoming WOL packets, you can select a maximum of two ports per Switch from among the last two 10BASE-T, 100BASE-TX, or 1000BASE-T ports and the first two SFP ports. Note, however, that possible combinations are limited. Also note that for AX2530S-24S4X, the only ports that can be used are 0/23 and 0/24.

For example, a combination of 10BASE-T, 100BASE-TX, or 1000BASE-T port 0/23 and SFP port 0/25 is not possible because this combination is not indicated as a possible combination in *Table 12-6 Combinations of ports that can be set as ports to monitor for incoming WOL packets*.

Table 12-6 Combinations of ports that can be set as ports to monitor for incoming WOL packets

Model	10BASE-T, 100BASE-TX, or 1000BASE-T port			SFP port				Shared SFP/SFP+ port
AX2530S-24T AX2530S-24TD	0/1 to 0/22	0/23	0/24	--	0/25	0/26	0/27 to 0/28	--
AX2530S-24T4X	0/1 to 0/22	0/23	0/24	--	--	--	--	0/25 to 0/28
AX2530S-48T AX2530S-48TD	0/1 to 0/46	0/47	0/48	--	0/49	0/50	0/51 to 0/52	--
AX2530S-48T2X	0/1 to 0/46	0/47	0/48	--	0/49	0/50	--	0/51 to 0/52
AX2530S-24S4X AX2530S-24S4X D	--	--	--	0/1 to 0/22	0/23	0/24	--	0/25 to 0/28
Port selection (two ports)	N	Y	Y	N	--	--	N	N
	N	--	--	N	Y	Y	N	N
	N	Y	--	N	--	Y	N	N
	N	--	Y	N	Y	--	N	N
Port selection (one port)	N	Y	--	N	--	--	N	N
	N	--	Y	N	--	--	N	N
	N	--	--	N	Y	--	N	N
	N	--	--	N	--	Y	N	N

Legend

Y: Selection is possible.

N: Selection is impossible.

--: Not applicable

Note that you need to configure the settings in such a way that the option is enabled on a port basis. Configuration is complete only when a possible combination of ports is configured. If an impossible combination of ports is configured, a configuration error message is output.

(b) Wake-up conditions

The Switch wakes when one of the ports monitoring for WOL packets receives a packet that contains a broadcast MAC address followed by consecutive 16 system MAC addresses of the Switch.

Note that at least one minute is required for the Switch to become ready for use.

(3) Wake-up option: option that wakes the Switch when a link-up state is detected

If the option that wakes the Switch when a port link-up state is detected is enabled and all of the following conditions are satisfied, the Switch wakes up:

1. The scheduled time for waking the Switch arrives.
2. All ports set to monitor for a link-up state are in a link-down state.
3. The statuses in condition 1 and 2 continues at least five minutes (default).

The link-down state continuation time used as the threshold can be changed by a configuration setting.

If the Switch wakes when a link-up state for a specific port is detected, the Switch starts in schedule-enabled mode.

(a) Ports that can monitor for a link-up state

All ports can monitor for a link-up state.

(b) Wake-up conditions

When a link-up state is detected on at least one of the ports that changes to the link-up state, the Switch wakes.

Note that at least one minute is required for the Switch to become ready for use.

(4) Special wake-up conditions for wake-up options

If a transceiver (SFP or SFP+) is inserted while the Switch is in sleep mode with a wake-up option enabled, the Switch wakes. However, the Switch does not wake up if a transceiver is removed.

If the Switch wakes when insertion of a transceiver is detected, the Switch starts in schedule-enabled mode. Therefore, after the Switch has been awakened by inserting a transceiver, if the scheduled time for enabling the power saving functionality arrives, the Switch will resume sleep mode.

The following table describes the ports that can monitor for insertion of a transceiver.

Table 12-7 Ports that can monitor for insertion of a transceiver

Model	Ports that can monitor for insertion of a transceiver	Remarks
AX2530S-24T AX2530S-24TD AX2530S-24T4X	0/25 to 0/28	Only ports for which the option that wakes the Switch when a WOL packet is detected or when a port link-up state is detected is enabled can monitor for insertion of a transceiver.
AX2530S-48T AX2530S-48TD AX2530S-48T2X	0/49 to 0/52	
AX2530S-24S4X AX2530S-24S4XD	0/1 to 0/28	

12.1.5 Cooling fan control functionality (semi-fanless operation) [48T] [48TD]

The cooling fan functionality stops fans in an environment that is determined to be acceptable by internal temperature monitoring and in which forced cooling of the device is not required. The functionality also turns on the fans to start forced cooling when the ambient temperature is too high (semi-fanless operation). This can prevent noise and reduce power consumption.

This functionality is enabled by executing the `system fan-control` configuration command. (If this command is not specified, the fans run continuously.)

Conditions that will cause the fans to start and stop when using this configuration command:

- Start conditions: When an internal temperature of 74 degrees Celsius or higher is detected
- Stop conditions: When an internal temperature of 73 degrees Celsius or lower continues for 10 minutes

This functionality is supported by the AX2530S-48T model only. Even if you start the device with this functionality enabled, the cooling fans always run for approximately 10 minutes immediately after the device starts.

Note that if both this functionality and the Long Life Solution fan operation mode (`system fan mode`) are enabled, the Long Life Solution fan operation mode (`system fan mode`) takes precedence.

The following table describes how fans operate if both this functionality and the fan operation mode are enabled concurrently.

Table 12-8 How fans operate if both this functionality and the fan operation mode are enabled concurrently

Semi-fanless operation (<code>system fan-control</code>)	Fan operation mode setting (<code>system fan mode</code>)	Fan operating status	Remarks
Enabled	<code>system fan mode 2</code>	Always-on operation	Equivalent to the cooling-critical setting (<code>system fan-control</code> disabled)
	<code>system fan mode 1</code> or nothing	Semi-fanless operation	
Disabled	<code>system fan mode 2</code>	Always-on operation	Equivalent to the cooling-critical setting
	<code>system fan mode 1</code> or nothing	Always-on operation	

12.1.6 Scheduling power saving functionality

You can schedule the power saving functionality to run for a specific time range. Scheduling allows you to specify a combination of types of power saving functionality and the time range during which they are to be enabled. When the specified start time arrives, power saving functionality is initiated automatically. Once you have scheduled the power saving functionality, you can also disable it for a particular time range. A set time range when power saving functionality is enabled is referred to as a scheduled time range and a time when power saving functionality is not enabled is referred to as a normal time range.

(1) Specifiable power saving functionality

To set up a power saving schedule, specify the types of functionality and the time range for which they are to be enabled. The power saving functionality available for user-defined power saving is listed below. To schedule power saving functionality, select one or more types of functionality that you want to enable concurrently according to your requirements.

A Switch only allows one combination of the different functionality types to be specified for scheduling.

- LED behavior control
- Port power saving
- Sleep mode

(a) Scheduled LED brightness behavior control

This functionality changes the LED brightness, on a scheduled time range basis, according to a schedule.

How the LEDs behave can be set separately for normal time ranges and scheduled time ranges. The trigger settings for starting automatic LED behavior control are common to both normal and scheduled time ranges.

Table 12-9 LED behavior settings for scheduled time ranges and LED behavior

LED behavior settings for scheduled time ranges	Configuration common to both normal and scheduled time ranges	
	When triggers for automatic LED behavior control have been set	When triggers for automatic LED behavior control have not been set
Command not set	Automatic	Normal brightness
Normal brightness	Automatic	Normal brightness
Power saving brightness	Power saving brightness	Power saving brightness
OFF	OFF	OFF

(b) Scheduled port power saving

This functionality implements power saving for ports in scheduled time ranges according to a schedule.

(c) Sleep functionality

This functionality places the Switch in sleep mode in scheduled time ranges according to a schedule. The functionality wakes the Switch in normal time ranges. The functionality allows you to plan a power saving schedule for the Switch that takes into account long holidays, weekends, public holidays, and evenings.

(2) Mode in which the Switch wakes

You can use the `set power-control schedule` operation command to select either of the following modes to be used when the Switch wakes:

- Schedule-enabled mode

In this mode, the settings for the normal time range and the scheduled time range are both applied. In scheduled time ranges, the settings for scheduled time ranges are applied. In other time ranges, the settings for normal time ranges are applied.

When a scheduled time range expires or the Switch wakes because a port link-up state has been detected, the Switch operates in schedule-enabled mode.

- Schedule-disabled mode

In this mode, only the settings for normal time ranges are applied. The settings for normal time ranges are applied even in a scheduled time range.

The schedule-disabled mode is applied when sleep mode is forcibly canceled by holding down the RESET button or when the Switch wakes because an incoming WOL packet has been detected.

Note that schedule-disabled mode automatically switches to schedule-enabled mode when a normal time range arrives.

(3) Scheduling power saving

Set the time range when the switch is to operate in power saving mode. Specify the start time and end time in any of the following ways:

- Enabling power saving by date and time
- Enabling power saving by day of the week and time
- Enabling power saving by daily time range
- Disabling power saving by date and time

You can use these methods in combination to enable or disable power saving functionality at various times.

You can use the `schedul e-power-control time-range` configuration command to set a maximum of 50 scheduled time ranges.

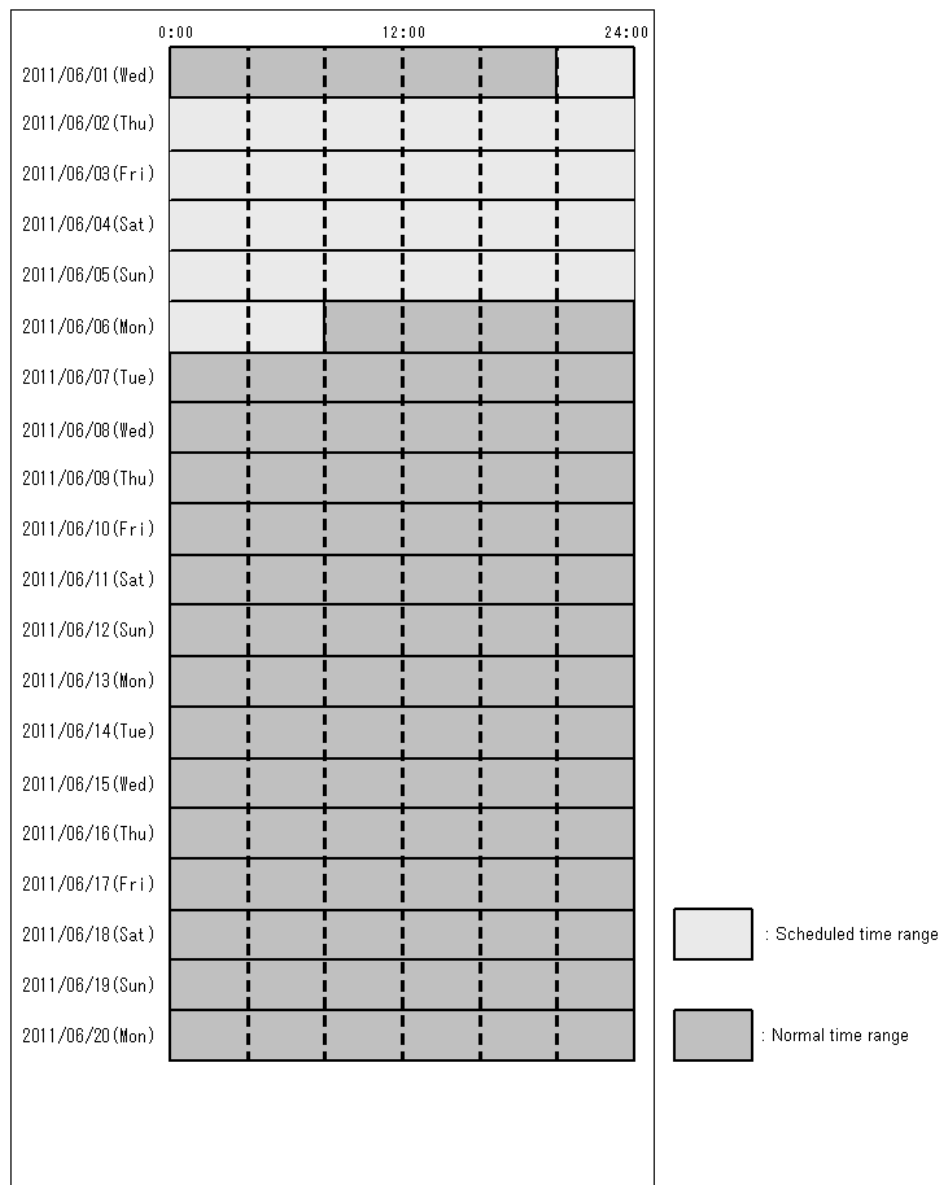
(a) Enabling power saving by date and time

Specify the start and end dates and times for implementing power saving.

Example:

From June 2 to June 5, 2011, the business system will have a reduced workload. In line with this expectation, schedule power saving from 20:00 on June 1 to 8:00 on June 6, 2011. The following figure shows the operation schedule.

Figure 12-2 Power saving schedule (by date)



(b) Enabling power saving by day of the week and time

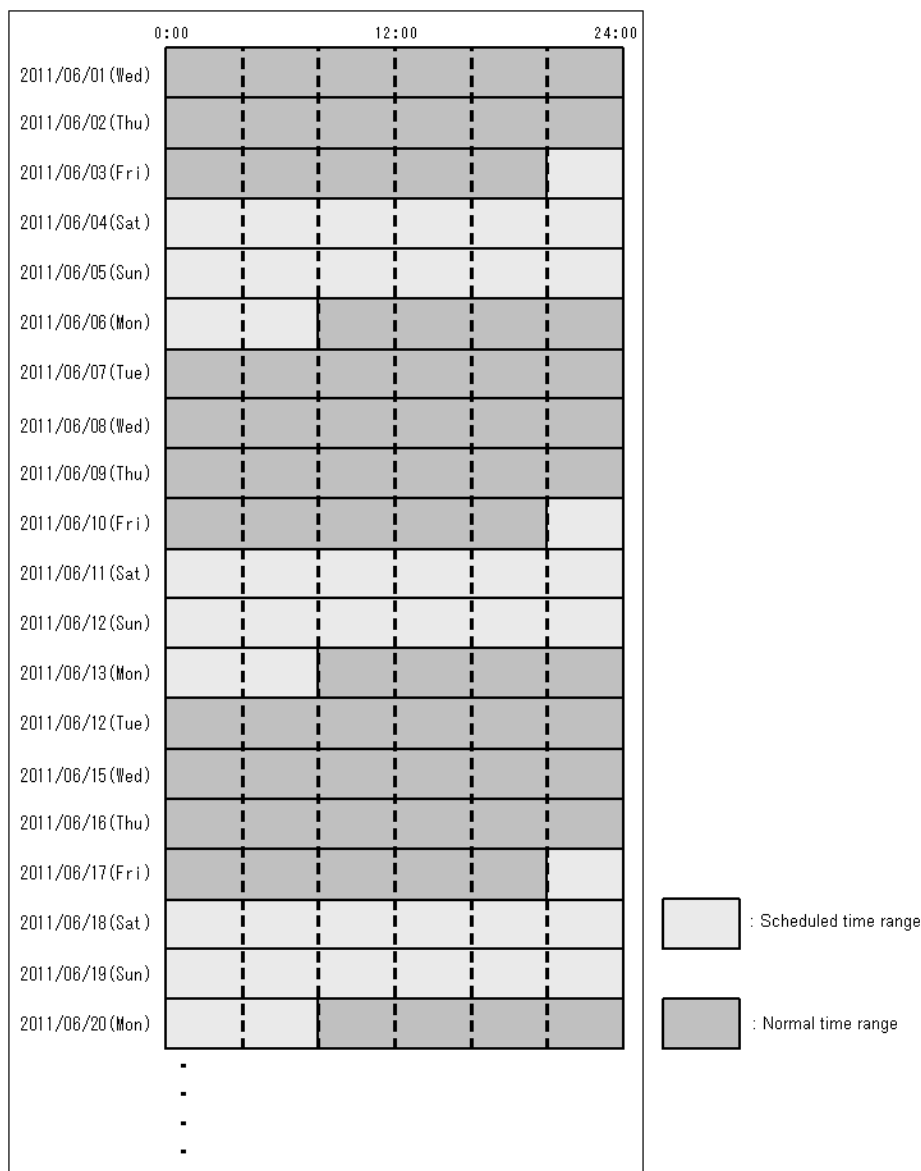
Specify the start and end days of the week and times for implementing power saving.

Example:

The office is closed every Saturday and Sunday, and the business system has a reduced workload on these two days. Therefore, schedule power saving from 20:00

every Friday to 8:00 every Monday. The following figure shows the operation schedule.

Figure 12-3 Power saving schedule (by day of the week)

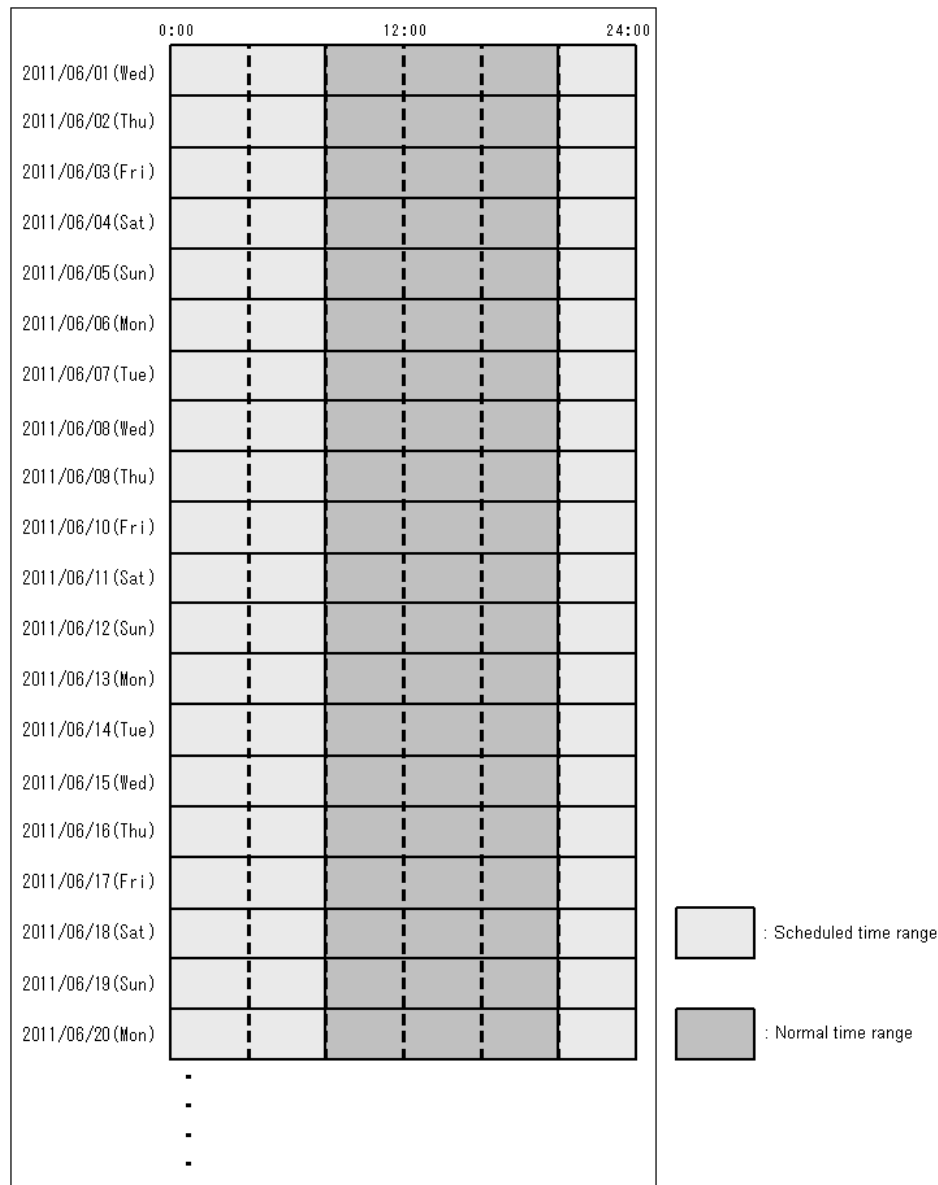


(c) Enabling power saving by daily time range

Specify the start time and end time for implementing power saving.

Example:

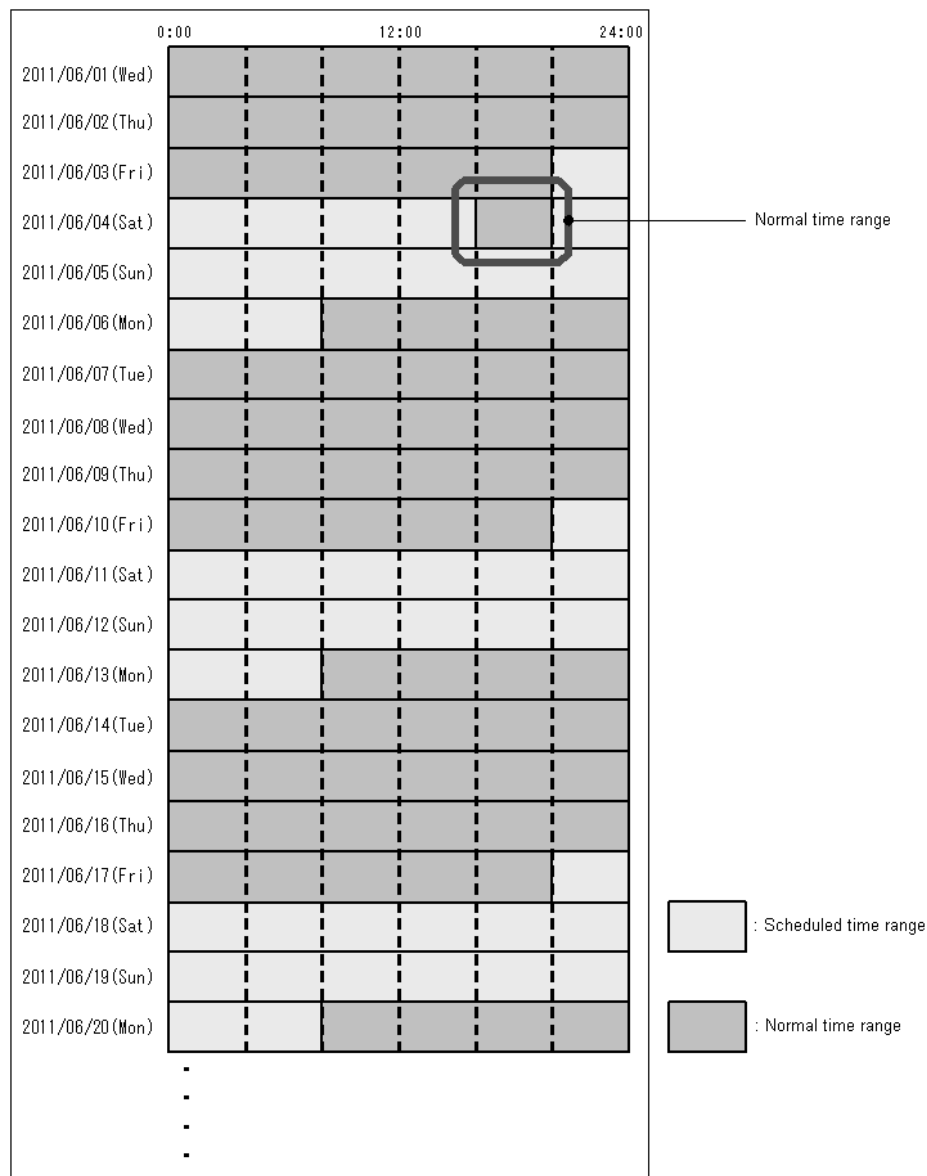
Normal office hours are from 8:30 to 17:00 every day, so the business system needs to operate at normal power from 8:00 to 20:00. Schedule power saving from 20:00 every day to 8:00 the following day. The following figure shows the operation schedule.

Figure 12-4 Power saving schedule (daily)**(d) Disabling power saving by date and time**

You can disable the power saving functionality 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 saving 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 June 4, 2011. The following figure shows the operation schedule.

Figure 12-5 Power saving schedule (disable)

12.1.7 Obtaining and displaying power consumption information

A Switch periodically obtains power consumption information. You can display this information by using the [show power](#) operation command to check the power saving results. You can also use private MIBs to obtain power consumption information.

The following table describes the items that can be displayed.

Table 12-10 Items that can be displayed as power consumption information

Item	Description	Operation commands	MIB
Current power consumption	Power consumption information obtained by using an operation command or a MIB	Y	Y
Power consumption for the last 24 hours	Power consumption for the last 24 hours obtained from the power consumption information checked at one-hour intervals (fixed) since startup of the Switch	Y	N

Item	Description	Operation commands	MIB
Cumulative power consumption	The total of power consumption measured at one-hour intervals (fixed) since startup of the Switch	Y	Y

Legend

Y: This item is displayed.

N: This item is not displayed.

For details about MIBs (private MIBs), see the *MIB Reference*.

Power consumption is monitored even when a Switch is in sleep mode.

Note that acquired information is stored in volatile memory (RAM) on the Switch. Although the information is lost when the Switch is turned off, it is retained if the Switch is restarted without turning off the power.

Table 12-11 Conditions under which power consumption information is retained

Restart means	Whether information is retained or lost	Remarks
Power is turned off and on	Lost	The power is turned off when, for example, regular maintenance is performed.
The reload operation command is executed.	Retained	This is a restart by an operation command.
The RESET button is pressed.	Retained	This is a restart initiated by pressing the RESET button.
The Switch is restarted because of a failure.	Retained	This is a restart executed automatically when a software or hardware failure occurs.

12.1.8 Notes on using the power saving functionality

(1) Scheduling power saving functionality

To use the same power saving functionality during a normal time range and a scheduled time range, specify settings for both time ranges.

Example:

If you want to block a port during a normal time range, you need to set the **shutdown** configuration command. Similarly, if you also want to block the port during a scheduled time range, you need to set the **schedule power-control shutdown** configuration command.

(2) Time lag in starting and ending power saving functionality

Because scheduling uses a software timer, a situation such as 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 a port resumes at the end of a scheduled time range in which the port is blocked. Allow a certain margin when you schedule the power saving functionality.

(3) Placing a Switch in sleep mode

Note the following points if you schedule the sleep functionality:

1. The Switch does not go into sleep mode if entering the scheduled time range in configuration command mode during operation in configuration command mode. The Switch goes into sleep mode after exiting configuration command mode (after moving to administrator mode).
2. If entering the scheduled time range 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.
3. An unsaved configuration will be discarded when going into sleep mode. The following confirmation message appears when exiting configuration command mode.

Unsaved changes would be lost when the machine goes to sleep!

Do you exit "configure" without save ? (y/n):

Press **n**, and then execute the **save** command. The changes are saved.

4. If there is no key input for a specified period (default: 60 minutes), you are automatically logged out. If automatic logout occurs while editing a configuration, an unsaved configuration is discarded.
5. The Switch automatically wakes up from sleep mode and restarts once in 20 days. Then, it goes into sleep mode again after startup. (Automatic wake-up as described here does not occur if a wake-up option is enabled.)
6. 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 ranges.
7. If the sleep functionality is used, the Switch is placed in sleep mode when a scheduled time range arrives. Therefore, the following commands do not take effect if they have been set:
 - **schedule power-control port-led**
 - **schedule power-control port cool-standby**
 - **schedule power-control shutdown**

(a) Sleep mode and scheduled time ranges with "infinity" specified

The infinity specification for scheduled time ranges assumes that a setting that detects a link-up state for waking the Switch is also used. With the infinity specification, the Switch can be awakened (in schedule-enabled mode) by placing a port in the link-up state only when the Switch needs to be used. After the Switch has been used, it can be made to sleep automatically by placing the port into the link-down state.

If you do not enable the option for detecting a port link-up state, sleep mode is canceled in the cases listed below. However, in these cases, the Switch wakes in schedule-disabled mode.

- If sleep mode is set without any wake-up option enabled:
When the RESET button on the front of the Switch is held down (forced cancellation of sleep mode)
- If the option that wakes the Switch when detecting an incoming WOL packet is enabled:
When an incoming WOL packet is detected
When the RESET button on the front of the Switch is held down (forced cancellation of sleep mode)

If infinity is specified, schedule-disabled mode is not canceled automatically. For the Switch to sleep again, schedule-disabled mode must be changed to schedule-enabled mode by using the **set power-control schedule** operation command.

(4) When enabling a wake-up option for sleep mode

1. Wake-up options are enabled when sleep mode is set.
2. The ports for which a wake-up option is enabled assume that **no shutdown** is set.
3. While the Switch is in sleep mode with a wake-up option enabled, the Switch only monitors whether a wake-up condition is satisfied, and accepts no communication or operations from the console.
4. If a wake-up option is enabled for Switch ports, the ports are active even while the Switch is in sleep mode. Therefore, power consumption in sleep mode increases compared with when no wake-up option is enabled.
5. If a wake-up option is enabled for sleep mode of a Switch model equipped with fans, the Switch operates as follows:
 - [48T] [48TD] During scheduled time ranges, Switch operation is equivalent to that of semi-fanless models. (Fans always operate during normal time ranges, but the Switch operates in the same way as a semi-fanless model during scheduled time ranges.)
 - [10G model] Fans always operate during normal and scheduled time ranges.
6. If a wake-up option is enabled, it takes the Switch about one minute to be able to detect the applicable wake-up condition after the Switch enters sleep mode. (This also applies for a condition in *Special wake-up conditions for wake-up options*.)

(a) Wake-up option: If the option that wakes the Switch when an incoming WOL packet is detected is enabled

1. When the wake-up condition is satisfied, the Switch wakes in schedule-disabled mode. However, the mode automatically switches to schedule-enabled mode when a normal time range arrives.
2. Make sure the line speed of a port that is used to detect an incoming WOL packet is the same as the line speed of the partner device. If you choose to use the default setting (auto-negotiation), make sure auto-negotiation is also set on the partner device.

(b) Wake-up option: If the option that wakes the Switch when a port link-up state is detected is enabled

1. When the wake-up condition is satisfied, the Switch wakes in schedule-enabled mode. Therefore, if the settings for normal time ranges are different from the settings for scheduled time ranges, the power saving settings might be initialized. This problem is avoided by making sure the same settings are used for normal time ranges and scheduled time ranges.
2. Do not use a directly attached cable for connection to a port that is used to detect a link-up state.
3. If this option is enabled for a port, the port is always released from blocking status when the Switch enters sleep mode even if the port has been set to become blocked or has been blocked programmatically before the Switch enters sleep mode. Consequently, an unintentional link-up state might be detected.

Be careful when any of the following exists for a port for which this option is enabled:

- The **schedule power-control shutdown** configuration command is set.
If both the above command and this option are set for a port, the Switch repeatedly sleeps and wakes during scheduled time ranges.
- A port is blocked as a result of any of the following:
 - Stopping operation by using the **inactive** operation command
 - The standby link functionality of link aggregation

- The BPDU guard functionality of Spanning Tree Protocols
- The storm control functionality
- The SML (split multi-link) functionality [OS-L2A]
- Detection of a unidirectional link failure by the UDLD functionality
- The L2 loop detection functionality

After the Switch mode changes to sleep mode as a result of any of the above, a link-up state will be detected when the port is released from blocking status, and sleep mode will be canceled.

(5) 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 range of the sleep status is longer than the lease time of an IP address distributed by the DHCP server. If the time range 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 updated 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.

12.2 Configuration of the power saving functionality

12.2.1 List of configuration commands

The following table describes the configuration commands for the power saving functionality.

Table 12-12 List of configuration commands

Command name		Description
For setting a normal time range	For setting a scheduled time range	
<code>system port-led</code>	<code>schedul e- power- control port- led</code>	Configures a Switch's LED behavior.
<code>system port-led trigger interface[#]</code>		Adds detection of a link-up or link-down state for the specified physical port as a trigger for automatic LED behavior.
<code>system port-led trigger console[#]</code>		Adds login to and logout from a Switch via a console (RS232C) connection as a trigger for automatic LED behavior.
<code>system port-led trigger mc[#]</code>		Adds insertion and removal of a memory card as a trigger for automatic LED behavior.
<code>power- control port cool- standby</code>	<code>schedul e- power- control port cool- standby</code>	Enables the power saving functionality for link-down ports.
<code>system fan- control[#]</code>		Enables cooling fan control (semi-fanless operation).
<code>shutdown</code>	<code>schedul e- power- control shut down</code>	Sets port blocking.
--	<code>schedul e- power- control system- sleep</code>	Sets sleep mode.
--	<code>schedul e- power- control wakeup- option linkup</code>	Enables a wake-up option for sleep mode. The Switch wakes when it detects a link-up state for a specific port.
--	<code>schedul e- power- control wakeup- option wol</code>	Enables a wake-up option for sleep mode. The Switch wakes when it detects an incoming WOL packet for a specific port.
--	<code>schedul e- power- control ti me- range</code>	Specifies the time range of the power saving schedule.

Legend

--: Not applicable.

#

The setting is common to both normal and scheduled time ranges.

12.2.2 Configuring automatic LED behavior control

(1) Setting automatic LED behavior control

Points to note

Set the Switch's LED brightness level to power saving brightness.

Command examples

1. `(config)# system port-led economy`

Sets the Switch's LED brightness level to power saving brightness.

(2) Setting triggers for performing automatic LED behavior control

LED behavior can be changed automatically by adding triggers for automatic LED behavior control to the LED settings.

Points to note

Set the console, physical ports (link-up and link-down states), and a memory card (insertion or removal) as triggers for automatically controlling LED behavior on the Switch.

Command examples

1. `(config)# system port-led enable`

Sets the Switch's LED brightness level to normal brightness.

2. `(config)# system port-led trigger console`

`(config)# system port-led trigger interface gigabitethernet 0/1,
gigabitethernet 0/20`

`(config)# system port-led trigger mc`

Sets the console, ports 0/1 and 0/20 (link-up and link-down states), and a memory card (insertion or removal) as triggers for automatic LED behavior control.

12.2.3 Configuring the power saving functionality for link-down ports

Points to note

Enable the power saving functionality for link-down ports.

Command examples

1. `(config)# power-control port cool-standby`

Enables the power saving functionality that reduces power when a link-down state is detected for any port.

12.2.4 Configuring the cooling fan control functionality (semi-fanless operation)

Points to note

Set the cooling fan control functionality to monitor the internal temperature in order to stop cooling fans when compulsory cooling is not necessary.

Command examples

1. `(config)# system fan-control`

Sets the cooling fan control functionality to stop cooling fans when compulsory cooling is not necessary.

12.2.5 Configuring scheduled power saving

You can enable power saving by using the sleep functionality or other power saving settings.

- Sleep mode (New Year holidays and other long vacation time ranges)
- Settings for LED behavior control and power saving for link-down ports, which can be used independently of sleep mode
- Setting whereby the Switch is activated only when infinity is specified for sleep mode

(1) Setting sleep mode for the New Year holidays

Points to note

Place the Switch in sleep mode during the New Year holidays.

Command examples

1. `(config)# schedule power-control system-sleep`
Sets what types of power saving functionality will be enabled during scheduled time ranges. In this example, the Switch is set to go into sleep mode.
2. `(config)# schedule power-control time-range 1 date start-time 101228 2300 end-time 110104 0600 action enable`
Sets a power saving schedule that runs from 23:00 on December 28, 2010, to 6:00 on January 4, 2011.
3. `(config)# schedule power-control time-range 2 date start-time 111228 2300 end-time 120104 0600 action enable`
Sets a power saving schedule that runs from 23:00 on December 28, 2011, to 6:00 on January 4, 2012.
4. `(config)# schedule power-control time-range 3 date start-time 121228 2300 end-time 130104 0600 action enable`
Sets a power saving schedule that runs from 23:00 on December 28, 2012, to 6:00 on January 4, 2013.
5. `(config)# end`
Unsaved changes would be lost when the machine goes to sleep!
Do you exit "configure" without save ? (y/n):
Because sleep mode is set as the type of power saving functionality to be used, the above message appears when the configuration mode ends.
6. `Do you exit "configure" without save ? (y/n): n`
`(config)# save`
Enter **n** to save the changes, and then execute the **save** command.

Notes

For details, see *12.1.8(3) Placing a Switch in sleep mode*.

(2) Setting LED behavior and power saving for link-down ports, which are to be in effect during a scheduled time range

Points to note

Turn off LEDs, enable the power saving functionality for link-down ports, and block unused ports.

The following table compares the operating status existing before configuration (normal time ranges) and the operating status existing after configuration (scheduled time ranges).

Table 12-13 Example of configuration settings

Item	Normal time range	Scheduled time range
LED behavior	Normal brightness	OFF
Power saving functionality for link-down ports	All ports operate normally.	Power to link-down ports is reduced.
Port blocking	no shutdown is set for all ports.	shutdown is set for unused ports 0/21 to 0/24.

Command examples

- ```
(config) # schedule-power-control port-led disable
```

```
(config) # schedule-power-control port cool-standby
```

```
(config) # schedule-power-control shutdown interface gigabitethernet 0/21-24
```

Sets what types of power saving functionality will be enabled during scheduled time ranges. The above configuration turns off LEDs, applies the power saving functionality for link-down ports, and blocks unused ports.
- ```
(config) # schedule-power-control time-range 1 weekly start-time fri 2000 end-time mon 0800 action enable
```

Sets a power saving schedule that runs from 20:00 every Friday to 8:00 every Monday.
- ```
(config) # schedule-power-control time-range 2 date start-time 110404 1600 end-time 110404 2000 action disable
```

Disables the power saving schedule for the time range from 16:00 to 20:00 on April 4, 2011.

## Notes

- You can set multiple scheduled time ranges. When a scheduled time range arrives, all the types of power saving functionality set by using the **schedule power-control** configuration commands are executed. You cannot set the types of power saving functionality to be used for each scheduled time range.
- If there is an overlap of time of execution between different **action** parameters, the **action disable** setting has precedence.

**(3) Setting that activates the Switch only when infinity is specified for sleep mode**

## Points to note

Use the sleep functionality with a wake-up option specified for power saving at the Switch.

For the wake-up option, the option that wakes the Switch when a link-up state is detected is set for specified ports.

After the Switch has been used, it can be made to sleep by placing all the specified ports into the link-down state.

## Command examples

- ```
(config) # schedule-power-control system-sleep
```

Sets what types of power saving functionality will be enabled during scheduled time ranges. In this example, sleep mode is set for the Switch.

2. `(config)# schedule-power-control wakeup-option linkup interface gigabitethernet 0/1, gigabitethernet 0/4`
Sets the option that wakes the Switch when a link-up state is detected for ports 0/1 and 0/4.
3. `(config)# schedule-power-control time-range 1 infinity action enable`
Specifies infinity for scheduled time ranges.
4. `(config)# end`
Unsaved changes would be lost when the machine goes to sleep!
Do you exit "configure" without save ? (y/n):
Because sleep mode is set as the type of power saving functionality to be used, the above message appears when the configuration mode ends.
5. Do you exit "configure" without save ? (y/n): n
`(config)# save`
Enter **n** to save the changes, and then execute the **save** command.

Notes

1. For details, see *12.1.8(3) Placing a Switch in sleep mode* and *12.1.8(4) When enabling a wake-up option for sleep mode*.

12.3 Operation of the power saving functionality

12.3.1 List of operation commands

The following table describes the operation commands for the power saving functionality.

Table 12-14 List of operation commands

Command name	Description
<code>show power-control port</code>	Shows the status of port power saving control.
<code>show power-control schedule</code>	Shows the status of the schedule functionality.
<code>set power-control schedule</code>	Changes the mode from which the Switch will wake up (either schedule-enabled or schedule-disabled mode).
<code>show power</code>	Shows the information about the power consumption of the Switch.
<code>clear power</code>	Clears the information about the power consumption of the Switch.

12.3.2 Displaying the LED behavior

You can check the LED behavior settings by using the `show system` operation command and viewing `Brightness mode`. For details, see *11.1.3 Checking the switch status*.

12.3.3 Displaying the status of port power saving control

You can check the status of port power saving control by executing the `show power-control port` operation command.

Figure 12-6 Results of executing show power-control port

```
> show power-control port

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

12.3.4 Displaying the cooling fan control status

The cooling fan control status is indicated under `Fan` in the information displayed by the `show system` operation command. For details, see *11.1.3 Checking the switch status*.

12.3.5 Displaying the schedule status

You can use the `show power-control schedule` operation command to display the current power saving schedule status and the times that the power saving schedule takes effect.

Figure 12-7 Results of executing the show power-control schedule

```
> show power-control schedule 100801

Date 2010/07/09(Fri) 18:08:07 UTC
Current Schedule Status : Disable
Schedule Power Control Date :
  2010/08/01(Sun) 00:00 UTC - 2010/08/02(Mon) 06:00 UTC
  2010/08/03(Tue) 00:00 UTC - 2010/08/03(Tue) 06:00 UTC
  2010/08/04(Wed) 00:00 UTC - 2010/08/04(Wed) 06:00 UTC
  2010/08/05(Thu) 00:00 UTC - 2010/08/05(Thu) 06:00 UTC
  2010/08/06(Fri) 00:00 UTC - 2010/08/06(Fri) 06:00 UTC
  2010/08/06(Fri) 23:00 UTC - 2010/08/16(Mon) 06:00 UTC
  2010/08/17(Tue) 00:00 UTC - 2010/08/17(Tue) 06:00 UTC
  2010/08/18(Wed) 00:00 UTC - 2010/08/18(Wed) 06:00 UTC
  2010/08/19(Thu) 00:00 UTC - 2010/08/19(Thu) 06:00 UTC
  2010/08/20(Fri) 00:00 UTC - 2010/08/20(Fri) 06:00 UTC

>
```

12.3.6 Displaying the information about power consumption

You can use the `show power` operation command to display information about the power consumption of a Switch.

Figure 12-8 Results of executing show power

```
> show power

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

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

>
```

13. Software Management

This chapter describes how to update the software. For further details, see the *Software Update Guide*.

13.1 List of operation commands

13.2 Updating software

13.3 Registering a license

13.1 List of operation commands

The following table describes the operation commands related to software management.

Table 13-1 List of operation commands

Command name	Description
<code>ppupdate</code>	Updates the software to a later version, which was copied from the memory card to the RAMDISK or which was downloaded via FTP, TFTP, or a similar method.
<code>set license</code>	Registers a purchased license to the switch.
<code>show license</code>	Shows authorized licenses.
<code>erase license</code>	Erases the specified license.

13.2 Updating software

Software update means updating an older version of your software to a later version. To perform a software update, copy the update files from a memory card to the RAMDISK on the Switch and then execute the `ppupdate` operation command, or transfer an update file from a remote operation terminal (PC) to the Switch 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 shows an overview of software update.

Figure 13-1 Overview of software update (via a memory card)

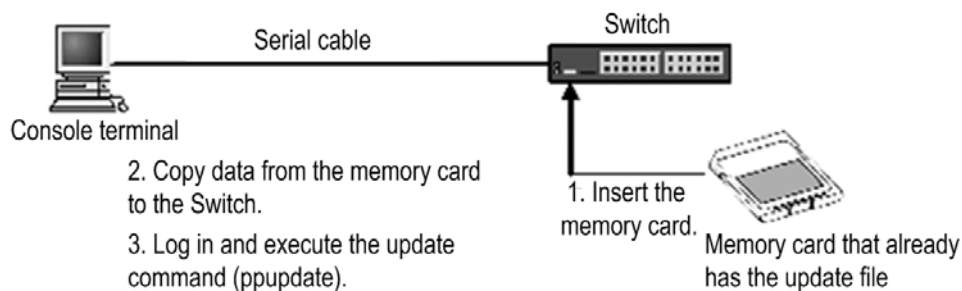
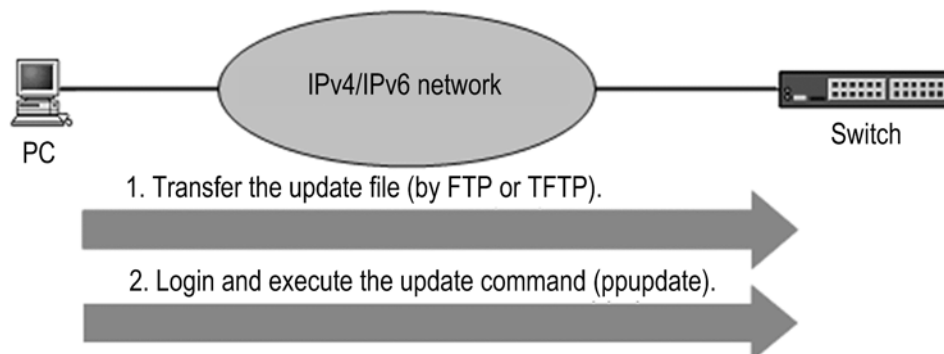


Figure 13-2 Overview of software update (via FTP or TFTP)



13.2.1 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.

13.3 Registering a license

Licenses are required to use additional functionality incorporated in the Switch. If a license is not registered, you cannot use the additional functionality. For details about registering and erasing licensed software, see the *License Installation Guide*.

14. Ethernet

This chapter describes Ethernet as used with this Switch.

14.1	Description of information common to all Ethernet interfaces
14.2	Configuration common to all Ethernet interfaces
14.3	Operations common to all Ethernet interfaces
14.4	Description of the 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces
14.5	Configuration of 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces
14.6	Description of the 100BASE-FX interface [24S4X] [24S4XD]
14.7	Configuration of the 100BASE-FX interface [24S4X] [24S4XD]
14.8	Description of the 1000BASE-X interface
14.9	Configuration of the 1000BASE-X interface
14.10	Description of the 10GBASE-R interface [10G model]
14.11	Configuration of the 10GBASE-R interface [10G model]
14.12	Description of shared SFP/SFP+ ports [10G model]
14.13	Configuration of shared SFP/SFP+ ports [10G model]

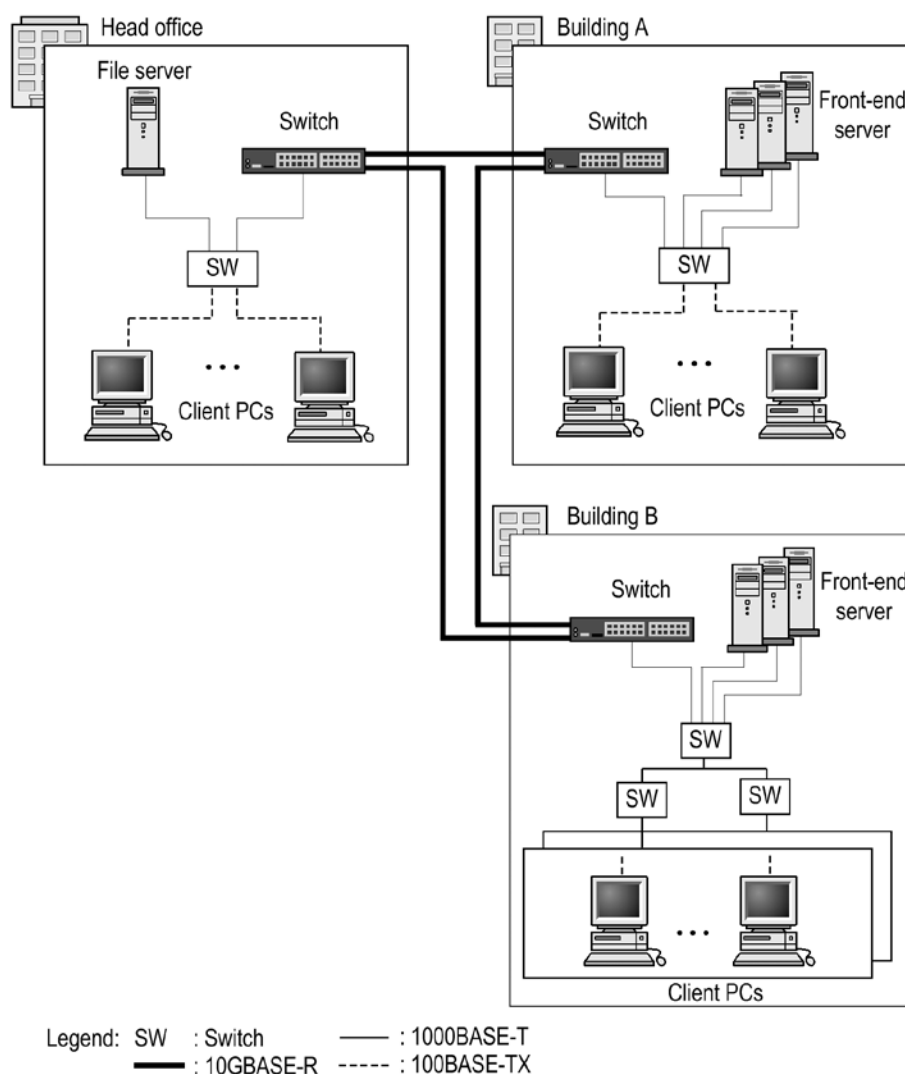
14.1 Description of information common to all Ethernet interfaces

14.1.1 Network configuration example

Typically, Switches can be used as Layer 2 floor switches and Layer 2 distribution switches for enterprise local area networks. 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.

The figure below shows an example of an Ethernet configuration that uses Switches.

Figure 14-1 Ethernet configuration example



14.1.2 Physical interfaces

There are three 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

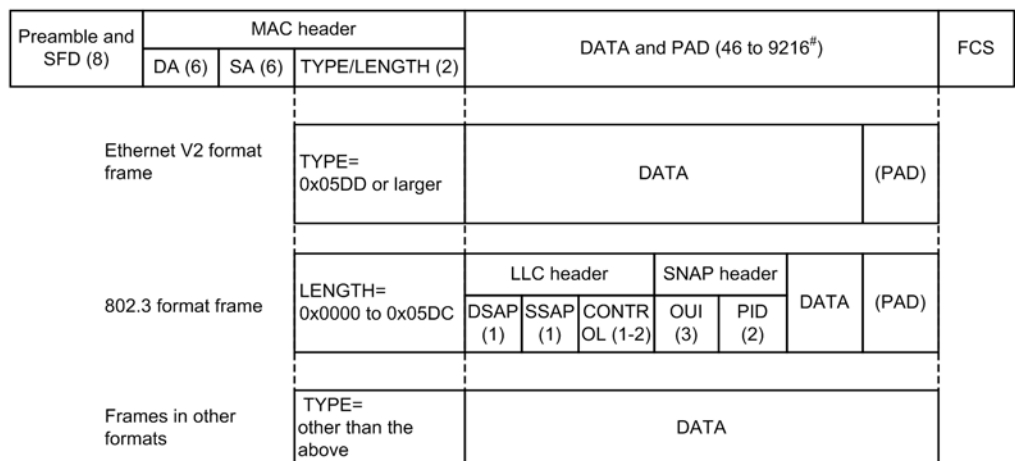
#

Includes IEEE 802.3ah.

14.1.3 Control on the MAC and LLC sublayers

The following figure shows frame formats.

Figure 14-2 Frame formats



(n): Field length (units: octets)

#: 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 (Start Frame Delimiter) field contains a 64-bit binary number. The first 62 bits are repetitions of **10**, and the last two bits are **11** (**1010...1011**). This field is added to the beginning of the frame when the frame is sent. 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 a 16-bit format or local addresses.

(c) TYPE/LENGTH field

The following table describes how the TYPE/LENGTH field is handled.

Table 14-1 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 (UI frame only). 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) 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.

(4) Handling of padding

If the length of a sent frame is less than 64 octets, padding is added immediately before the FCS field in the MAC sublayer. The values to be padded are undefined.

14.1.4 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 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 14-2 Functionality that uses a device MAC address

Functionality	Purpose
VLAN	MAC address for VLAN interfaces
LACP for link aggregation	Device identifier

Functionality	Purpose
Spanning Tree Protocols	Device identifier
Ring Protocol	Device identifier
LLDP	Device identifier
IEEE 802.3ah/UDLD	Device identifier
Unlink redundancy (flush control frame transmission)	Device identifier
L2 loop detection	Device identifier
CFM	Device identifier

14.1.5 Order of Ethernet frames

A Switch uses software to forward some frames. Therefore, the order of forwarded frames might change. The order of frames might also change when priority control based on CoS values[#] is operating.

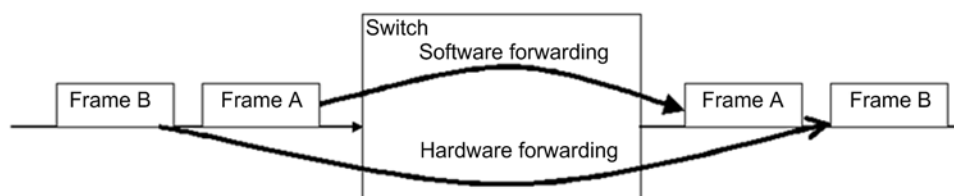
#

CoS values are an index for showing the priority of the frames on a Switch.

(1) Changes in the order of forwarded frames due to software forwarding

The frames a Switch uses software to forward are some types of IGMP or MLD snooping frames (such as query).

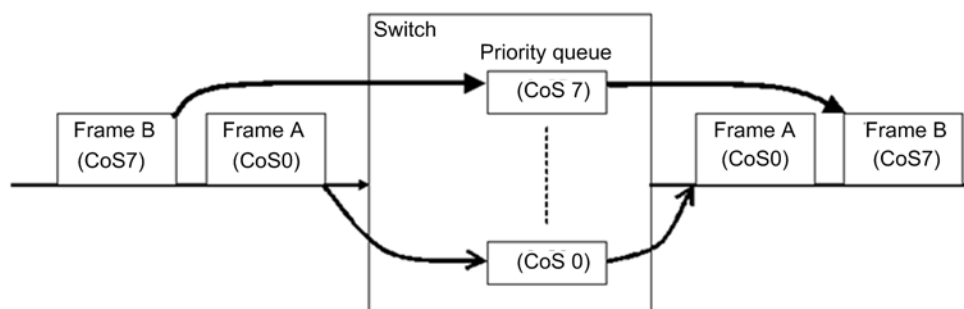
Figure 14-3 How the frame order changes due to software forwarding



(2) Changes in the frame order due to priority control

Priority control based on CoS values is enabled on a Switch by default. Therefore, the frame order might change when frames that have different CoS values are received.

Figure 14-4 Changes in the frame order due to priority control



14.2 Configuration common to all Ethernet interfaces

14.2.1 List of configuration commands

The following table describes the configuration commands common to all Ethernet interfaces.

Table 14-3 List of configuration commands

Command name	Description
<code>bandwidth</code>	Sets the bandwidth of a port.
<code>description</code>	Sets supplementary information for a port.
<code>duplex</code> (gigabitethernet)	Sets duplex mode for a port with an Ethernet interface whose maximum line speed is 1000 Mbit/s.
<code>duplex</code> (tengigabitethernet) [10G model]	Sets duplex mode for a shared SFP/SFP+ port that uses 1000BASE-X.
<code>flowcontrol</code>	Sets flow control for a port.
<code>interface gigabitethernet</code>	Sets an Ethernet interface configuration with a maximum line speed of 1000 Mbit/s.
<code>interface tengigabitethernet</code> [10G model]	Sets an Ethernet interface configuration with a maximum line speed of 10 Gbit/s.
<code>link debounce</code>	Sets the time required before a link-down is detected.
<code>link up-debounce</code>	Sets the time required before a link-up is detected.
<code>mdi x auto</code>	Sets the automatic MDIX functionality for a port.
<code>mtu</code>	Sets the MTU for a port.
<code>shutdown</code>	Shuts down the port.
<code>speed</code> (gigabitethernet)	Sets the transmission speed for a port with an Ethernet interface whose maximum line speed is 1000 Mbit/s.
<code>speed</code> (tengigabitethernet) [10G model]	Sets the transmission speed for a shared SFP/SFP+ port that uses 1000BASE-X.
<code>system mtu</code>	Sets an MTU that is common to all ports.

14.2.2 Configuring a port that has an Ethernet interface

Points to note

To configure Ethernet, specify the port number of the interface, and then move to `config-if` mode to set up the information.

Command examples

1. `(config)# interface gigabitethernet 0/1`

Specifies that settings are for port 0/1, which uses a 1-gigabit Ethernet interface.

14.2.3 Configuring multiple ports at one time

Points to note

When Ethernet is configured, the same information sometimes needs to be set for multiple ports. In such cases, the same information can be set for the ports at the same time by using a range specification.

Command examples

1. `(config)# interface range gigabitethernet 0/1-10, gigabitethernet 0/15-20, ten-gigabitethernet 0/25`

Specifies the ports to be configured. The ports specified in this example are ports 0/1 to 0/10 and 0/15 to 0/20, which use the 1-gigabit Ethernet interface, and port 0/25, which uses the 10G-bit Ethernet interface.

2. `(config-if-range)# *****`
`(config-if-range)# exit`

Performs the same configuration for all the ports.

14.2.4 Shutting down an Ethernet interface

Points to note

Configuring an Ethernet interface might require the execution of multiple commands. If a port 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 all ports, and then release the ports from the shutdown status after configuration has been completed. Always make sure that ports that will not be used are shut down.

Command examples

1. `(config)# interface gigabitethernet 0/10`

Specifies that port 0/10 is to be configured.

2. `(config-if)# shutdown`

Shuts down the port.

3. `(config-if)# *****`

Configures all ports.

4. `(config-if)# no shutdown`
`(config-if)# exit`

Releases the ports from the shutdown status

Additional information

You can also use the `inactivate` operation command to stop the operation of a port. Note that if a switch deactivated by using this command restarts, the status of the

port 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 port from the shutdown status by using the **no shutdown** configuration command to configure the interface. (After specifying the configuration settings, execute the **save** command to save the settings.)

14.2.5 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, a Switch can send or receive frames whose maximum size is the specified MTU plus the size of one VLAN tag.

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 port

Points to note

Set 8192 octets as the MTU for port 0/10. This setting enables the sending and receiving jumbo frames (8206 octets for frames without a VLAN tag and 8210 octets for frames with VLAN tags).

Command examples

1.

```
(config)# interface gigabitEthernet 0/10
(config-if)# shutdown
(config-if)# mtu 8192
```

Sets the MTU of the port 0/10 to 8192 octets.
2.

```
(config-if)# no shutdown
(config-if)# exit
```

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 or 100BASE-TX half-duplex connection is used. This note also applies when auto-negotiation results in a 10BASE-T or 100BASE-TX half-duplex connection.

(2) Setting the MTU for all ports

Points to note

Set 4096 octets as the MTU for all ports on the Switch. This configuration enables the sending and receiving of jumbo frames (4110 octets for frames without a VLAN tag and 4114 octets for frames with VLAN tags).

Command examples

1.

```
(config)# system mtu 4096
```

Sets the MTU of all ports on the 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 or 100BASE-TX half-duplex connection is used. This note also applies when auto-negotiation results in a 10BASE-T or

100BASE-TX half-duplex connection.

14.2.6 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 time is not set, you do not need to set one.

Command examples

1. `(config)# interface gigabitethernet 0/10`

Specifies that port 0/10 is to be configured.

2. `(config-if)# link debounce time 5000`

`(config-if)# exit`

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.

14.2.7 Configuring the link-up detection timer

If the wait time before a link-up is detected after the detection of a link failure 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 0/10`

Specifies that the port 0/10 is to be configured.

2. `(config-if)# link up-debounce time 5000`

`(config-if)# exit`

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.

14.3 Operations common to all Ethernet interfaces

14.3.1 List of operation commands

The following table describes the operation commands common to all Ethernet interfaces.

Table 14-4 List of operation commands

Command name	Description
<code>show interfaces</code>	Shows Ethernet information.
<code>show port</code>	Shows Ethernet information in list format.
<code>clear counters</code>	Clears the Ethernet statistics counters.
<code>inactivate</code>	Changes the status of an Ethernet port from active to inactive.
<code>activate</code>	Changes the status of an Ethernet port from inactive to active.
<code>test interfaces</code>	Conducts a line test.
<code>no test interfaces</code>	Stops a line test, and displays the test results.

14.3.2 Checking the Ethernet operating status

(1) Checking the operating status of all Ethernet ports

You can use the `show port` operation 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` operation command.

Figure 14-5 Example of displaying the status of all Ethernet ports on the Switch

```
> show port
```

```
Date 2010/12/19 15:21:43 UTC
```

```
Port Counts: 28
```

Port	Name	Status	Speed	Duplex	FCtl	FrLen	ChGr/Status
0/1	geth0/1	up	1000BASE-T	full (auto)	off	9234	-/-
0/2	geth0/2	up	1000BASE-T	full (auto)	off	9234	-/-
0/3	geth0/3	up	1000BASE-T	full (auto)	off	9234	-/-
0/4	geth0/4	up	1000BASE-T	full (auto)	off	9234	-/-
0/5	geth0/5	down	-	-	-	-	-/-
0/6	geth0/6	down	-	-	-	-	-/-
0/7	geth0/7	down	-	-	-	-	-/-

```
:
```

```
:
```

```
:
```

```
>
```

14.4 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).

14.4.1 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 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.

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.

Table 14-5 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
		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
Auto-negotiation	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

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	
	10/100BASE-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
	10/100/1000BASE-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 14-5 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. (For details about this action, see *14.4.1(6) Down-shift functionality*.)

(3) 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. For the flow control configuration, you can select the enabled mode, the disabled mode, or the mode determined depending on the auto-negotiation result and then can set the mode separately

for sending and receiving settings. 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 receive setting 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 14-6 Flow control for sending on the switch*, *Table 14-7 Flow control for receiving on the switch*, and *Table 14-8 Flow control operation determined by the auto-negotiation result*.

Table 14-6 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.
desi red	desi red	Sending on the remote device is regulated.

Legend

on: Enabled.

off: Disabled. If either **on** or **off** is set when **desi red** is set on the remote device, the flow control operation mode is determined by the negotiation result. For details about flow control, see *Table 14-8 Flow control operation determined by the auto-negotiation result*.

desi red: Enabled. If auto-negotiation is selected, the flow control operation mode is determined from the negotiation result. For details about flow control, see *Table 14-8 Flow control operation determined by the auto-negotiation result*.

Table 14-7 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.
desi red	desi red	Sending on the Switch is regulated.

Legend

on: Enabled.

off: Disabled. If either **on** or **off** is set when **desi red** is set on the remote device, the flow control operation mode is determined by the negotiation result. For details about flow control, see *Table 14-8 Flow control operation determined by the auto-negotiation result*.

desi red: Enabled. If auto-negotiation is selected, the flow control operation mode is determined from the negotiation result. For details about flow control, see *Table 14-8 Flow control operation determined by the auto-negotiation result*.

Table 14-8 Flow control operation determined by the auto-negotiation result

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
desired	on	Enabled	Enabled	on	on	Yes	Yes
			Disabled	off	on	Yes	No
			desired	on	on	Yes	Yes

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	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

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
			desi red	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. 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 14-9 MDI and MDI-X pin mappings

RJ45 Pin No.	MDI			MDI-X		
	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.

For details about frame formats, see *14.1.3 Control on the MAC and LLC sublayers*. For details about tagged frame formats, see *18.1.5 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 14-10 Jumbo frame support status

Item	Frame format		Description
	EthernetV2 [#]	IEEE 802.3 [#]	
Frame length (octets)	Untagged: 1519 to 9234 Tagged: 1523 to 9238	N	Total field size of DA (in the MAC header) to DATA (FCS included).
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 *14.1.3 Control on the MAC and LLC sublayers*.

(6) Down-shift functionality

The down-shift functionality is enabled when auto-negotiation is enabled. If an attempt to establish a link by auto-negotiation fails, this functionality disables the highest speed for auto-negotiation advertisement, and attempts to establish a link at the next highest speed. (There is no operation that disables the down-shift functionality.)

(a) Applicable lines

This functionality is supported by 1000BASE-T.

(b) Line speed switchover

If a link is not established after auto-negotiation has been completed, the line speed for auto-negotiation advertisement switches from phase 1 down. If a link is not established even with the lowest line speed, the line speed returns to phase 1, and the down-shift operation is continued.

Table 14-11 Line speed switchover

No.	Down-shift functionality	Phase	Configuration definition (speed parameter setting) ^{#1}				Remarks
			auto	auto 10 100 1000	auto 10 100	auto 1000 or auto 100 or auto 10	
1	On	1	10 100 1000	10 100 1000	10 100	--	
2		2	10 100	10 100	10	--	
3		3	10	10	--	--	

--: No down-shift operation is performed. Ordinary auto-negotiation operation is performed.

#1: The numeric values are line speeds.

(7) Notes on a 10BASE-T, 100BASE-TX, or 1000BASE-T connection

- If the transmission speed and the duplex mode (full or half) settings on the Switch and a remote device are different, the Switch and the remote device will be unable to connect.
If these settings on the devices are different, communication might stop. If communication stops, execute the **inactivate** operation command, and then execute the **activate** operation 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 10BASE-T or 100BASE-TX for a full-duplex interface, always make sure that you set the connecting interface of the remote device to full-duplex.
- If 1000BASE-T is used, only full-duplex auto-negotiation mode is supported.

14.4.2 SFP for 10BASE-T/100BASE-TX/1000BASE-T

For the Switch, you can establish a 10BASE-T, 100BASE-TX, or 1000BASE-T connection with an SFP port or a shared SFP/SFP+ port by using a special SFP.

For the communication functionality available with 10BASE-T, 100BASE-TX, or 1000BASE-T ports, SFP ports, and shared SFP/SFP+ ports, there are no differences other than whether the interface type is fixed to the type indicated in the following table.

Table 14-12 Ports on which SFP for 10BASE-T, 100BASE-TX, or 1000BASE-T can be used

Model	Available port number	Interface type	Remarks
AX2530S-24T AX2530S-24TD	0/25 to 0/28	1000BASE-T fixed	SFP port
AX2530S-24T4X	0/25 to 0/28	1000BASE-T fixed	Shared SFP/SFP+ port

14 Ethernet

Model	Available port number	Interface type	Remarks
AX2530S-48T AX2530S-48TD	0/49 to 0/52	1000BASE-T fixed	SFP port
AX2530S-48T2X	0/49 to 0/50	1000BASE-T fixed	SFP port
	0/51 to 0/52	1000BASE-T fixed	Shared SFP/SFP+ port
AX2530S-24S4 AX2530S-24S4XD	0/1 to 0/24	10BASE-T/100BASE-TX/1000BASE-T	SFP port
	0/25 to 0/28	1000BASE-T fixed	Shared SFP/SFP+ port

14.5 Configuration of 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces

14.5.1 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.

(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 0/10
(config-if)# shutdown
(config-if)# speed 100
(config-if)# duplex half
```

Configures the switch so that the connection with the remote device is a 100BASE-TX, half-duplex connection.

2.

```
(config-if)# no shutdown
(config-if)# exit
```

(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 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
(config-if)# exit
```

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.

14.5.2 Configuring flow control

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.

Points to note

Make sure that you determine flow control settings that do not conflict with the settings on the remote device.

Command examples

1. `(config)# interface gigabitethernet 0/10`

`(config-if)# shutdown`

`(config-if)# flowcontrol send off`

`(config-if)# flowcontrol receive off`

Stops the passing of pause packets between the Switch and the remote device.

2. `(config-if)# no shutdown`

`(config-if)# exit`

14.5.3 Configuring the automatic MDIX functionality

The 10BASE-T, 100BASE-TX, or 1000BASE-T port on a Switch support 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.

(1) Fixing the MDI mode

Points to note

Specify the settings that fix the MDI mode to MDI-X for a specific port.

Command examples

1. `(config)# interface gigabitethernet 0/10`

Specifies port 0/10 as the port to be configured.

2. `(config-if)# no mdix auto`

`(config-if)# exit`

Disables the automatic MDIX functionality so that MDI-X is always selected.

14.6 Description of the 100BASE-FX interface [24S4X] [24S4XD]

14.6.1 Functionality

This section describes an Ethernet interface that uses a 100BASE-FX optical fiber cable.

(1) Connection interface

(a) 100BASE-FX

100BASE-FX is supported. A transmission speed of 100 Mbit/s and the duplex mode (full) 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)

When specifying configuration settings, specify the following mode:

- Transmission speed: fixed to 100 Mbit/s, duplex mode: fixed to full duplex

(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 14-13 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 full duplex
Fixed settings	100BASE half duplex	N
	100BASE full duplex	100BASE full duplex
Auto-negotiation	100BASE half duplex	N
	100BASE full duplex	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. For the flow control configuration, you can select the enabled mode or the disabled mode and then can set the mode separately for sending and receiving settings. 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 receive setting 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 14-14 Flow control for sending on the switch* and *Table 14-15 Flow control for receiving on the switch*.

For 100BASE-FX, no specific operation is performed when auto-negotiation is set because auto-negotiation is not supported.

Table 14-14 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.
desi red	desi red	Sending on the remote device is regulated.

Legend

on: Enabled; **off**: Disabled; **desi red**: Enabled

Table 14-15 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.
desi red	desi red	Sending on the Switch is regulated.

Legend

on: Enabled; **off**: Disabled; **desi red**: 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.

For details about frame formats, see *14.1.3 Control on the MAC and LLC sublayers*. For details about tagged frame formats, see *18.1.5 VLAN tags*. The following table describes the jumbo frame support status.

Table 14-16 Jumbo frame support status

Item	Frame format		Description
	Ethernet V2 [#]	IEEE 802.3 [#]	
Frame length (octets)	Untagged: 1519 to 9234 Tagged: 1523 to 9238	N	Total field size of DA (in the MAC header) to DATA (FCS included).
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 *14.1.3 Control on the MAC and LLC sublayers*.

(4) Notes on a 100BASE-FX connection

- Make sure you use the following settings for 100BASE-FX ports:
 - Transmission speed: fixed to 100 Mbit/s, duplex mode: fixed to full duplex
- If a transceiver not indicated in the *Hardware Instruction Manual* is used, correct operation is not guaranteed.

14.6.2 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 switches support SFPs for 100BASE-FX connections:

- AX2530S-24S4X and AX2530S-24S4XD

The SFP for a 100BASE-FX connection can be established with SFP slot ports 0/1 to 0/24.

14.7 Configuration of the 100BASE-FX interface [24S4X] [24S4XD]

14.7.1 Configuring ports

(1) Setting the transmission speed and duplex mode

For ports that use 100BASE-FX, make sure you set a transmission speed and full-duplex mode (fixed).

Points to note

In the following example, the transmission speed is set at 100 Mbit/s, and full-duplex mode (fixed) is set. Make sure you specify these settings also on a remote device.

Command examples

1. `(config)# interface gigabitethernet 0/24`
`(config-if)# shutdown`
`(config-if)# speed 100`
`(config-if)# duplex full`

Configures the switch so that it connects to the remote device at a transmission speed of 100 Mbit/s in full-duplex mode.

2. `(config-if)# no shutdown`
`(config-if)# exit`

Notes

Make sure you use the above settings when using 100BASE-FX.

14.7.2 Configuring flow control

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.

Points to note

Make sure that you determine flow control settings that do not conflict with the settings on the remote device.

Command examples

1. `(config)# interface gigabitethernet 0/24`
`(config-if)# shutdown`
`(config-if)# flowcontrol send off`
`(config-if)# flowcontrol receive off`
 Stops the passing of pause packets between the Switch and the remote device.
2. `(config-if)# no shutdown`
`(config-if)# exit`

Notes

Because auto-negotiation does not function when 100BASE-FX is used, flow control by auto-negotiation is not performed.

14.8 Description of the 1000BASE-X interface

14.8.1 Functionality

This section describes an Ethernet interface that uses a 1000BASE-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. A transmission speed of 1000 Mbit/s and the duplex mode (full) are configured as fixed settings.

1000BASE-SX:

Used for short-distance connections.

(550 m max. in multi-mode)

1000BASE-SX2:

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, 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 14-17 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 14-17 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

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. For the flow control configuration, you can select the enabled mode, the disabled mode, or the mode determined depending on the auto-negotiation result and then can set the mode separately for sending and receiving settings. 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 receive setting 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 14-18 Flow control for sending on the switch*, *Table 14-19 Flow control for receiving on the switch*, and *Table 14-20 Flow control operation determined by the auto-negotiation result*.

Table 14-18 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.
desi red	desi red	Sending on the remote device is regulated.

Legend

on: Enabled.

off: Disabled. If either **on** or **off** is set when **desi red** is set on the remote device, the flow control operation mode is determined by the negotiation result. For details about flow control, see *Table 14-20 Flow control operation determined by the auto-negotiation result*.

desi red: Enabled. If auto-negotiation is selected, the flow control operation mode is determined from the negotiation result. For details about flow control, see *Table 14-20 Flow control operation determined by the auto-negotiation result*.

Table 14-19 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.
desi red	desi red	Sending on the Switch is regulated.

Legend

on: Enabled.

off: Disabled. If either **on** or **off** is set when **desi red** is set on the remote device, the flow control operation mode is determined by the negotiation result. For details about flow control, see *Table 14-20 Flow control operation determined by the auto-negotiation result*.

desi red: Enabled. If auto-negotiation is selected, the flow control operation mode is determined from the negotiation result. For details about flow control, see *Table 14-20 Flow control operation determined by the auto-negotiation result*.

Table 14-20 Flow control operation determined by the auto-negotiation result

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
		Enabled	Enabled	on	on	Yes	Yes
			Disabled	off	on	Yes	No
			desired	on	on	Yes	Yes
off	desired	Enabled	Enabled	on	on	No	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	Yes	Yes
			Disabled	off	on	Yes	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	off	on	Yes	No
			desired	on	on	Yes	Yes
		Enabled	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

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	Enabled	on	on	No	Yes
			Disabled	off	on	No	No
			desi red	on	on	Yes	Yes
		desi red	Enabled	on	on	Yes	Yes
			Disabled	off	on	No	No
			desi red	on	on	Yes	Yes
	off	Enabled	Enabled	off	off	No	No
			Disabled	off	off	No	No
			desi red	off	off	No	No
		Disabled	Enabled	on	off	No	Yes
			Disabled	off	off	No	No
			desi red	on	off	No	Yes
		desi red	Enabled	off	off	No	No
			Disabled	off	off	No	No
			desi red	off	off	No	No
	desi red	Enabled	Enabled	on	on	Yes	Yes
			Disabled	off	off	No	No
			desi red	on	on	Yes	Yes
		Disabled	Enabled	on	on	No	Yes
			Disabled	off	off	No	No
			desi red	on	on	Yes	Yes
		desi red	Enabled	on	on	Yes	Yes

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	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.

For details about frame formats, see *14.1.3 Control on the MAC and LLC sublayers*. For details about tagged frame formats, see *18.1.5 VLAN tags*. The following table describes the jumbo frame support status.

Table 14-21 Jumbo frame support status

Item	Frame format		Description
	Ethernet V2 [#]	IEEE 802.3 [#]	
Frame length (octets)	Untagged: 1519 to 9234 Tagged: 1523 to 9238	N	Total field size of DA (in the MAC header) to DATA (FCS included).
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 *14.1.3 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.

14.9 Configuration of the 1000BASE-X interface

14.9.1 Configuring ports

(1) Setting the transmission speed and duplex mode

You can set the transmission speed and duplex mode used for communication between a Switch and a remote device. By default, the transmission speed and duplex mode are determined automatically by auto-negotiation between the Switch and the partner device.

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 0/25`
`(config-if)# shutdown`
`(config-if)# speed 1000`
`(config-if)# duplex full`

Configures the 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`
`(config-if)# exit`

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.

14.9.2 Configuring flow control

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.

Points to note

Make sure that you determine flow control settings that do not conflict with the settings on the remote device.

Command examples

1. `(config)# interface gigabitethernet 0/25`
`(config-if)# shutdown`
`(config-if)# flowcontrol send off`
`(config-if)# flowcontrol receive off`
 Stops the passing of pause packets between the Switch and the remote device.
2. `(config-if)# no shutdown`
`(config-if)# exit`

14.10 Description of the 10GBASE-R interface [10G model]

14.10.1 Functionality

This section describes an Ethernet interface that uses 10GBASE-R.

(1) Connection interface

(a) 10GBASE-R

The 10GBASE-SR, 10GBASE-LR, and 10GBASE-ER interfaces, and direct attach cables are supported. A transmission speed of 10 Gbit/s and the duplex mode (full) are configured as fixed settings.

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)

Direct attach cables:

Used for connecting devices.

(Transmission distance: 30 cm, 1 m, 3 m, or 5 m)

(b) 10GBASE-R connection specifications

For details about the physical specifications for the 10GBASE-R interface, see the *Hardware Instruction Manual*.

(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. For the flow control configuration, you can select the enabled mode or the disabled mode and then can set the mode separately for sending and receiving settings. 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 receive setting 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 14-22 Flow control for sending on the switch* and *Table 14-23 Flow control for receiving on the switch*.

For 10GBASE-R, no flow control operation is performed when auto-negotiation is set

because auto-negotiation is not supported.

Table 14-22 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.
desi red	desi red	Sending on the remote device is regulated.

Legend

on: Enabled; **off**: Disabled; **desi red**: Enabled

Table 14-23 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.
desi red	desi red	Sending on the Switch is regulated.

Legend

on: Enabled; **off**: Disabled; **desi red**: 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.

For details about frame formats, see *14.1.3 Control on the MAC and LLC sublayers*. For details about tagged frame formats, see in *18.1.5 VLAN tags*. The following table describes the jumbo frame support status.

Table 14-24 Jumbo frame support status

Item	Frame format		Description
	Ethernet V2 [#]	IEEE 802.3 [#]	
Frame length (octets)	Untagged: 1519 to 9234 Tagged: 1523 to 9238	N	Total field size of DA (in the MAC header) to DATA (FCS included).
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 *14.1.3 Control on the MAC and LLC sublayers*.

(4) Notes on 10GBASE-R connection

1. 10GBASE-R does not support half-duplex mode and auto-negotiation. The duplex mode is fixed to full-duplex.
2. If a transceiver not indicated in the *Hardware Instruction Manual* is used, correct operation is not guaranteed.

14.11 Configuration of the 10GBASE-R interface [10G model]

14.11.1 Configuring flow control

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.

Points to note

Make sure that you determine flow control settings that do not conflict with the settings on the remote device.

Command examples

1. `(config)# interface tengigabitethernet 0/25`

`(config-if)# shutdown`

`(config-if)# flowcontrol send off`

`(config-if)# flowcontrol receive off`

Stops the passing of pause packets between the Switch and the remote device.

2. `(config-if)# no shutdown`

`(config-if)# exit`

14.12 Description of shared SFP/SFP+ ports [10G model]

14.12.1 Functionality

This section describes a shared SFP/SFP+ port

(1) Connection interface

Shared SFP/SFP+ ports support SFP+ transceivers for 10GBASE-R, SFP transceivers for 1000BASE-X, and SFP transceivers for 10BASE-T, 100BASE-TX, and 1000BASE-T. Direct attach cables are supported to connect between shared 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 *14.10 Description of the 10GBASE-R interface [10G model]*.

(b) 1000BASE-X/1000BASE-T

- 1000BASE-X

The SFP modules for 1000BASE-SX, 1000BASE-LX, 1000BASE-LH, 1000BASE-LHB, and 1000BASE-BX interfaces are supported. For details on the interfaces, see *14.8 Description of the 1000BASE-X interface*.

- 1000BASE-T

The SFP modules for 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces can be used only for interfaces whose type is 1000BASE-T interface fixed. For details on the interfaces, see *14.4 Description of the 10BASE-T, 100BASE-TX, and 1000BASE-T interfaces*.

(c) Direct attach cables

Direct attach cables feature SFP+ connectors at both ends and are used to connect between shared SFP/SFP+ ports. They function in the same way as 10GBASE-R. For details on the 10GBASE-R interface, see *14.10 Description of the 10GBASE-R interface [10G model]*.

It takes a few seconds to place ports in the link-up status when using a direct connection cable.

14.13 Configuration of shared SFP/SFP+ ports [10G model]

14.13.1 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.

Points to note

The settings are the same as other interfaces, and the interface name in the configuration will also be `tengi gabi tethernet` 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 tengi gabi tethernet 0/28`
`(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`
`(config-if)# exit`

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.

14.13.2 Configuring flow control

For details about the flow control settings, see *14.9.2 Configuring flow control* or *14.11.1 Configuring flow control*.

15. Link Aggregation

This chapter describes link aggregation and its use.

15.1	Description of the basic link aggregation functionality
15.2	Configuration of the basic link aggregation functionality
15.3	Description of the link aggregation extended functionality
15.4	Configuration of the link aggregation extended functionality
15.5	Operation for link aggregation

15.1 Description of the basic link aggregation functionality

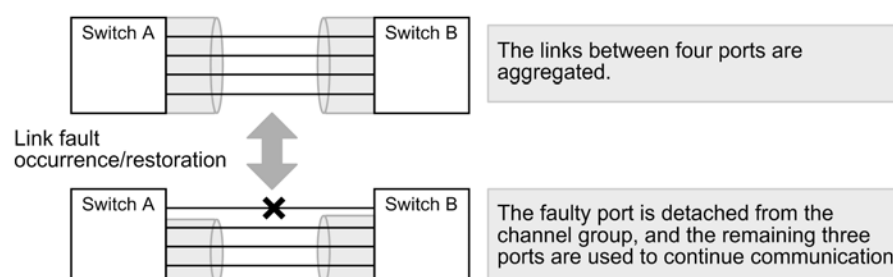
15.1.1 Overview

Link aggregation is functionality that connects devices by establishing multiple links between the Ethernet ports of each neighboring 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.

15.1.2 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 15-1 Example of a link aggregation configuration



15.1.3 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 neighboring 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 15-1 Supported specifications for link aggregation

Item	Supported specifications	Remarks
Number of channel groups per switch	64	--
Maximum number of ports per group	8	--
Link aggregation modes	<ul style="list-style-type: none"> ● LACP ● Static 	--

Item	Supported specifications	Remarks
Transmission speed between ports	Different transmission speeds cannot be used.	Slower lines [#] are detached from the group.
Duplex mode	Only full-duplex mode is supported.	--

Legend

--: Not applicable

#

Lines that are slower than the highest transmission speeds of ports that are in the link-up state at that time.

15.1.4 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 group is changed.

15.1.5 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 15-2 Port allocation for sending frames

Forward	Frame type	Information used for port allocation
Layer 2 forwarding	Frame for which MAC address has not been learned yet (broadcast and multicast frames)	Destination MAC address Source MAC address Reception port number or reception channel group number
	IP frame for which the MAC address has been learned	Destination IP address Source IP address Destination TCP/UDP port number Source TCP/UDP port number
	Non-IP frame for which the MAC address has been learned	Destination MAC address Source MAC address Reception VLAN EtherType

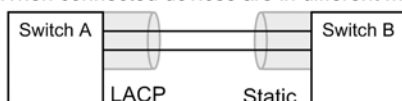
15.1.6 Notes on using link aggregation

(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.

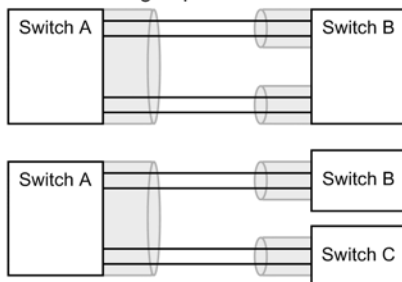
Figure 15-2 Examples of configurations in which link aggregation is not possible

- 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 above. Next, return the ports to the link-up state.

(3) If CPU load is excessive

If CPU load is excessive when LACP link aggregation mode is used, the LACPDU (link aggregation control protocol data units) that the Switch sends or receives might be discarded, or the sending or reception might be delayed. Then, a temporary communication stoppage might occur. If a temporary communication stoppage frequently occurs, the CPU might become overloaded. In such cases, increase the LACPDU sending interval or use static link aggregation.

15.2 Configuration of the basic link aggregation functionality

15.2.1 List of configuration commands

The following table describes the configuration commands for the basic link aggregation functionality.

Table 15-3 List of configuration commands

Command name	Description
<code>channel-group lacp system-priority</code>	Sets the LACP system priority for each channel group.
<code>channel-group mode</code>	Adds a port to a channel group and sets a link aggregation mode.
<code>channel-group periodic-timer</code>	Sets the LACPDU sending interval.
<code>description</code>	Sets supplementary information about a channel group.
<code>interface port-channel</code>	Sets an item related to a port channel interface.
<code>lacp port-priority</code>	Sets the LACP port priority.
<code>lacp system-priority</code>	Sets the LACP system priority for the channel groups for which the <code>channel-group lacp system-priority</code> command is not set.
<code>shutdown</code>	Shuts down a port in a channel group to stop communication.

15.2.2 Configuring static link aggregation

Points to note

For static link aggregation, use the `channel-group mode` configuration 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` configuration command.

Command examples

1. `(config)# interface range gigabitethernet 0/1-2`
Places the Switch in Ethernet interface configuration mode for configuring ports 0/1 and 0/2.
2. `(config-if-range)# channel-group 3 mode on`
`(config-if-range)# exit`
Adds ports 0/1 and 0/2 to channel group 3 in static mode.

15.2.3 Configuring LACP link aggregation

(1) Setting the channel group

Points to note

For LACP link aggregation, use the `channel-group mode` configuration 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 0/1-2`
Places the Switch in Ethernet interface configuration mode for configuring ports 0/1 and 0/2.
2. `(config-if-range)# channel-group 3 mode active`
`(config-if-range)# exit`
Adds ports 0/1 and 0/2 to channel group 3 in LACP mode. If `active` mode is specified, the LACP starts sending LACPDU s in active mode, independently of the remote device. If `passive` mode is specified, the LACP starts sending LACPDU s only when LACPDU s are received from the remote device.

(2) Setting the system priority

Set the LACP system priority. 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 3`
`(config-if)# channel-group lacp system-priority 50`
`(config-if)# exit`
Sets the LACP system priority level of channel group 3 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 0/1`
`(config-if)# lacp port-priority 100`
`(config-if)# exit`

Sets the LACP port priority level of port 0/1 to 100.

(4) Setting the LACPDU sending interval

Points to note

Set the interval at which the remote device sends LACPDU to the Switch. The Switch receives LACPDU 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 3
(config-if)# channel-group periodic-timer short
(config-if)# exit
```

Sets the LACPDU sending interval of channel group 3 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.

15.2.4 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** configuration 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 be match.
- If the **channel-group mode** configuration 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** configuration command is specified.
- If the **channel-group mode** configuration 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** configuration command.

The following table describes the commands related to port channel interfaces.

Table 15-4 Related commands for a port channel interface

Functionality	Command
VLAN	<code>switchport mode</code>
	<code>switchport access</code>
	<code>switchport protocol</code>
	<code>switchport trunk</code>
	<code>switchport mac</code>
	<code>switchport mac auto-vlan</code>
	<code>switchport vlan mapping</code>
	<code>switchport vlan mapping enable</code>
Spanning Tree Protocols	<code>spanning-tree portfast</code>
	<code>spanning-tree bpduguard</code>
	<code>spanning-tree guard</code>
	<code>spanning-tree link-type</code>
	<code>spanning-tree port-priority</code>
	<code>spanning-tree cost</code>
	<code>spanning-tree vlan port-priority</code>
	<code>spanning-tree vlan cost</code>
	<code>spanning-tree single port-priority</code>
	<code>spanning-tree single cost</code>
	<code>spanning-tree mst port-priority</code>
	<code>spanning-tree mst cost</code>
Common to Layer 2 authentication	<code>authentication arp-relay</code>
	<code>authentication ip access-group</code>
	<code>authentication force-authorized vlan</code>
	<code>authentication logout linkdown</code>

Functionality	Command
	<code>authentication max-user(interface)</code>
IEEE 802.1X	<code>dot1x authentication</code>
	<code>dot1x ignore-eapol-start</code>
	<code>dot1x max-req</code>
	<code>dot1x multiple-authentication</code>
	<code>dot1x port-control</code>
	<code>dot1x reauthentication</code>
	<code>dot1x supplicant-detection</code>
	<code>dot1x timeout reauth-period</code>
	<code>dot1x timeout tx-period</code>
	<code>dot1x timeout supp-timeout</code>
	<code>dot1x timeout server-timeout</code>
	<code>dot1x timeout keep-unauth</code>
	<code>dot1x timeout quiet-period</code>
Web authentication	<code>web-authentication authentication</code>
	<code>web-authentication html-fileset</code>
	<code>web-authentication port</code>
MAC-based authentication	<code>mac-authentication authentication</code>
	<code>mac-authentication port</code>
Multistep authentication	<code>authentication multi-step</code>
DHCP snooping	<code>ip arp inspection limit rate</code>
	<code>ip arp inspection trust</code>
	<code>ip dhcp snooping limit rate</code>
	<code>ip dhcp snooping trust</code>
	<code>ip verify source</code>
Uplink redundancy	<code>switchport backup interface</code>

Functionality	Command
	<code>switchport backup flush-request transmit</code>
L2 loop detection	<code>loop-detect on</code>
CFM	<code>ethernet cfm enable</code>
	<code>ethernet cfm mep</code>
	<code>ethernet cfm mip</code>

(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 0/1-2`
`(config-if-range)# channel-group 3 mode on`
`(config-if-range)# exit`

Adds ports 0/1 and 0/2 to channel group 3 in static mode. The port channel interface for channel group 3 is automatically generated.

2. `(config)# interface port-channel 3`
Switches channel group 3 to port channel interface configuration mode.
3. `(config-if)# switchport mode trunk`
`(config-if)# exit`
Sets channel group 3 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 0/1-2`
`(config-if-range)# channel-group 3 mode on`
`(config-if-range)# exit`
Adds ports 0/1 and 0/2 to channel group 3 in static mode.
2. `(config)# interface port-channel 3`
`(config-if)# shutdown`


```
(config-if)# exit
```

Changes the mode to port channel interface mode, and sets **shutdown**. Channel group 3 is shut down, so communication over ports 0/1 and 0/2 stops.

15.2.5 Deleting a channel group

Before you remove ports from a channel group or delete an entire channel group, 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

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 15-4 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 0/1
(config-if)# shutdown
```

Sets **shutdown** for port 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
(config-if)# exit
```

Deletes the channel group settings from port 0/1.

(2) Deleting an entire channel group

Points to note

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 **interface port-channel**. After this deletion, the **channel-group mode** configuration command is automatically deleted from each port registered in the channel group. Be careful when using a port for another purpose because the related commands that were set for the ports by using the **interface port-channel** command before the channel group was deleted remain after the removal. (For details about the related commands, see *Table 15-4 Related commands for a port channel interface*.)

Command examples

1.

```
(config)# interface range gigabitethernet 0/1-2
(config-if-range)# shutdown
(config-if-range)# exit
```

15 Link Aggregation

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 3**

Deletes channel group 3. The **channel-group mode** configuration command set for ports 0/1 and 0/2 are also deleted automatically.

15.3 Description of the link aggregation extended functionality

15.3.1 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.

Use this functionality 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.

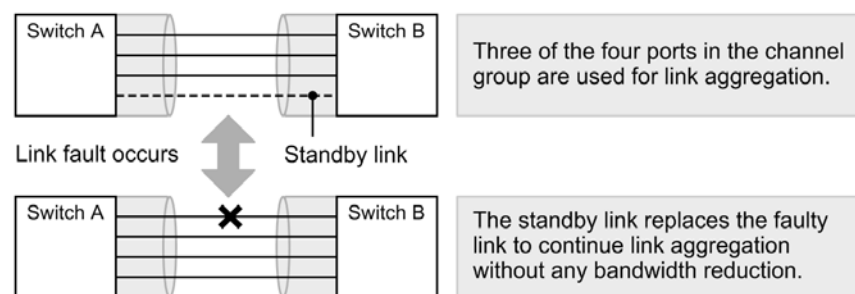
Standby ports are determined based on the port priority and port number set in the configuration. The following table describes the selection principle.

Table 15-5 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).
↑		
↓	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).
Low		

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 15-3 Example of standby link functionality operation



The Switch determines the ports to be used for a channel group as described below:

- The ports in full duplex mode that are not in the link-up state are excluded.
- The ports whose transmission speed is different from ports (which must belong to the same channel group) that are in the link-up state and have the highest transmission speed at a specific point in time are excluded.
- Ports from the remaining ports are allocated to the channel group until the maximum number of ports set by the command is reached, starting with the port that has the highest priority (the smaller value, the higher priority). For ports that have the same

priority value, the port whose port number is smaller is allocated first.

If `no-link-down` is not specified, and if the maximum number of ports have already been allocated to the channel group, the ports whose priority is lower than the priority of the ports allocated to the channel group are shut down. If there are no configuration entries that specify port priority settings and a slower port with a smaller port number is first placed in the link-up state, faster ports with larger port numbers are shut down.

(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 (standby ports) 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 (standby ports) 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 for static link aggregation, 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.

If all ports in a channel group are placed in the link-up state in half duplex mode, the channels in that group are not placed in the link-up state. However, some packets can be received.

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 the following case:

- The maximum number of active ports is set to 1 by using the `max-active-port` configuration command.

15.4 Configuration of the link aggregation extended functionality

15.4.1 List of configuration commands

The following table describes the commands used to configure the link aggregation extended functionality.

Table 15-6 List of configuration commands

Command name	Description
<code>channel-group lacp system-priority</code>	Sets the system priority for a channel group.
<code>channel-group max-active-port</code>	Enables the standby link functionality, and sets how many ports in the channel group can be used for link aggregation.
<code>lacp port-priority</code>	Sets the port priority. The port priority is used to select standby links.
<code>lacp system-priority</code>	Sets the LACP system priority for the channel groups for which the <code>channel-group lacp system-priority</code> command is not set.

15.4.2 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 3`
Switches channel group 3 to port channel interface configuration mode.
2. `(config-if)# channel-group max-active-port 3`
Enables the standby link functionality for channel group 3, and sets the maximum number of active ports in the channel group to 3. Channel group 3 operates in link-down mode.
3. `(config-if)# exit`
Changes the mode to global configuration mode.
4. `(config)# interface port-channel 5`
`(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 5, 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 0/1`
`(config-if)# channel-group 5 mode on`
`(config-if)# lacp port-priority 300`

15 Link Aggregation

```
(config-if)# exit
```

Adds port 0/1 to channel group 5, 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.

15.5 Operation for link aggregation

15.5.1 List of operation commands

The following table describes the operation commands for link aggregation.

Table 15-7 List of operation commands

Command name	Description
<code>show channel - group</code>	Shows link aggregation information.
<code>show channel - group statistics</code>	Shows the statistics for sent and received data packets for link aggregation.
<code>show channel - group statistics lacp</code>	Shows the statistics for sent and received LACPDUs.
<code>clear channel - group statistics lacp</code>	Clears the statistics for sent and received LACPDUs.

15.5.2 Checking link aggregation information

(1) Checking the connection status for link aggregation

When the `show channel - group` operation command is executed, link aggregation information is displayed. In the command execution result, **CH Status** indicates the connection status of a 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` operation command.

Figure 15-4 Results of executing show channel-group

```
> show channel - group

Date 2012/12/06 18:20:48 UTC
ChGr: 31 Mode: LACP
  CH Status      : Down    Elapsed Time: -
  Max Active Port: 8
  MAC address    : -        VLAN ID: 4093
  Actor System   : Priority: 128  MAC: 0012.e2a4.fe51  Key: 31
  Partner System : -
  Port Information
    0/23 Down State: Detached
    0/25 Down State: Detached
ChGr: 32 Mode: LACP
  CH Status      : Up      Elapsed Time: 00:15:16
  Max Active Port: 8
  Description    : lab network
  MAC address    : 0012.e254.ba14 VLAN ID: 4093
  Periodic Timer : Long
  Actor System   : Priority: 128  MAC: 0012.e2a4.fe51  Key: 32
  Partner System : Priority: 128  MAC: 0012.e2a8.85a2  Key: 32
  Port Information
    0/26 Up State: Distributing
ChGr: 33 Mode: LACP
  CH Status      : Down    Elapsed Time: -
  Max Active Port: 8
  MAC address    : -        VLAN ID: 4093
  Actor System   : Priority: 128  MAC: 0012.e2a4.fe51  Key: 33
```

```

Partner System : -
Port Information
  0/22 Up      State: Detached
ChGr: 64 Mode: Static
CH Status      : Up      Elapsed Time: 00:15:21
Max Active Port: 8
MAC address    : 0012.e254.ba12 VLAN ID: 4093
Port Information
  0/24 Up      State: Distributing

```

>

(2) Checking the operating status of each port

When the `show channel - group detail` operation command is executed, detailed status information of each port is displayed. In the command execution result, **Status** indicates the communication status of a port.

The following figure shows an example of executing the `show channel - group detail` operation command.

Figure 15-5 Results of executing show channel-group detail

```

> show channel-group detail

Date 2012/12/06 18:22:36 UTC
ChGr: 31 Mode: LACP
  CH Status      : Down      Elapsed Time: -
  Max Active Port: 8
  MAC address    : -          VLAN ID: 4093
  Actor System   : Priority: 128  MAC: 0012.e2a4.fe51  Key: 31
  Partner System : -
  Port Information
    Port: 0/23 Down
      State: Detached      Speed: -      Duplex: -
      Actor Port : Priority: 128
    Port: 0/25 Down
      State: Detached      Speed: -      Duplex: -
      Actor Port : Priority: 128
ChGr: 32 Mode: LACP
  CH Status      : Up      Elapsed Time: 00:17:04
  Max Active Port: 8
  Description    : lab network
  MAC address    : 0012.e254.ba14 VLAN ID: 4093
  Periodic Timer : Long
  Actor System   : Priority: 128  MAC: 0012.e2a4.fe51  Key: 32
  Partner System : Priority: 128  MAC: 0012.e2a8.85a2  Key: 32
  Port Information
    Port: 0/26 Up
      State: Distributing  Speed: 1G      Duplex: Full
      Actor Port : Priority: 128
      Partner System: Priority: 128  MAC: 0012.e2a8.85a2  Key: 32
      Partner Port : Priority: 128  Number: 23
ChGr: 33 Mode: LACP
  CH Status      : Down      Elapsed Time: -
  Max Active Port: 8
  MAC address    : -          VLAN ID: 4093
  Actor System   : Priority: 128  MAC: 0012.e2a4.fe51  Key: 33
  Partner System : -
  Port Information
    Port: 0/22 Up
      State: Detached      Speed: 1G      Duplex: Full
      Actor Port : Priority: 128
ChGr: 64 Mode: Static

```



```
CH Status      : Up      Elapsed Time: 00:17:11
Max Active Port: 8
MAC address    : 0012.e254.ba12  VLAN ID: 4093
Port Information
Port: 0/24 Up
  State: Distributing  Speed: 1G    Duplex: Full
```

>

16. Layer 2 Switching Overview

This chapter describes an overview of the Layer 2 switch functionality used to forward data over Layer 2 of the OSI model for the Switch.

16.1 Overview

16.2 Supported

16.3 Compatibility between Layer 2 switch functionality and other functionality

16.1 Overview

16.1.1 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.

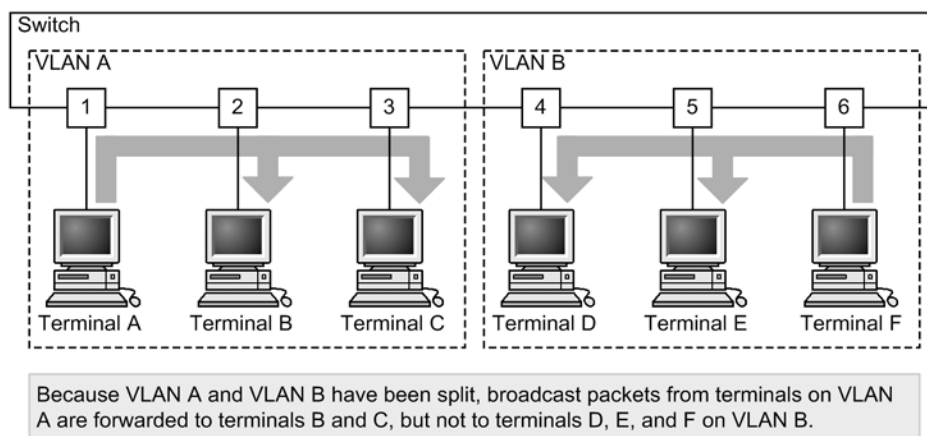
Layer 2 switches forward frames according to the entries in the MAC address table. When an entry matches the destination MAC address, the frame is forwarded to the port in the entry only if the port in the entry matches the port on which the frame was received. If no entries match, the frame is forwarded to all ports other than the one on which the frame was received. This kind of forwarding is called flooding.

16.1.2 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 shows a VLAN overview. Because the broadcast domain is divided between VLAN A and VLAN B, no frames will arrive.

Figure 16-1 VLAN overview



16.2 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 16-1 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
	VLAN tunneling	The aggregation, and tunneling, of the VLANs of multiple users on another VLAN
	Tag translation	The translation 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.
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

16.3 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 16-2 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 VLAN	
		IGMP snooping	
		MLD snooping	
		Layer 2 authentication	Partial ^{#2}
		Port mirroring (mirrored ports)	No

Functionality used		Functionality	Available
Change of VLAN tag TPIDs		Tag translation	Partial ^{#3}
		SML [OS-L2A]	
VLAN extended functionality	Tag translation	Change of VLAN tag TPIDs	Partial ^{#3}
		PVST+	No
		IGMP snooping	Partial ^{#4}
		MLD snooping	
		DHCP snooping	
		Sending filters for VLAN interfaces	
		Sending filters that contain VLAN conditions	
		SML [OS-L2A]	
		Uplink redundancy	
	VLAN tunneling	Protocol VLAN	No
		MAC VLAN	
		PVST+	
		Single Spanning Tree	
		Multiple Spanning Tree	
		IGMP snooping	
		MLD snooping	
		DHCP snooping	
		Layer 2 authentication	
		Sending filters for VLAN interfaces	
		Sending filters that contain VLAN conditions	
		Uplink redundancy	Partial ^{#5}
		sFlow statistics functionality	Partial ^{#6}

Functionality used		Functionality	Available
	L2 protocol frame transparency functionality (BPDU)	PVST+	No
		Single Spanning Tree	
		Multiple Spanning Tree	
	L2 protocol frame transparency functionality (EAP)	Layer 2 authentication	Partial ^{#2}
	Inter-port relay blocking functionality	Spanning Tree Protocols	Partial ^{#7}
		IGMP snooping	
		MLD snooping	
		DHCP snooping	
		GSRP aware	
		CFM	

#1

When using the VLAN tunneling functionality, do not use a native VLAN on a trunk port.

#2

For details, see *5 Overview of Layer 2 Authentication Functionality* in the *Configuration Guide Vol. 2*.

#3

For the port on which the functionality is enabled, you cannot set and change TPIDs.

#4

For the port on which the functionality is enabled, tag translation cannot be performed.

#5

On uplink ports, VLAN tunneling cannot be used.

#6

- Frames with two or more VLAN tags are not counted in the flow statistics.
- When using the VLAN tunneling functionality and sFlow statistics functionality together, frames that contain VLAN tags for tunneling ports (frames that contain two or more VLAN tags when the frames are sent to the trunk port) might not be counted in the flow statistics.

#7

For more details, see *19.7.2 Notes on using the inter-port relay blocking functionality*.

Table 16-3 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	
	Layer 2 authentication	Partial ^{#1}
	Uplink redundancy	Partial ^{#2}
	SML [OS-L2A]	No
Single Spanning Tree	VLAN tunneling	No
	L2 protocol frame transparency functionality (BPDU)	
	Multiple Spanning Tree	
	Layer 2 authentication	Partial ^{#1}
	Uplink redundancy	Partial ^{#2}
	SML [OS-L2A]	No
Multiple Spanning Tree	VLAN tunneling	No
	L2 protocol frame transparency functionality (BPDU)	
	Single Spanning Tree	
	PVST+	
	Loop guard	
	Layer 2 authentication	Partial ^{#1}
	Uplink redundancy	Partial ^{#2}
	SML [OS-L2A]	No

#1

For details, see 5 *Overview of Layer 2 Authentication Functionality* in the manual

Configuration Guide Vol. 2.

#2

Spanning Tree Protocols are forcibly disabled on ports set as the primary port or secondary port in uplink redundancy.

Table 16-4 Restrictions on the Ring Protocol

Functionality used	Functionality	Available
Ring Protocol	DHCP snooping (terminal filter functionality)	Partial ^{#1}
	Layer 2 authentication	Partial ^{#2}
	Uplink redundancy	Partial ^{#3}
	SML [OS-L2A]	No

#1

Set ports that are not ring ports as ports on which terminal filter is to be enabled by DHCP snooping.

#2

For details, see *5 Overview of Layer 2 Authentication Functionality* in the manual *Configuration Guide Vol. 2*.

#3

Set ports that are not ring ports as the primary port and secondary port in uplink redundancy.

Table 16-5 Restrictions on IGMP or MLD snooping

Functionality used	Functionality	Available
IGMP snooping	Default VLAN	No
	VLAN tunneling	
	Tag translation	Partial ^{#1}
	Layer 2 authentication	Partial ^{#2}
	SML [OS-L2A]	No
MLD snooping	Default VLAN	No
	VLAN tunneling	
	Tag translation	Partial ^{#1}
	SML [OS-L2A]	No

#1

For the port on which IGMP snooping and MLD snooping are enabled, tag translation cannot be used.

#2

For details, see *5 Overview of Layer 2 Authentication Functionality* in the manual *Configuration Guide Vol. 2*.

17. MAC Address Learning

This chapter describes the MAC address learning functionality and its use.

17.1	Description of MAC address learning
------	-------------------------------------

17.2	MAC address learning configuration
------	------------------------------------

17.3	MAC address learning operation
------	--------------------------------

17.1 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.

17.1.1 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 they are deleted due to aging. Learning is performed per VLAN, and the MAC address table is managed using pairs of MAC addresses and VLANs. The same MAC address is also registered if its paired VLAN is different.

17.1.2 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.

17.1.3 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 aging time might be necessary for a learned entry to be deleted.

Note that if a port goes down, all entries learned from the port are deleted. Entries learned from channel groups are deleted when the channel groups go down.

17.1.4 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 17-1 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.

17.1.5 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.

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 17-2 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	Destination port specification	Specifies one port or channel group.

17.1.6 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 17-3 When the MAC address table is cleared

Trigger	Description
Port down ^{#1}	Entries learned from the target port are deleted.
Channel group down ^{#2}	Entries learned from the target channel group are deleted.
Execution of the <code>clear mac-address-table</code> operation command	The MAC address table is cleared according to the parameters.
Spanning Tree topology change	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 the 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.

Trigger	Description
Switching between the GSRP master and backup states	When the Switch runs as 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 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.
Path switching 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 path switching is performed and flush control frames for neighboring rings are sent from the master node.
Primary port and secondary port switching due to uplink redundancy	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.
Single port on the neighboring device in an SML configuration down [OS-L2A]	When the MAC address table entry for a port is cleared: If the single port of the neighboring device in an SML configuration is down, the MAC address of the port is cleared on the device. In addition, in the entries whose learned interface is shown as peer-link in the MAC address table on the Switch, the MAC address of the down single port on the neighboring device is cleared.
Execution of the clear mac-address-table operation command at either of devices that make up an SML configuration [OS-L2A]	When the MAC address table for the entire device is cleared: When the MAC address table is cleared by using the operation command on either of the devices in an SML configuration, the MAC address table on the other device is also cleared. In such cases, the device on which the operation command is executed records as log entries a KEY input event and clearing of the MAC address table, and the other device records only clearing of the MAC address table as a log entry.
Change of SML status [OS-L2A]	When the SML status changes from Full to Standalone or Conflict , the MAC addresses of the learned interface entries for which peer-link is displayed are cleared from the MAC address table of each switch.

#1

Port down due to a line failure, execution of the **inactivate** operation command, or the settings in the **shutdown** configuration command.

#2

Channel group down due to the LACP, a line failure, or the settings in the **shutdown** configuration command.

17.1.7 Notes

(1) Aging time when the Layer 2 authentication functionality is used

The aging time for the learned entry can be set in the configuration. However, when the Layer 2 authentication functionality is used, aging is performed as described in to the following table.

Table 17-4 Aging time when the Layer 2 authentication functionality is used

Layer 2 authentication functionality configuration status	Configured aging time in the MAC address table	Aging	
		Operation	Aging time
One of the following authentication functionality is operating: 1. IEEE 802.1X <ul style="list-style-type: none"> Authentication mode: port-based authentication (static) or port-based authentication (dynamic) The non-communication monitoring functionality is enabled 2. Web authentication <ul style="list-style-type: none"> Authentication mode: fixed VLAN mode or dynamic VLAN mode The non-communication monitoring functionality is enabled 3. MAC-based authentication <ul style="list-style-type: none"> Authentication mode: fixed VLAN mode or dynamic VLAN mode The non-communication monitoring functionality is enabled 	Set to 0 seconds.	N	--
	Set in the range from 10 to 300 seconds.	Y	300 seconds
	Set in the range from 301 to 1000000 seconds.	Y	Specified time
	Not set	Y	300 seconds
All other cases	Set to 0 seconds.	N	--
	Set in the range from 10 to 300 seconds.	Y	Specified time
	Set in the range from 301 to 1000000 seconds.	Y	Specified time
	Not set	Y	300 seconds

Legend

Y: Aging is performed

N: Aging is not performed

--: Not applicable.

17.2 MAC address learning configuration

17.2.1 List of configuration commands

The following table describes the configuration commands for MAC address learning.

Table 17-5 List of configuration commands

Command name	Description
<code>mac-address-table aging-time</code>	Sets the aging time for MAC address learning.
<code>mac-address-table static</code>	Sets a static entry.

17.2.2 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.

Notes

When the Layer 2 authentication functionality is used concurrently, an aging time of 10 to 300 seconds set by the command is set to 300 seconds. For details, see *17.1.7(1) Aging time when the Layer 2 authentication functionality is used*.

17.2.3 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 destination are specified for a static entry. A port or channel group is specified as the output destination.

(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 0/1`

Sets the destination for frames for the destination MAC address 0012.e200.1122 to port 0/1 on VLAN 10.

Notes

1. On VLAN 10, any frames from source MAC address 0012.e200.1122 received by a means other than port 0/1 are discarded.

2. A VLAN that matches a VLAN automatically assigned to a port by the Layer 2 authentication functionality cannot be configured.

(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.

17.3 MAC address learning operation

17.3.1 List of operation commands

The following table describes the operation commands for MAC address learning.

Table 17-6 List of operation commands

Command name	Description
<code>show mac-address-table</code>	Shows information about the MAC address table. When the <code>learning-counter</code> parameter is specified, the learning address count for MAC address learning is displayed for each port.
<code>clear mac-address-table</code>	Clears the MAC address table.

17.3.2 Checking the status of MAC address learning

The `show mac-address-table` operation 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` operation command displays the entries registered by MAC address learning, static entries, and entries registered by the Layer 2 authentication functionality, IGMP snooping, and MLD snooping.

Figure 17-1 Results of executing `show mac-address-table`

```
> show mac-address-table
```

```
Date 2010/08/09 21:30:08 UTC
Aging time : 300
MAC address      VLAN    Type      Port-list
0012.e2cf.fd5d    1       Dot1x     0/6
0012.e203.0110    1       Dynamic   0/15
0012.e203.0132    1       Dynamic   0/49
0012.e200.00fb    1       Snoop     0/3, 0/6-15, 0/18-22, 0/24-32, 0/34-44, 0/48-49
0012.e27f.ffffa   1       Snoop     0/6
0012.e2a5.429c    2       Dynamic   0/24, 0/48
0012.e2a5.e756    2       MacAuth   0/50
0012.e2a5.e895    4094    Static    0/24, 0/48
0012.e2a5.ee4e    4094    WebAuth   0/5
```

```
>
```

17.3.3 Checking the MAC address learning count

The `show mac-address-table` operation 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 connected terminals 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 17-2 Results of executing show mac-address-table (with the learning-counter parameter specified)

```
> show mac-address-table learning-counter
```

```
Date 2010/08/09 21:47:47 UTC
```

Port	Count
------	-------

0/1	0
-----	---

0/2	13961
-----	-------

0/3	12
-----	----

0/4	2
-----	---

0/5	0
-----	---

0/6	0
-----	---

0/7	0
-----	---

0/8	0
-----	---

0/9	0
-----	---

0/10	0
------	---

0/11	0
------	---

0/12	0
------	---

0/13	0
------	---

0/14	0
------	---

0/15	1
------	---

:

:

:

ChGr: 8	0
---------	---

ChGr: 62	13
----------	----

ChGr: 63	1
----------	---

ChGr: 64	34
----------	----

```
>
```

18. VLAN

VLAN functionality divides a switch internally into virtual groups. This chapter describes VLANs and their use.

18.1	Description of the basic VLAN functionality
18.2	Configuration of the basic VLAN functionality
18.3	Description of port VLANs
18.4	Configuration of port VLANs
18.5	Description of protocol VLANs
18.6	Configuration of protocol VLANs
18.7	Description of MAC VLANs
18.8	Configuration of MAC VLANs
18.9	VLAN operation

18.1 Description of the basic VLAN functionality

This section provides an overview of VLANs.

18.1.1 VLAN type

The following table describes the types of VLAN supported by the Switches.

Table 18-1 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.

18.1.2 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 18-2 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. Any received tagged frames are discarded.	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. Any received tagged frames are handled according to the configuration settings. For details, see <i>18.7.4 Optional functionality for MAC ports</i> .	MAC VLAN Port VLAN
Trunk port	Handles a tagged frame as all types of VLANs. With this port, the VLAN is determined by the VLAN tag. Any received untagged frames are handled on the native VLAN.	Port VLAN Protocol VLAN MAC VLAN
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

The table below describes the types of VLANs that can be used for each port type. A trunk port that handles VLAN tags can be used with all types of VLANs.

Table 18-3 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 a tunneling port. This VLAN is called the native VLAN on each port.

On each port other than access ports or tunneling ports, the port VLAN already created for each port can be set as the native VLAN. VLAN 1 (the default VLAN) is used as the native VLAN for ports not specified in the configuration.

18.1.3 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, the ports might not automatically belong to the default VLAN. The following ports do not automatically belong to the default VLAN:

- Access ports for which a VLAN other than VLAN 1 is specified
- All ports, when VLAN tunneling is configured
- Mirror ports
- SML peer link port [OS-L2A]

Ports other than access ports (protocol ports, MAC ports, trunk ports, and tunneling ports) cannot be automatically assigned to a VLAN.

18.1.4 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.

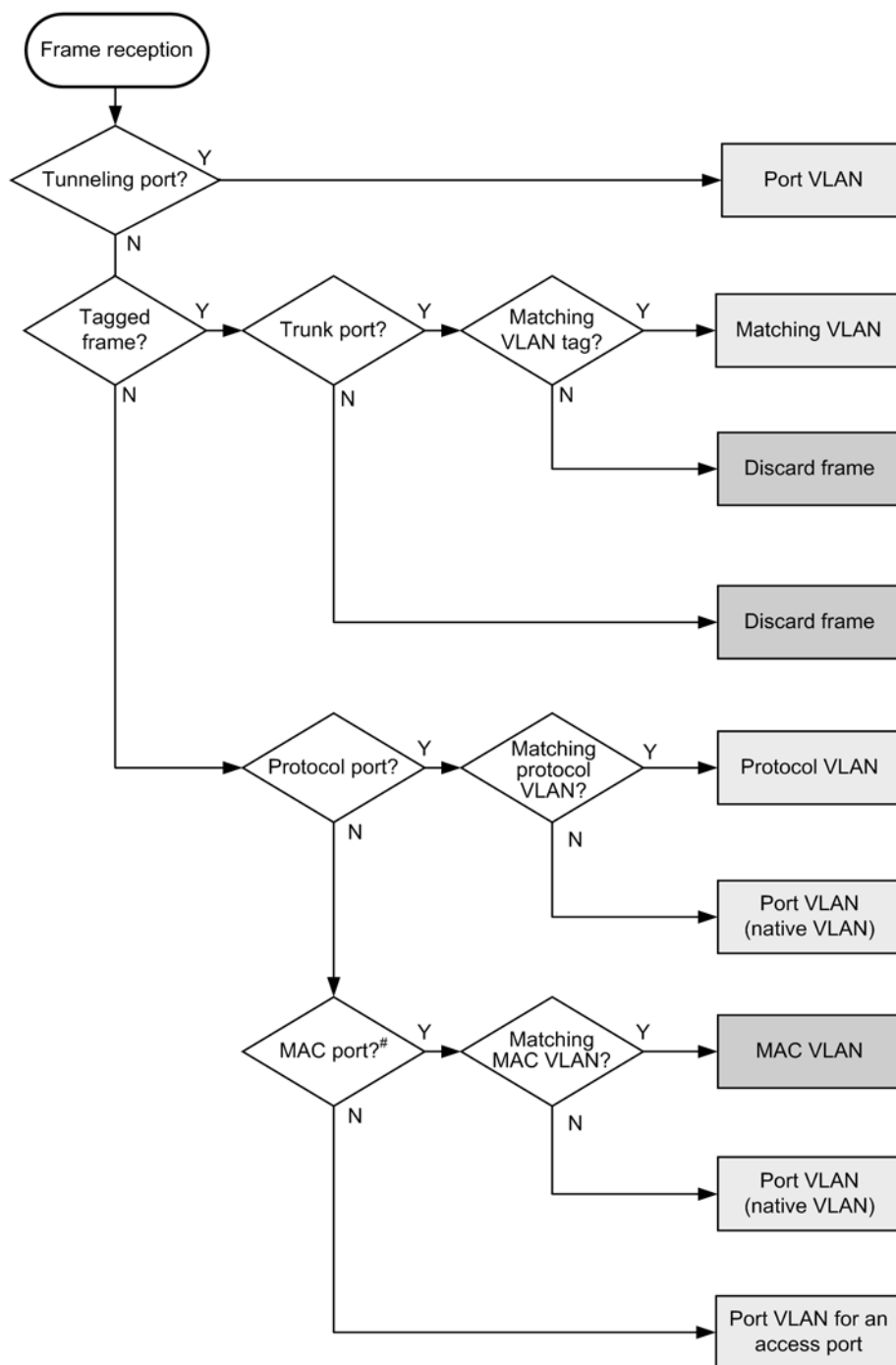
Table 18-4 Priority for determining the VLAN

Port type	Priority
Access port	Port VLAN
Protocol port	Protocol VLAN > port VLAN (native VLAN)
MAC port	VLAN tag [#] > MAC VLAN > port VLAN (native VLAN)
Trunk port	VLAN tag > port VLAN (native VLAN)
Tunneling port	Port VLAN

#

Tagged frames can be handled depending on the configuration. For details, see *18.7.4 Optional functionality for MAC ports*.

The following figure shows the algorithm for determining the VLAN.

Figure 18-1 Algorithm for determining the VLAN

#: Depending on the configuration settings, the tagged framed can also be used.

18.1.5 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 are handled on trunk ports and MAC ports. For a communication between trunk

ports or MAC ports, the partner switch also must recognize VLAN tags on the trunk port or MAC port.

(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 a VLAN tag are inserted: Ethernet V2 and 802.3.

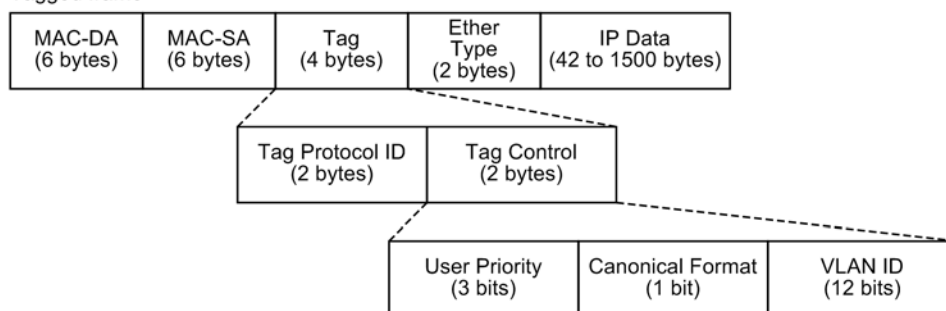
Figure 18-2 Tagged-frame format

● Ethernet II frame

Normal frame

MAC-DA (6 bytes)	MAC-SA (6 bytes)	Ether Type (2 bytes)	IP Data (46 to 1500 bytes)
---------------------	---------------------	----------------------------	-------------------------------

Tagged frame



● 802.3LLC/SNAP frame

Normal frame

MAC-DA (6 bytes)	MAC-SA (6 bytes)	Length (2 bytes)	LLC (3 bytes)	SNAP (5 bytes)	IP Data (38 to 1492 bytes)
---------------------	---------------------	---------------------	------------------	-------------------	-------------------------------

Tagged frame

MAC-DA (6 bytes)	MAC-SA (6 bytes)	Tag (4 bytes)	Length (2 bytes)	LLC (3 bytes)	SNAP (5 bytes)	IP Data (34 to 1492 bytes)
---------------------	---------------------	------------------	---------------------	------------------	-------------------	-------------------------------

The following table describes the fields for VLAN tags.

Table 18-5 VLAN tag fields

Field	Description	Conditions for the Switch
TPID (Tag Protocol ID)	Holds 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.
VLAN ID	Indicates the VLAN ID [#] .	VLAN IDs from 1 to 4094 can be used.

#

When tag translation is enabled, VLAN IDs set by tag translation are used. For details, see *19.3 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 user priority of frames to be forwarded by the Switch is the same as that of received frames. The default user priority value is as follows:

- When received frames are forwarded frames: 3
- Frames originated by the device: 7

The user priority of frames to be sent can be changed by configuration. For details about changing the user priority, see the following:

- Forwarded frames: *3.4 Description of marking* in the manual *Configuration Guide Vol. 2*
- Frames originated by the device: *3.10 Description of user priority for frames originated by a Switch* in the manual *Configuration Guide Vol. 2*

18.1.6 Notes on VLAN usage

(1) Notes on use with other functionality

For details, see *16.3 Compatibility between Layer 2 switch functionality and other functionality*.

18.2 Configuration of the basic VLAN functionality

18.2.1 List of configuration commands

The following table describes the configuration commands for the basic VLAN functionality.

Table 18-6 List of configuration commands

Command name	Description
<code>name</code>	Sets a VLAN name.
<code>state</code>	Sets the VLAN status (started/stopped).
<code>switchport access</code>	Sets a VLAN for an access port.
<code>switchport dot1q ethertype</code>	Sets the VLAN tag TPID for a port.
<code>switchport mac</code>	Sets the MAC VLAN port information.
<code>switchport mode</code>	Sets the port type (access, protocol, MAC, trunk, or tunneling).
<code>switchport protocol</code>	Sets a VLAN for a protocol port.
<code>switchport trunk</code>	Sets a VLAN for a trunk port.
<code>vlan</code>	Creates a VLAN. Sets VLAN-related information in VLAN configuration mode.
<code>vlan-dot1q-ethertype</code>	Sets the default value for VLAN tag TPIDs.

18.2.2 Configuring VLANs

Points to note

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` configuration command is used to switch to VLAN configuration mode. If a created VLAN is specified, only the mode is switched. 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**
(config-vlan) # exit

Stops in batch mode the port VLANs created with VLAN IDs 100 to 200.

18.2.3 Configuring ports

Points to note

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 0/1**

Switches to the Ethernet interface configuration mode for port 0/1.

2. **(config-if) # switchport mode access**
(config-if) # exit

Sets port 0/1 as an access port. Port 0/1 handles untagged frames for the port VLAN.

3. **(config) # interface port-channel 3**

Switches channel group 3 to port channel interface configuration mode.

4. **(config-if) # switchport mode trunk**
(config-if) # exit

Sets channel group 3 as a trunk port. Port channel 3 handles tagged frames.

18.2.4 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** configuration command. The VLANs handled by this port are set using the **switchport trunk allowed vlan** configuration command.

To add VLANs, the **switchport trunk vlan add** configuration command is used. To remove VLANs, the **switchport trunk vlan remove** configuration command is used. If the **switchport trunk allowed vlan** configuration command is executed again after having already been used to configure settings, the list of specified VLAN IDs replaces the current list.

Command examples

1. `(config)# vlan 10-20, 100, 200-300`
`(config-vlan)# exit`
`(config)# interface gigabitethernet 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 0/1, and sets it as a trunk port. At this point, port 0/1 does not belong to any VLAN.
2. `(config-if)# switchport trunk allowed vlan 10-20`

Sets VLANs 10 to 20 for port 0/1. Port 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 0/1.
4. `(config-if)# switchport trunk allowed vlan remove 15, 16`

Deletes VLAN 15 and VLAN 16 from the VLANs handled by port 0/1. At this point, port 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`
`(config-if)# exit`

Sets VLANs 200 to 300 as VLANs to be handled by port 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 *18.4.3 Configuring native VLANs for trunk ports*.

18.2.5 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` configuration command can be used to set the default value for the switch, and the `switchport dot1q ethertype` configuration 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 is set for each port in 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 0x9100.
2. `(config)# interface gigabitethernet 0/1`

Switches to the Ethernet interface configuration mode for port 0/1.

3. `(config-if)# switchport dot1q ethertype 8100`
`(config-if)# exit`

Sets the TPID of port 0/1 to 0x8100. Port 0/1 recognizes 0x8100 as the VLAN tag TPID. 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.

18.3 Description of port VLANs

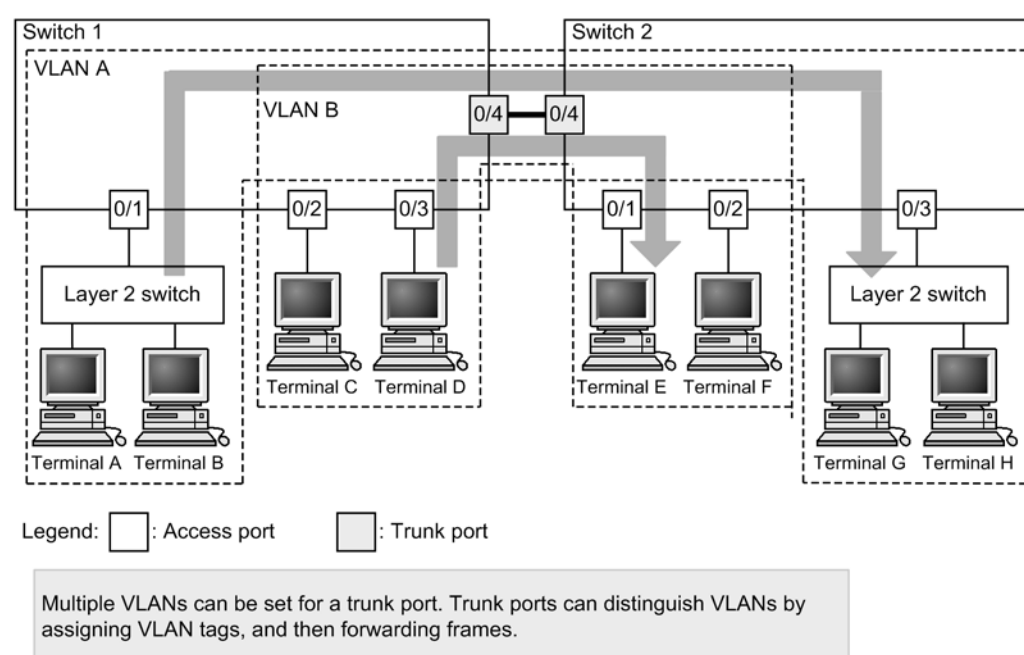
A port VLAN divides a VLAN into groups by port.

18.3.1 Access ports and trunk ports

In a port VLAN, a single VLAN is assigned 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 0/1 to 0/3 set port VLANs as access ports. These switches are connected by a trunk port (port 0/4). VLAN tags are used in this case.

Figure 18-3 Example port VLAN configuration



18.3.2 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. This VLAN can also be changed to another port VLAN in the configuration.

For example, when VLAN B is set as the native VLAN for the trunk port in *Figure 18-3 Example port VLAN configuration*, VLAN B forwards untagged frames, even for the trunk port.

18.3.3 Notes on port VLAN usage

(1) Note on tagged frames on access ports

Access ports handle untagged frames, discard any received tagged frames, and cannot send them. 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.

18.4 Configuration of port VLANs

18.4.1 List of configuration commands

The following table describes the configuration commands for port VLANs.

Table 18-7 List of configuration commands

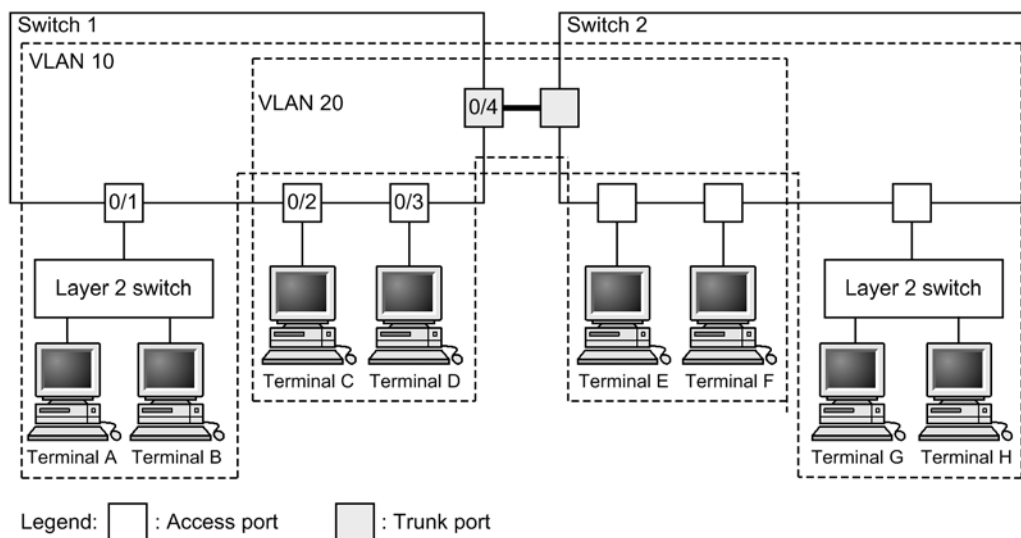
Command name	Description
<code>switchport access</code>	Sets a VLAN for an access port.
<code>switchport mode</code>	Sets the port type (access or trunk).
<code>switchport trunk</code>	Sets a VLAN for a trunk port.
<code>vlan</code>	Creates a port VLAN. Sets VLAN-related information in VLAN configuration mode.

18.4.2 Configuring a port VLAN

The following explains how to set a port VLAN. The figure below shows example settings for Switch 1.

Port 0/1 is set for port VLAN 10. Ports 0/2 and 0/3 are set for port VLAN 20. Port 0/4 is the trunk port, and all VLANs are set for it.

Figure 18-4 Example port VLAN settings



(1) Creating a port VLAN

Points to note

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`
`(config-vlan) # exit`

Creates VLAN ID 10 and VLAN ID 20 as port VLANs.

(2) Setting access ports

When a single VLAN is set to a single port and untagged frames are handled, the port is set as an access port.

Points to note

Set a port for the access port, and set the VLANs handled by the access port.

Command examples

1. `(config)# interface gigabitethernet 0/1`
Switches to the Ethernet interface configuration mode for port 0/1.
2. `(config-if)# switchport mode access`
`(config-if)# switchport access vlan 10`
`(config-if)# exit`
Sets port 0/1 as an access port. Then, sets VLAN 10.
3. `(config)# interface range gigabitethernet 0/2-3`
Switches ports 0/2 and 0/3 to Ethernet interface configuration mode. Because the configuration is the same for ports 0/2 and 0/3, setting is done as a batch operation.
4. `(config-if-range)# switchport mode access`
`(config-if-range)# switchport access vlan 20`
`(config-if-range)# exit`
Sets ports 0/2 and 0/3 as access ports. Then, sets VLAN 20.

(3) Setting trunk ports

Points to note

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 0/4`
Switches to the Ethernet interface configuration mode for port 0/4.
2. `(config-if)# switchport mode trunk`
`(config-if)# switchport trunk allowed vlan 10, 20`
`(config-if)# exit`
Sets port 0/4 as a trunk port. Then, sets VLAN 10 and VLAN 20.

18.4.3 Configuring native VLANs for trunk ports

Points to note

Set a native VLAN for handling untagged frames on a trunk port. Port VLANs or MAC VLANs can be set for a native VLAN.

When the VLAN ID of a native VLAN is specified for the `switchport trunk allowed vlan` configuration 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)# vlan 300 mac-based`
`(config-vlan)# exit`

Creates VLAN ID 300 as a MAC VLAN.

3. `(config)# interface gigabitethernet 0/1`
`(config-if)# switchport mode trunk`

Switches to the Ethernet interface configuration mode for port 0/1. Then, sets the port as a trunk port. At this point, the native VLAN for trunk port 0/1 is the default VLAN.

4. `(config-if)# switchport trunk allowed vlan 1, 10, 20, 300`
`(config-if)# switchport trunk native vlan 300`
`(config-if)# exit`

Sets trunk port 0/1 to VLANs 1, 10, 20, and 300 using the `allowed vlan` specification, and sets the native VLAN to VLAN 300. VLAN 1 (the default VLAN), VLAN 10, and VLAN 20 handle tagged frames. VLAN 300 (the native VLAN) handles untagged frames.

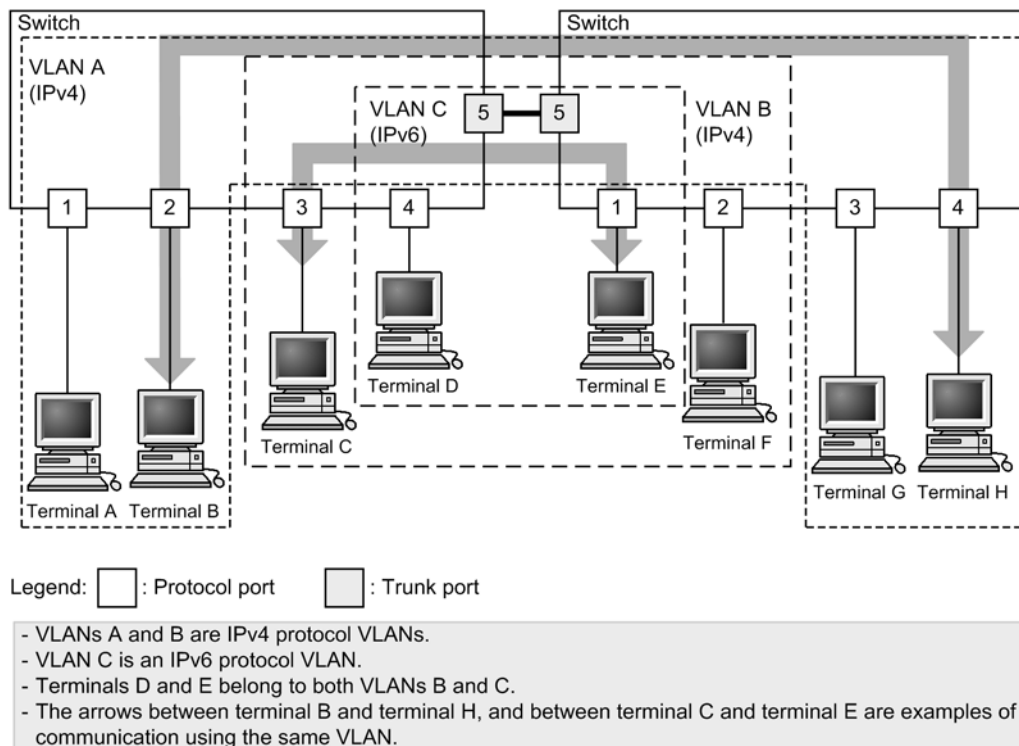
18.5 Description of protocol VLANs

18.5.1 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 example, VLANs A and B are configured with the IPv4 protocol, and VLAN C is configured with the IPv6 protocol.

Figure 18-5 Example protocol VLAN configuration



18.5.2 Distinguishing protocols

The following table describes the three types of values that can be used to distinguish protocols.

Table 18-8 Values for distinguishing protocols

Distinguishing value	Overview
EtherType value	Protocols are distinguished by the EtherType value of Ethernet V2 format frames.
LLC value	Protocols are distinguished by the LLC value (DSAP or SSAP) of 802.3 format frames.
SNAP EtherType value	Protocols are distinguished by the EtherType value of 802.3 format frames. This applies only to frames with an LLC value of AA AA 03.

Protocols are created according to the configuration and are associated with VLANs. Multiple protocols can be associated with a single protocol VLAN.

18.5.3 Protocol ports and trunk ports

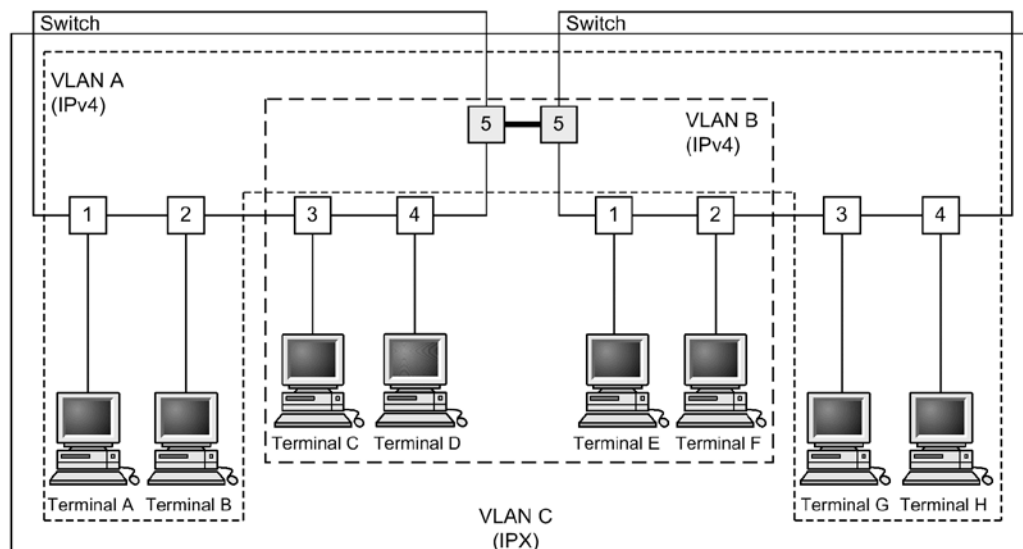
Protocol ports identify the protocol for untagged frames. The ports used for protocol VLANs are set as protocol ports. Different VLANs over multiple protocols can be assigned to a protocol port. Trunk ports are used to connect multiple protocol VLANs to another LAN switch. Note that because trunk ports distinguish VLANs by their VLAN tag, they do not distinguish VLANs according to protocol.

18.5.4 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. This VLAN also can be changed to another port VLAN in the configuration.

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 18-6 Example configuration using the native VLAN for the protocol port



Legend: : Protocol port : Trunk 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.

18.6 Configuration of protocol VLANs

18.6.1 List of configuration commands

The following table describes the configuration commands for protocol VLANs.

Table 18-9 List of configuration commands

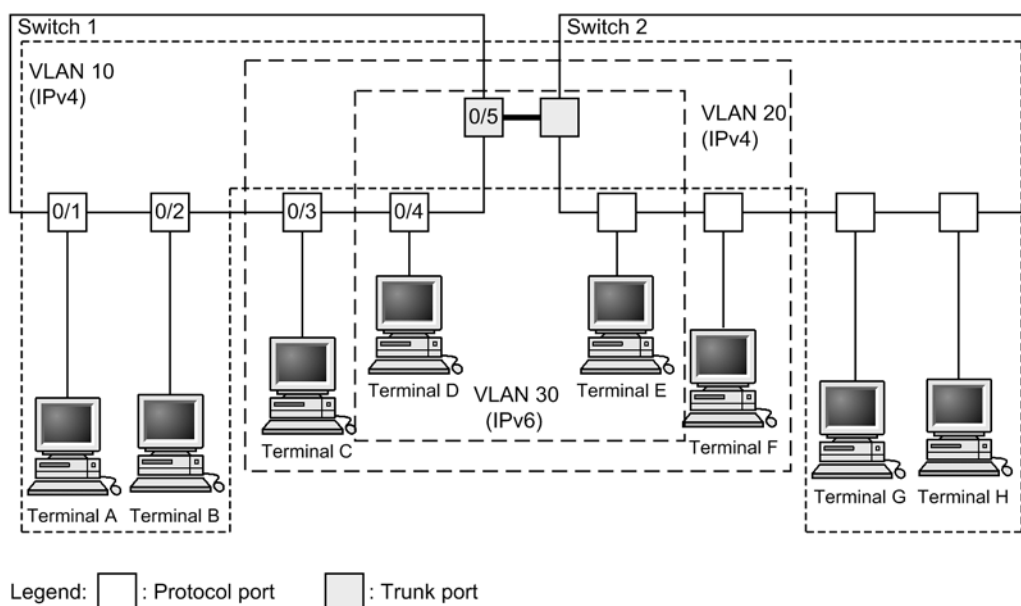
Command name	Description
<code>protocol</code>	Sets the protocol for identifying VLANs in protocol VLANs.
<code>switchport mode</code>	Sets the port type (protocol or trunk).
<code>switchport protocol</code>	Sets the VLAN for protocol ports.
<code>switchport trunk</code>	Sets the VLAN for a trunk port.
<code>vlan-protocol</code>	Sets the protocol name and protocol value for a protocol VLAN.
<code>vlan protocol-based</code>	Creates a protocol VLAN. Sets VLAN-related information in VLAN configuration mode.

18.6.2 Creating protocol VLANs

The following explains how to set a protocol VLAN. The figure below shows example settings for Switch 1.

Ports 0/1 and 0/2 are set for IPv4 protocol VLAN 10. Ports 0/3 and 0/4 are set for IPv4 protocol VLAN 20. Port 0/4 belongs to both VLAN 20 and IPv6 protocol VLAN 30 at the same time. Port 0/5 is the trunk port, and all VLANs are set for it.

Figure 18-7 Example settings for protocol VLANs



(1) Creating protocols to distinguish VLANs

Points to note

Before creating protocol VLANs, use the `vlan-protocol` command to set protocols

for distinguishing VLANs. Set the protocol name and protocol value for a protocol. Multiple protocol values can be associated with a single name.

Because the IPv4 protocol requires that both an IPv4 EtherType value and ARP EtherType value are specified at the same time, two protocol values are associated with IPv4.

Command examples

1. `(config) # vlan-protocol IPV4 ethertype 0800, 0806`

Creates a protocol named IPV4. The IPv4 EtherType value 0800 and the ARP EtherType 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 EtherType value 86DD is associated as the protocol value.

Notes

If the EtherType value is 05FF or less, 0000 is used.

(2) Creating protocol VLANs

Points to note

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`

`(config-vlan) # exit`

Creates VLAN 30 as a protocol VLAN. Specifies the created IPv6 protocol 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 0/1-2`

Switches ports 0/1 and 0/2 to Ethernet interface configuration mode. Because ports

0/1 and 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 0/1 and 0/2 as protocol ports. Then, sets VLAN 10.

3.

```
(config)# interface range gigabitethernet 0/3-4
(config-if-range)# switchport mode protocol-vlan
(config-if-range)# switchport protocol vlan 20
(config-if-range)# exit
```

Sets ports 0/3 and 0/4 as protocol ports. Then, sets VLAN 20.

4.

```
(config)# interface gigabitethernet 0/4
(config-if)# switchport protocol vlan add 30
(config-if)# exit
```

Adds VLAN 30 to port 0/4. Two types of protocol VLANs, IPv4 and IPv6, are set for port 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 0/5
```

Switches to the Ethernet interface configuration mode for port 0/5.
2.

```
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 10, 20, 30
(config-if)# exit
```

Sets port 0/5 as a trunk port. Then, sets VLAN 10, VLAN 20, and VLAN 30.

18.6.3 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 native VLANs.

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 0/1`

```
(config-if)# switchport mode protocol-vlan
```

Switches to the Ethernet interface configuration mode for port 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
```

```
(config-if)# exit
```

Sets the native VLAN for protocol port 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.

18.7 Description of MAC VLANs

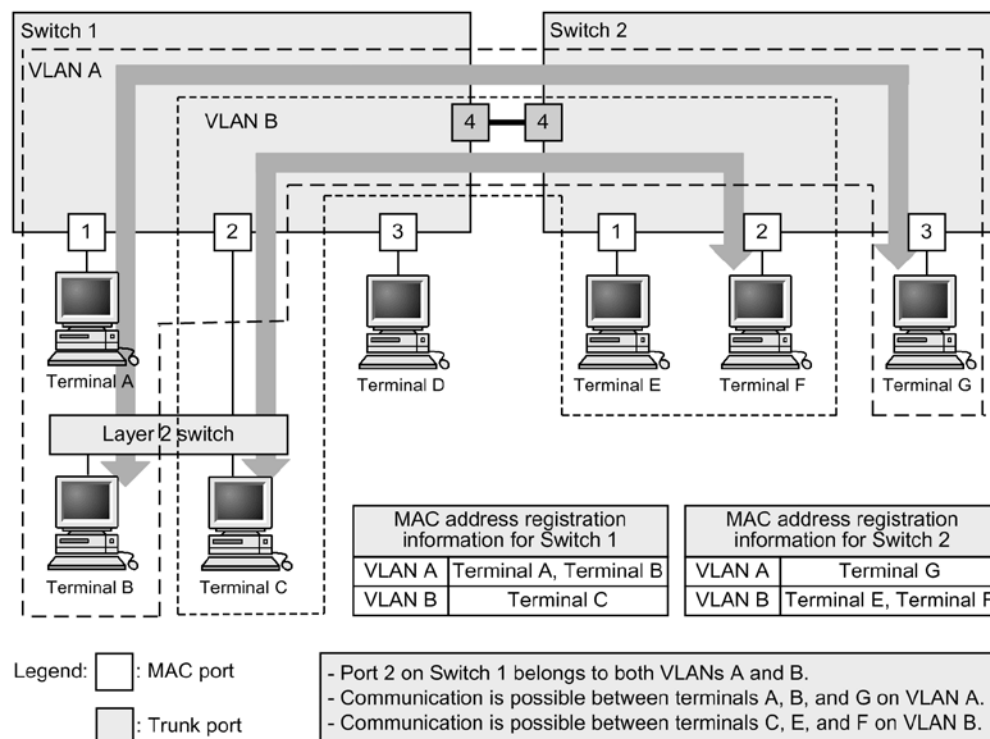
18.7.1 Overview

A MAC VLAN divides 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.

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 18-8 Example MAC VLAN configuration

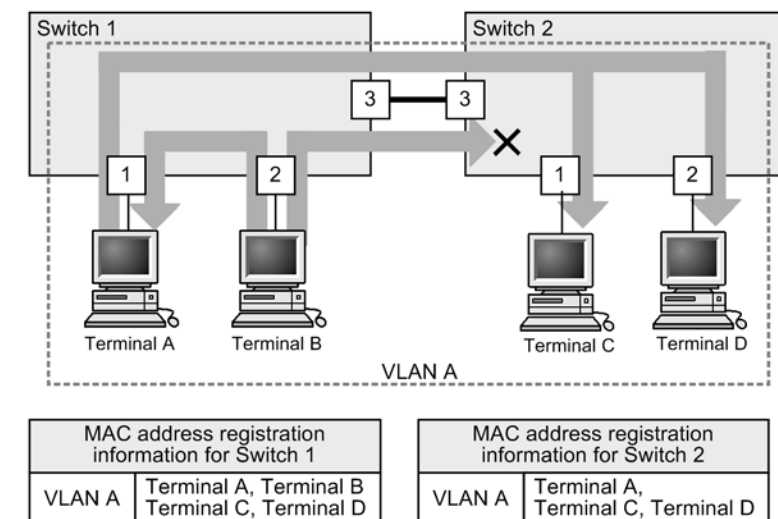


18.7.2 Connections between switches and MAC address settings

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 18-8 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 18-9 Switches connected by MAC port

Legend:  : MAC port

- Because terminal A is set on both Switches 1 and 2, terminal A can communicate with terminal C and terminal D.
- Because terminal B is not set on Switch 2, terminal B cannot communicate with terminal C and terminal D.
Terminal B can communicate with terminal A.

18.7.3 Linkage with the Layer 2 authentication functionality

(1) Dynamically registering MAC addresses with MAC VLANs

MAC VLANs can link with the Layer 2 authentication functionality to dynamically register MAC addresses with a VLAN. The following are the types of Layer 2 authentication functionality that can be linked:

- IEEE 802.1X: Port-based authentication (dynamic)
- Web authentication: Dynamic VLAN mode
- MAC-based authentication: Dynamic VLAN mode

When the same MAC address is set by configuration and the Layer 2 authentication functionality, the configuration MAC address is registered with the MAC VLAN.

To handle untagged frame devices such as a printer or a server in a VLAN intended for a MAC port without the Layer 2 authentication, use the `mac-address` configuration command to register the MAC address of the device with the MAC VLAN.

For IEEE 802.1X port-based authentication (dynamic), and Web authentication and MAC-based authentication in dynamic VLAN mode use the `mac-address-table static` configuration command to register the MAC address of the target device in the MAC address table.

Tagged frames can be forwarded to a MAC port in a VLAN for which the `switchport mac dot1q vlan` configuration command has been specified. For details about this functionality and the Layer 2 authentication functionality, see 18.7.4 *Optional functionality for MAC ports*.

For details about the Layer 2 authentication functionality, see 5 *Overview of Layer 2 Authentication Functionality* in the manual *Configuration Guide Vol. 2* and the description of each authentication functionality.

(2) Automatic VLAN assignment for a MAC port

To set VLANs for a MAC port, use the `switchport mac vlan` configuration command or assign VLANs automatically by using the Layer 2 authentication functionality.

The following are the types of Layer 2 authentication functionality for which automatic VLAN assignment is valid:

- IEEE 802.1X: Port-based authentication (dynamic)
- Web authentication: Dynamic VLAN mode
- MAC-based authentication: Dynamic VLAN mode

When a VLAN that is the same as an automatically assigned VLAN is set for a port by using the `switchport mac vlan` configuration command, the automatically assigned VLAN is canceled. However, authentication is not canceled for terminals that have already been authenticated because that configuration is followed.

To disable the automatic VLAN assignment for MAC ports, use the `no switchport mac auto-vlan` configuration command.

For details about the automatic VLAN assignment of the Layer 2 authentication functionality, see *5.4 Functionality common to all Layer 2 authentication modes* in the manual *Configuration Guide Vol. 2*.

18.7.4 Optional functionality for MAC ports

An optional functionality available for MAC ports is the forwarding of tagged frames of an arbitrary VLAN ID on a MAC port.

To use this option, set the `switchport mac dot1q vlan` configuration command. The types of VLANs that can be specified for the `switchport mac dot1q vlan` configuration command are port VLANs and MAC VLANs.

Because the devices for the tagged frames to be handled by VLANs specified in this option are handled according to VLAN tag in a frame, MAC addresses do not need to be registered by configuration.

(1) Behavior of received frames

Tagged frames for which a VLAN ID is set in the `switchport mac dot1q vlan` configuration command are forwarded to the corresponding VLAN. Note that when this command is configured, tagged frames that have a VLAN ID set in *Table 18-11 Configuration commands and specifiable VLAN types* are forwarded.

(2) Behavior of sent frames

Whether there are tags differs according to the destination of tagged frames in the VLAN set in the `switchport mac dot1q vlan` configuration command.

Table 18-10 Destination and processing of tagged frames

Destination	Tagged frame processing
Access port	Tags are removed, and untagged frames are sent.
Native VLANs for trunk ports	Tags are removed, and untagged frames are sent.
Other than native VLANs for trunk ports	Tagged frames are sent.
Native VLANs for protocol ports	Tags are removed, and untagged frames are sent.

Destination	Tagged frame processing
MAC VLANs for MAC ports	Tags are removed, and untagged frames are sent.
VLANs specified in <code>dot1q vlan</code> for MAC ports	Tagged frames are sent.

(3) Notes on using the optional functionality

(a) Exclusively configured VLANs

ALL VLANs specified by the following configuration command have an exclusive configuration. Already specified VLAN IDs cannot be specified for other commands.

Table 18-11 Configuration commands and specifiable VLAN types

Configuration command	Specifiable VLAN types
<code>switchport mac dot1q vlan</code>	Port VLAN, MAC VLAN
<code>switchport mac vlan</code>	MAC VLAN
<code>switchport mac native vlan</code>	Port VLAN

(b) `switchport mac dot1q vlan` configuration command

This command becomes available when the `switchport mode mac-vlan` configuration command has been set.

(c) Using the optional functionality with the Layer 2 authentication functionality

When the `switchport mac dot1q vlan` configuration command has been set for a MAC port, untagged frames, tagged frames, and Layer 2 authentication operate in the VLAN as follows.

- Untagged frames and Layer 2 authentication

Use is possible as described in *18.7.3 Linkage with the Layer 2 authentication functionality*.

- Tagged frames and Layer 2 authentication

When the Web authentication or MAC-based authentication in fixed VLAN mode is set for the interface port handling the VLAN, tagged frames whose VLAN IDs are set as described in *Table 18-11 Configuration commands and specifiable VLAN types* are authenticated in fixed VLAN mode.

To prevent tagged frames from being authenticated in fixed VLAN mode, use the `mac-address-table static` configuration command to register the corresponding MAC address and VLAN ID[#].

[#]: Specify the VLAN ID set in the `switchport mac dot1q vlan` configuration command.

18.8 Configuration of MAC VLANs

18.8.1 List of configuration commands

The following table describes the configuration commands for MAC VLANs.

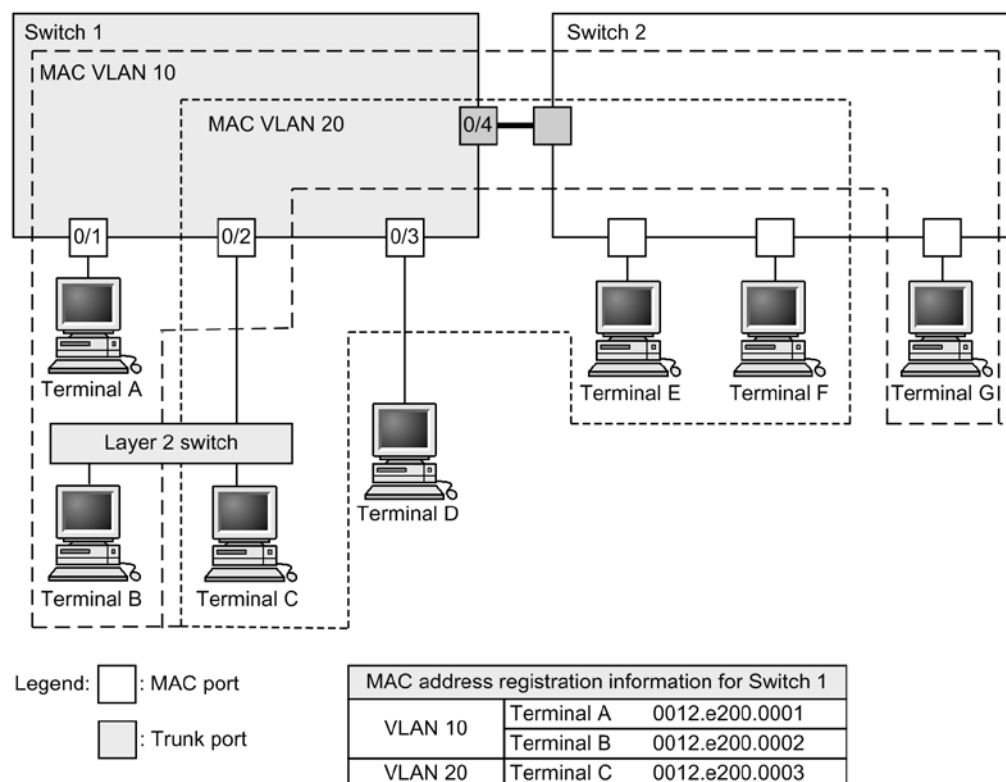
Table 18-12 List of configuration commands

Command name	Description
<code>mac-address</code>	Sets by configuration the MAC address of a terminal belonging to a VLAN in a MAC VALN.
<code>switchport mac vlan</code>	Sets the VLAN of a MAC port.
<code>switchport mac auto-vlan</code>	If no <code>switchport mac auto-vlan</code> is set, communication is possible only when post-authentication VLANs specified by the authentication functionality match VLANs specified by <code>switchport mac vlan</code> . This disables the automatic assigning of VLANs for MAC VLANs.
<code>switchport mode</code>	Sets the port type (MAC or trunk).
<code>switchport trunk</code>	Sets a VLAN for a trunk port.
<code>vlan mac-based</code>	Creates a MAC VLAN. Sets VLAN-related information in VLAN configuration mode.

18.8.2 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 the Layer 2 authentication functionality, see *Settings and Operation* for each authentication functionality in the manual *Configuration Guide Vol. 2*.

The figure below shows example settings for Switch 1. Port 0/1 is set for MAC VLAN 10. Port 0/2 is set for MAC VLANs 10 and 20, and port 0/3 is set for MAC VLAN 20. Note that terminal D, for which no MAC address is registered, is connected to port 0/3.

Figure 18-10 Example MAC VLAN settings

(1) Creating MAC VLANs and registering MAC addresses

Points to note

Create a MAC VLAN by specifying a VLAN ID and the **mac-based** parameter.

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`

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) # mac-address 0012. e200. 0003`
`(config-vlan) # exit`

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 0/1-2`

Switches ports 0/1 and 0/2 to Ethernet interface configuration mode. This setting is done in a batch operation because MAC VLAN 10 is set to ports 0/1 and 0/2.

2. `(config-if-range)# switchport mode mac-vlan`

`(config-if-range)# switchport mac vlan 10`

`(config-if-range)# exit`

Sets ports 0/1 and 0/2 for the MAC port, and sets VLAN 10.

3. `(config)# interface range gigabitethernet 0/2-3`

`(config-if-range)# switchport mode mac-vlan`

`(config-if-range)# switchport mac vlan add 20`

`(config-if-range)# exit`

Sets ports 0/2 and 0/3 as MAC ports, and sets VLAN 20. Because port 0/2 has already been set to VLAN 10, use the `switchport mac vlan add` configuration command for additional settings. Port 0/3 has the same meaning as the initial setting.

Notes

The `switchport mac vlan` configuration 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 MAC VLANs are already running, use the `switchport mac vlan add` and `switchport mac vlan remove` configuration commands.

(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 0/4`

Switches to the Ethernet interface configuration mode for port 0/4.

2. `(config-if)# switchport mode trunk`

`(config-if)# switchport trunk allowed vlan 10, 20`

`(config-if)# exit`

Sets port 0/4 as a trunk port. Then, sets VLAN 10 and VLAN 20.

18.8.3 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` configuration 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 VLANs 10 and 20 as MAC VLANs. Then, creates VLAN 30 as a port VLAN.

2. `(config) # interface gigabitethernet 0/1`

```
(config-if) # switchport mode mac-vlan
```

Switches to the Ethernet interface configuration mode for port 0/1. Sets the port as a MAC port.

3. `(config-if) # switchport mac vlan 10, 20`

Sets MAC VLANs 10 and 20 to port 0/1.

Port 0/1 permits only MAC VLAN 10 and 20 communication. Unregistered MAC addresses cannot be used for communication. To use an unregistered MAC address for communication, change the settings to allow communication to be established from the native VLAN.

4. `(config-if) # switchport mac native vlan 30`

```
(config-if) # exit
```

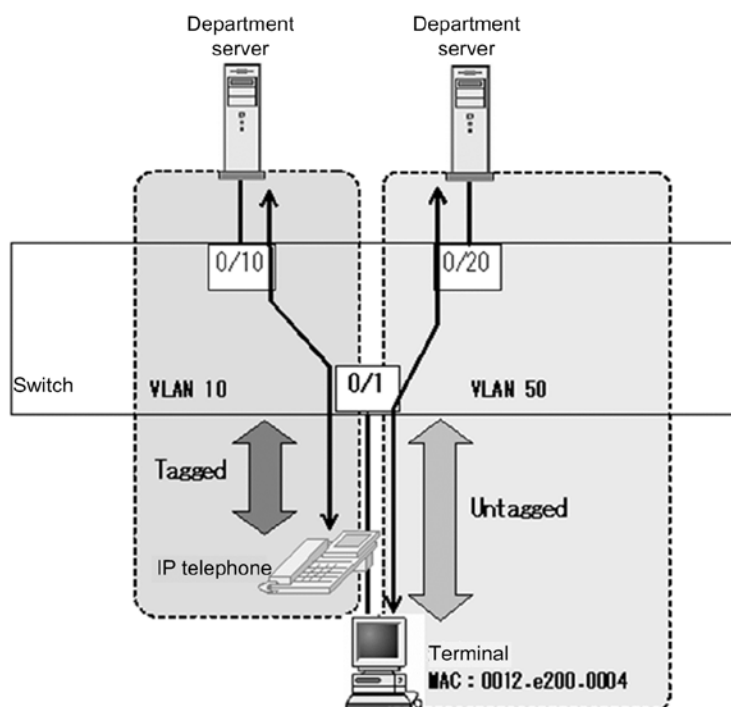
Sets port VLAN 30 as the native VLAN for port 0/1. VLAN 30 handles untagged frames from MAC addresses not registered for port 0/1.

18.8.4 Configuring tagged frame forwarding on a MAC port

When a tagged frame is received from an IP telephone, and an untagged frame is received from a terminal handled by the IP telephone on the same port as shown in the following figure, use the optional functionality for MAC ports.

This optional functionality enables tagged frame and untagged frame forwarding on the same MAC port by specifying a VLAN ID for tagged frame forwarding in the `switchport mac dot1q vlan` configuration command.

For details about the settings for authenticating IP telephones and terminals by using the Layer 2 authentication functionality, see the manual *Configuration Guide Vol. 2*.

Figure 18-11 Example of configuring tagged frame forwarding on a MAC port**Points to note**

Configure a MAC port, and configure the same port to handle tagged and untagged frames. In addition, the MAC address of a terminal is set for the MAC VLAN.

- VLAN 10: Handles tagged frames on the port VLAN.
- VLAN 50: Handles untagged frames on the MAC VLAN.

Command examples

1. `(config) # vlan 10`
`(config-vlan) # exit`

Creates VLAN 10 as a port VLAN.

2. `(config) # vlan 50 mac-based`
`(config-vlan) # mac-address 0012.e200.0004`
`(config-vlan) # exit`

Creates VLAN 50 as a MAC VLAN, and sets the MAC address (0012.e200.0004) for a terminal belonging to VLAN 50.

3. `(config) # interface gigabitethernet 0/1`
Switches to the Ethernet interface configuration mode for port 0/1.
4. `(config-if) # switchport mode mac-vlan`
Sets port 0/1 for the MAC port.
5. `(config-if) # switchport mac dot1q vlan 10`

Configures VLAN 10 as the VLAN that handles tagged frames on a MAC port.

6. `(config-if)# switchport mac vlan 50`
`(config-if)# exit`

Configures VLAN 50 as the VLAN that handles untagged frames on a MAC port.

Notes

1. When setting the `switchport mac dot1q vlan` configuration command, note the following:
 - Specifiable VLANs are port VLANs or MAC VLANs. VLANs specified in the `switchport mac vlan` or `switchport mac native vlan` configuration command cannot be specified.
 - This setting takes effect when `switchport mode mac-vlan` is set.
2. Do not connect a device that sends BPDUs to a port to which tagged frames are forwarded. (If you need to connect the device, set Spanning Tree Protocols to `Disable`.)

18.9 VLAN operation

18.9.1 List of operation commands

The following table describes the VLAN operation commands.

Table 18-13 List of operation commands

Command name	Description
<code>show vlan</code>	Shows information about VLANs.
<code>show vlan mac-vlan</code>	Shows the MAC addresses registered for MAC VLANs.

18.9.2 Checking VLAN status

(1) Checking the status of VLAN settings

VLAN information can be checked by using the `show vlan` operation 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 18-12 Results of executing show vlan

```
> show vlan

Date 2012/02/27 08:57:56 UTC
VLAN counts: 6
VLAN ID: 1      Type: Port based      Status: Up
  Learning: On      Tag-Translation:
  BPDU Forwarding:  EAPOL Forwarding:
  Router Interface Name: VLAN0001
  IP Address:
  Source MAC address: 0012.e262.1fdf(System)
  Description: VLAN0001
  Spanning Tree: None(-)
  AXRP RING ID:      AXRP VLAN group:
  IGMP snooping:      MLD snooping:
  Untagged(43) : 0/1-9, 0/13, 0/16-17, 0/20-21, 0/23, 0/25-52
  Tagged(0) :
VLAN ID: 10     Type: Port based      Status: Down
  Learning: On      Tag-Translation:
  BPDU Forwarding:  EAPOL Forwarding:
  Router Interface Name: VLAN0010
  IP Address:
  Source MAC address: 0012.e262.1fdf(System)
  Description: VLAN0010
  Spanning Tree: None(-)
  AXRP RING ID: 200  AXRP VLAN group: Control-VLAN
  IGMP snooping:      MLD snooping:
  Untagged(0) :
  Tagged(4) : 0/18-19, 0/22, 0/24
VLAN ID: 20     Type: Port based      Status: Up
  Learning: On      Tag-Translation:
  BPDU Forwarding:  EAPOL Forwarding:
  Router Interface Name: VLAN0020
  IP Address:
  Source MAC address: 0012.e262.1fdf(System)
```

```

Description: Ring-VL
Spanning Tree: PVST+(802.1D)
AXRP RING ID: 200   AXRP VLAN group: 1
AXRP Virtual-Link-VLAN
IGMP snooping:      MLD snooping:
Untagged(0)       :
Tagged(4)          : 0/18-19, 0/22, 0/24
VLAN ID: 30      Type: Protocol based   Status: Up
Protocol VLAN Information Name:
EtherType: LLC:   Snap-EtherType:
Learning: On      Tag-Translation:
BPDU Forwarding:  EAPOL Forwarding:
Router Interface Name: VLAN0030
IP Address:
Source MAC address: 0012.e262.1fdf(System)
Description: VLAN0030
Spanning Tree: None(-)
AXRP RING ID: 200   AXRP VLAN group: 2
IGMP snooping:      MLD snooping:
Untagged(2)        : 0/3, 0/13
Tagged(4)           : 0/18-19, 0/22, 0/24
VLAN ID: 51      Type: MAC based        Status: Up
Learning: On      Tag-Translation:
BPDU Forwarding:  EAPOL Forwarding:
Router Interface Name: VLAN0051
IP Address: 10.215.196.1/23
               3ffe:501:811:ff08::5/64
               fe80::212:e2ff:fe62:1fdf/64
Source MAC address: 0012.e262.1fdf(System)
Description: IPv4/IPv6
Spanning Tree: None(-)
AXRP RING ID:      AXRP VLAN group:
IGMP snooping:      MLD snooping:
Untagged(3)         : 0/6, 0/16, 0/20
Tagged(0)           :
VLAN ID: 4094     Type: Port based      Status: Up
Learning: On      Tag-Translation: On
BPDU Forwarding:  EAPOL Forwarding:
Router Interface Name: VLAN4094
IP Address:
Source MAC address: 0012.e262.1fdf(System)
Description: VLAN4094
Spanning Tree: None(-)
AXRP RING ID:      AXRP VLAN group:
IGMP snooping:      MLD snooping:
Untagged(0)        :
Tagged(5)           : 0/10-12, 0/14-15
Tag-Trans(5)        : 0/10-12, 0/14-15
>

```

(2) Checking the status of VLAN communication

The status of VLAN communication can be checked by using the `show vlan detail` operation 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 18-13 Results of executing show vlan detail

```
> show vlan 10,4094 detail
```

Date 2012/02/27 09:00:00 UTC

```

VLAN counts: 2
VLAN ID: 10    Type: Port based    Status: Down
  Learning: On      Tag-Translation:
  BPDU Forwarding:  EAPOL Forwarding:
  Router Interface Name: VLAN0010
  IP Address:
  Source MAC address: 0012.e262.1fdf(System)
  Description: VLAN0010
  Spanning Tree: None(-)
  AXRP RING ID: 200   AXRP VLAN group: Control-VLAN
  IGMP snooping:      MLD snooping:
  Port Information
    0/18(ChGr: 9)  Down -          Tagged
    0/19(ChGr: 9)  Down -          Tagged
    0/22(ChGr: 9)  Down -          Tagged
    0/24           Up   Blocking(AXRP) Tagged
VLAN ID: 4094  Type: Port based    Status: Up
  Learning: On      Tag-Translation: On
  BPDU Forwarding:  EAPOL Forwarding:
  Router Interface Name: VLAN4094
  IP Address:
  Source MAC address: 0012.e262.1fdf(System)
  Description: VLAN4094
  Spanning Tree: None(-)
  AXRP RING ID:      AXRP VLAN group:
  IGMP snooping:      MLD snooping:
  Port Information
    0/10(ChGr: 64) Up   Forwarding   Tagged   Tag-Translation: 4093
    0/11(ChGr: 64) Up   Forwarding   Tagged   Tag-Translation: 4093
    0/12(ChGr: 64) Down -   Tagged   Tag-Translation: 4093
    0/14(ChGr: 64) Up   Forwarding   Tagged   Tag-Translation: 4093
    0/15(ChGr: 64) Down -   Tagged   Tag-Translation: 4093
>

```

(3) Checking the VLAN ID list

The `show vlan summary` operation command can be used to check the set VLAN types, as well as their count and VLAN IDs.

Figure 18-14 Results of executing show vlan summary

```

> show vlan summary

Date 2012/02/27 08:59:46 UTC
Total (6)      : 1, 10, 20, 30, 51, 4094
Port based(4)  : 1, 10, 20, 4094
Protocol based(1) : 30
MAC based(1)   : 51
>

```

(4) Checking through VLAN list display

The `show vlan list` operation command provides an overview of the status of VLAN settings on one line. This command can be used to list the status 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 status of items specified for the parameter.

Figure 18-15 Results of executing show vlan list

```

> show vlan list

```



```

Date 2012/02/27 09:00:09 UTC
VLAN counts: 6
ID   Status   Fwd/Up /Cfg Name           Type  Protocol   Ext.  IP
  1 Up         3/  3/ 43 VLAN0001      Port  -          - - -
 10 Down      0/  1/  4 VLAN0010      Port  AXRP (C)   - - -
 20 Up        1/  1/  4 Ring-VL      Port  -          - - -
 30 Up        1/  1/  6 VLAN0030      Proto AXRP (-) - - -
 51 Up        1/  1/  3 IPv4/IPv6      MAC   -          - - 4/6
4094 Up       3/  3/  5 VLAN4094      Port  -          - T -
      AXRP (C: Control - VLAN)
      S: IGMP/MLD snooping T: Tag Translation
      4: IPv4 address configured 6: IPv6 address configured

```

>

(5) Checking MAC addresses registered for MAC VLANs

The `show vlan mac-vlan` operation 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`, `web-auth`, and `mac-auth` indicate a MAC address registered by the Layer 2 authentication functionality

Figure 18-16 Results of executing `show vlan mac-vlan`

```

> show vlan mac-vlan

Date 2010/08/10 06:12:04 UTC
VLAN counts: 1      Total MAC Counts: 3
VLAN ID: 100      MAC Counts: 3
    0000. e22b. ffdd(mac-auth)    000b. 972f. e22b(mac-auth)
    0050. daba. 4fc8(mac-auth)

```

>

18 VLAN

19. VLAN Extended Functionality

This chapter describes the VLAN extended functionality and its use.

19.1	Description of VLAN tunneling
19.2	Configuration of VLAN tunneling
19.3	Description of tag translation
19.4	Configuration of tag translation
19.5	Description of L2 protocol frame transparency functionality
19.6	Configuration of the L2 protocol frame transparency functionality
19.7	Description of the inter-port relay blocking functionality
19.8	Configuration of the inter-port relay blocking functionality
19.9	Operation for the VLAN extended functionality

19.1 Description of VLAN tunneling

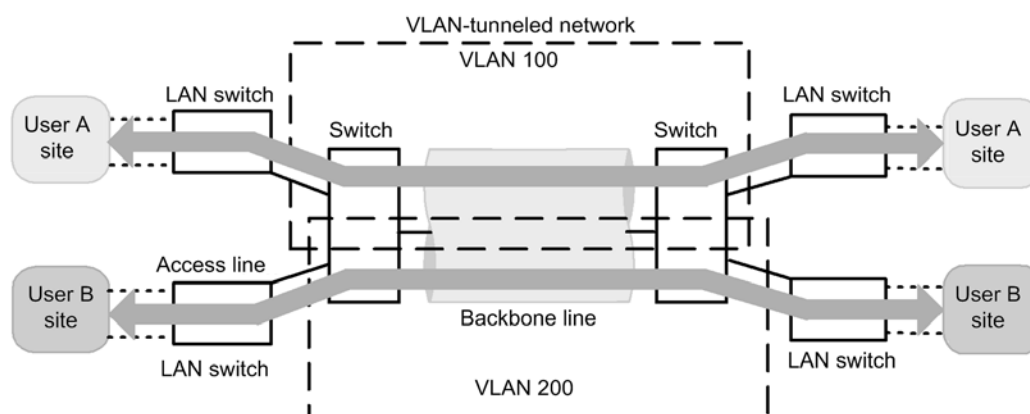
19.1.1 Overview

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 shows 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 19-1 VLAN tunneling overview (example wide-area Ethernet service application)



19.1.2 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.

19.1.3 Notes on VLAN tunneling usage

(1) Notes on use with other functionality

For details, see *16.3 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 `switchport trunk native vlan` 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 *3.4 Description of marking* in the manual *Configuration Guide Vol. 2*.

19.2 Configuration of VLAN tunneling

19.2.1 List of configuration commands

The following table describes the configuration commands for VLAN tunneling.

Table 19-1 List of configuration commands

Command name	Description
<code>switchport access</code>	Sets an access line for a tunneling port.
<code>switchport mode</code>	Sets the port type for setting an access line or backbone line.
<code>switchport trunk</code>	Sets a backbone line.
<code>mtu[#]</code>	Sets jumbo frames for a backbone line.

[#]

For details, see 9 *Ethernet* in the manual *Configuration Command Reference Vol. 2*.

19.2.2 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 0/1`

Switches to the Ethernet interface configuration mode for port 0/1.

2. `(config-if)# switchport mode dot1q-tunnel`
`(config-if)# switchport access vlan 10`
`(config-if)# exit`

Sets port 0/1 as a tunneling port. Then, sets VLAN 10.

For details about trunk port configuration, see 18.4 *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 14.2.5 *Configuring jumbo frames*.

19.3 Description of tag translation

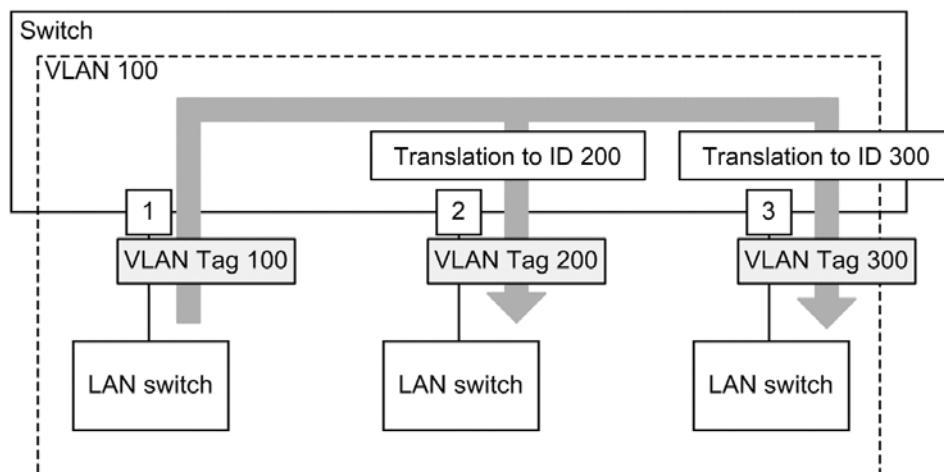
19.3.1 Overview

The tag translation functionality translates 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 set in 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 translated 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 19-2 Example configuration for tag translation



19.3.2 Notes on using tag translation

(1) Notes on use with other functionality

For details, see *16.3 Compatibility between Layer 2 switch functionality and other functionality*.

(2) VLANs that do not use tag translation

Ports that use tag translation must be configured so that all tag values used for the ports are translated. In a VLAN that does not use tag translation, ports that use tag translation must be explicitly configured to ensure that the tag values are translated to the same values.

If a frame has a tag value for which tag translation is not set, the frame is discarded when it is received. To send frames in a VLAN for which the tag translation setting is not configured, untagged frames are used. If untagged frames are not used, communication is not possible.

19.4 Configuration of tag translation

19.4.1 List of configuration commands

The following table describes the configuration commands for tag translation.

Table 19-2 List of configuration commands

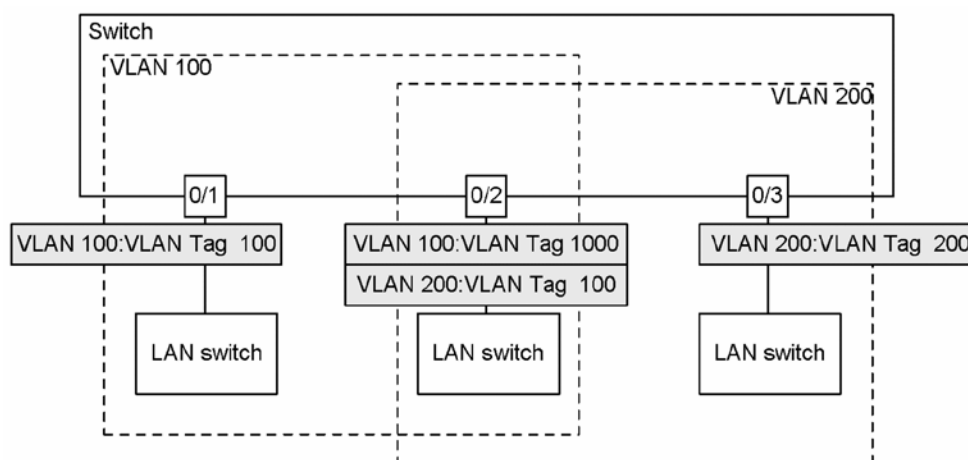
Command name	Description
<code>switchport vlan mapping</code>	Sets the ID to be translated.
<code>switchport vlan mapping enable</code>	Enables tag translation on the specified port.

19.4.2 Configuring tag translation

The figure below shows how tag translation is set. In the configuration in this example, port 0/2 is set.

In this example configuration, tag translation is applied to port 0/2. On port 0/2, VLAN 100 frames are sent and received by using VLAN tag 1000, and VLAN 200 frames are sent and received by 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 0/2, instead of being handled as VLAN 200.

Figure 19-3 Example tag translation setting



Points to note

Tag translation works by enabling the tag translation functionality, and setting the ID to be translated. Tag translation settings only take effect for trunk ports.

Tag translation is set by the `switchport vlan mapping` configuration command. Tag translation is enabled by the `switchport vlan mapping enable` configuration command. When tag translation is enabled, frames are not sent and received for VLANs for which translation is not set for the port.

Command examples

1. `(config)# interface gigabitethernet 0/2`
`(config-if)# switchport mode trunk`
`(config-if)# switchport trunk allowed vlan 100,200`
 Sets port 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 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`
`(config-if)# exit`

Enables tag translation on port 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.

19.5 Description of L2 protocol frame transparency functionality

19.5.1 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, these Layer 2 protocol frames are not forwarded.

The forwarded frames are simply handled as multicast frames on the Switch, and are not used as protocol frames by the Switch.

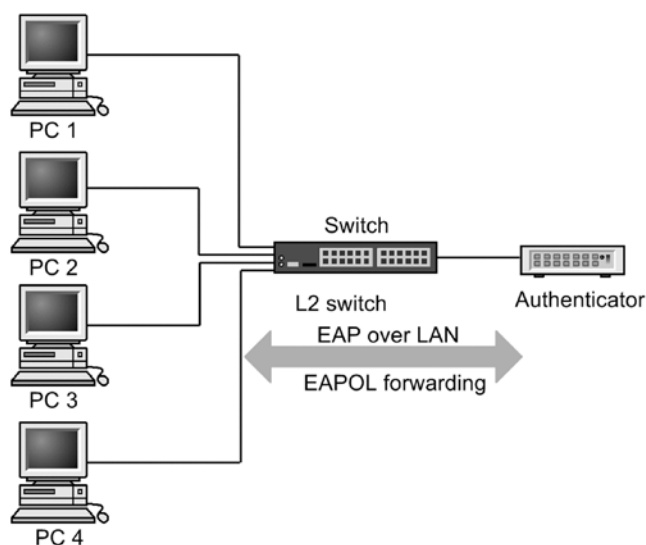
(1) BPDU forwarding functionality

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 when the Switch is used as an L2 switch between the authenticator and terminal (supplicant).

Figure 19-4 Example application of EAPOL forwarding functionality



19.5.2 Notes on L2 protocol frame transparency functionality

(1) Notes on use with other functionality

For details, see *16.3 Compatibility between Layer 2 switch functionality and other functionality*.

19.6 Configuration of the L2 protocol frame transparency functionality

19.6.1 List of configuration commands

The following table describes the configuration commands for the L2 protocol frame transparency functionality.

Table 19-3 List of configuration commands

Command name	Description
<code>l2protocol-tunnel eap</code>	Forwards EAPOL frames for IEEE 802.1X.
<code>l2protocol-tunnel stp</code>	Forwards Spanning Tree BPDUs.

19.6.2 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 Spanning Tree Protocols for the Switch.

Command examples

1. `(config)# spanning-tree disable`
`(config)# l2protocol-tunnel stp`

Sets BPDU forwarding functionality. Before setting BPDU forwarding functionality, stop the Spanning Tree Protocols. 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 EAPOLs without handling them as protocol frames.

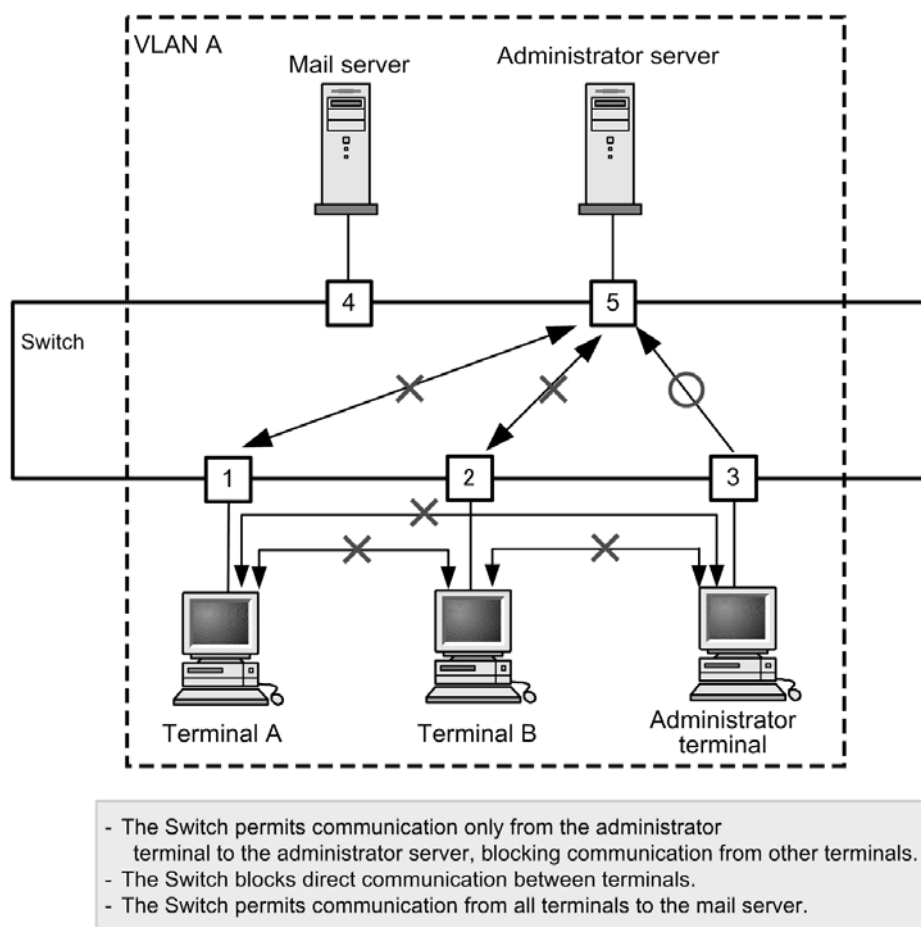
19.7 Description of the inter-port relay blocking functionality

19.7.1 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 19-5 Example application of inter-port relay blocking functionality



19.7.2 Notes on using the inter-port relay blocking functionality

(1) Notes on use with other functionality

The following table describes operation when the inter-port relay blocking functionality is used concurrently with the indicated functionality.

Table 19-4 Concurrent use of inter-port relay blocking and other functionality

functionality	Flow control operation
Spanning Tree Protocols	Depending on the topology, operating Spanning Tree Protocols on a port where communication is blocked might halt communication.
IGMP snooping	Operating IGMP snooping on a port where communication is blocked disables the inter-port relay blocking functionality for IGMP frames, preventing these frames from being forwarded.
MLD snooping	Operating MLD snooping on a port where communication is blocked disables the inter-port relay blocking functionality for MLD frames, preventing these frames from being forwarded.
DHCP snooping	Operating DHCP snooping on a port where communication is blocked disables the inter-port relay blocking functionality for DHCP frames (and ARP frames when dynamic ARP inspection is valid), preventing these frames from being forwarded.
GSRP aware	Operating GSRP on a port where communication is blocked disables the inter-port relay blocking functionality for GSRP aware frames, preventing these frames from being forwarded.
CFM	Operating CFM on a port where communication is blocked disables the inter-port relay blocking functionality for CFM frames, preventing these frames from being forwarded.

19.8 Configuration of the inter-port relay blocking functionality

19.8.1 List of configuration commands

The following table describes the configuration command for the inter-port relay blocking functionality.

Table 19-5 List of configuration commands

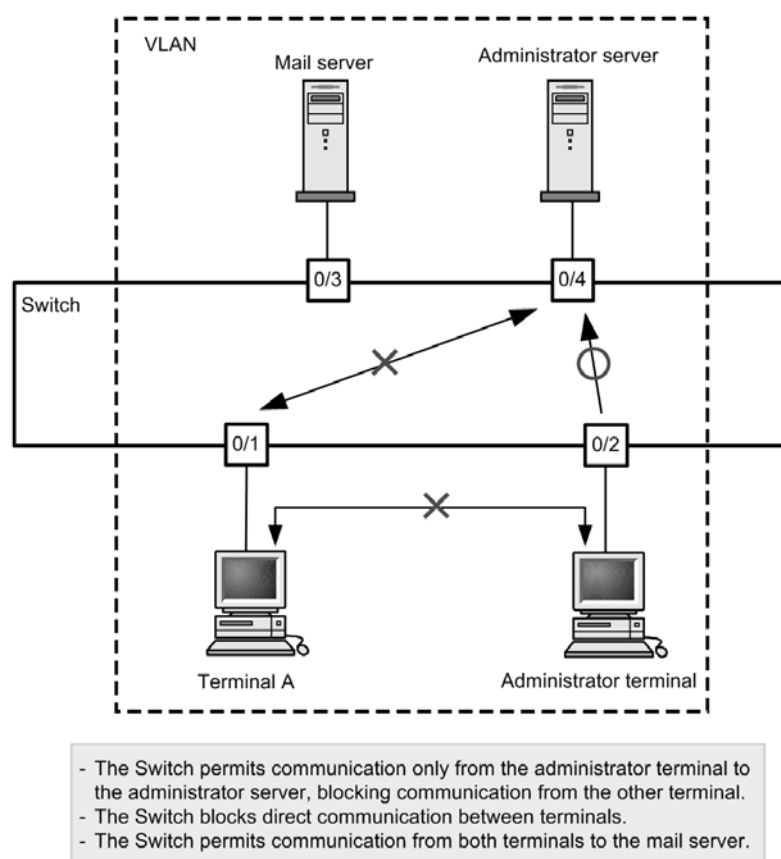
Command name	Description
<code>switchport isolation</code>	Blocks forwarding to the specified port.

19.8.2 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 0/1 to port 0/4 is blocked. Communication is also blocked between ports 0/1 and 0/2. Port 0/3 can communicate with any port.

Figure 19-6 Example settings for the inter-port relay blocking functionality



Points to note

The inter-port relay blocking functionality is set in 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 0/1`
Switches to the Ethernet interface configuration mode for port 0/1.
2. `(config-if)# switchport isolation interface gigabitethernet 0/2, gigabitethernet 0/4`
`(config-if)# exit`
Blocks forwarding from ports 0/2 and 0/4 on port 0/1. With this setting, one-way forwarding is blocked for transmission from port 0/1.
3. `(config)# interface gigabitethernet 0/2`
`(config-if)# switchport isolation interface gigabitethernet 0/1`
`(config-if)# exit`
Switches to the Ethernet interface configuration mode for port 0/2, and blocks forwarding from port 0/1 on port 0/2. With this setting, communication is blocked both ways between ports 0/1 and 0/2.
4. `(config)# interface gigabitethernet 0/4`
`(config-if)# switchport isolation interface gigabitethernet 0/1`
`(config-if)# exit`
Switches to the Ethernet interface configuration mode for port 0/4, and blocks forwarding from port 0/1 on port 0/4. With this setting, communication is blocked both ways between ports 0/1 and 0/4.

19.8.3 Changing blocked ports

Points to note

The `switchport isolation add` configuration command and the `switchport isolation remove` configuration command are used to change the ports blocked by the inter-port relay blocking functionality. When the `switchport isolation interface <interface id list>` configuration command is used to batch specify ports already set, the specified settings are replaced.

Command examples

1. `(config)# interface gigabitethernet 0/1`
`(config-if)# switchport isolation interface gigabitethernet 0/2-10`
Switches to the Ethernet interface configuration mode for port 0/1, and blocks forwarding to port 0/1 from ports 0/2 to 0/10.
2. `(config-if)# switchport isolation interface add gigabitethernet 0/11`
`(config-if)# switchport isolation interface remove gigabitethernet 0/5`
Adds port 0/11, and removes port 0/5 setting. Communication to port 0/1 from ports 0/2 to 0/4 and from ports 0/6 to 0/11 is blocked.
3. `(config-if)# switchport isolation interface gigabitethernet 0/3-4`
`(config-if)# exit`

19 VLAN Extended Functionality

Sets ports 0/3 and 0/4 as ports to be blocked. The previous configuration is completely overwritten. Only forwarding to port 0/1 from ports 0/3 and 0/4 is blocked. Communication is allowed for all other ports.

19.9 Operation for the VLAN extended functionality

19.9.1 List of operation commands

The following table describes the operation command for the VLAN extended functionality.

Table 19-6 List of operation commands

Command name	Description
<code>show vlan</code>	Checks the status of the configuration for the VLAN extended functionality.

19.9.2 Checking the 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` operation command. The following table describes how to use the `show vlan detail` operation command to check the VLAN extended functionality.

Table 19-7 Using show vlan detail to check the VLAN extended functionality

functionality	How to check
VLAN tunneling	<code>VLAN tunneling enabled</code> is displayed at the beginning of the results (This is displayed only when VLAN tunneling is enabled.)
Tag translation	<code>Tag-Translation</code> is displayed for <code>Port Information</code> .
L2 protocol frame transparency functionality	Information is displayed in the <code>BPDU Forwarding</code> and <code>EAPOL Forwarding</code> .

Figure 19-7 Results of executing show vlan detail

```
> show vlan 10, 4094 detail

Date 2011/09/06 07:37:32 UTC
VLAN counts: 2 ... 1
VLAN ID: 10   Type: Port based   Status: Down
  Learning: On      Tag-Translation:
  BPDU Forwarding:  EAPOL Forwarding: ... 3
      :
      :
Port Information
  0/10(ChGr: 64) Up   Forwarding   Tagged   Tag-Translation: 4093 ... 2
  0/11(ChGr: 64) Up   Forwarding   Tagged   Tag-Translation: 4093
  0/12(ChGr: 64) Down -   Tagged   Tag-Translation: 4093
  0/14(ChGr: 64) Up   Blocking(CH) Tagged   Tag-Translation: 4093
  0/15(ChGr: 64) Down -   Tagged   Tag-Translation: 4093
>
```

1. Because VLAN tunneling is disabled, `VLAN tunneling enabled` is not displayed.
2. Indicates that tag translation is set for this port.
3. Indicates that BPDU forwarding functionality and EAPOL forwarding functionality are not set.

20. Spanning Tree Protocols

This chapter describes the Spanning Tree functionality and its use.

20.1 Overview of Spanning Tree Protocols
20.2 Configuration of the Spanning Tree operating mode
20.3 Description of PVST+
20.4 PVST+ configuration
20.5 PVST+ operation
20.6 Description of Single Spanning Tree
20.7 Configuration of Single Spanning Tree
20.8 Operation for Single Spanning Tree
20.9 Description of Multiple Spanning Tree
20.10 Configuration of Multiple Spanning Tree
20.11 Operation for Multiple Spanning Tree
20.12 Description of common Spanning Tree functionality
20.13 Configuration of the common Spanning Tree functionality
20.14 Operation for common Spanning Tree functionality

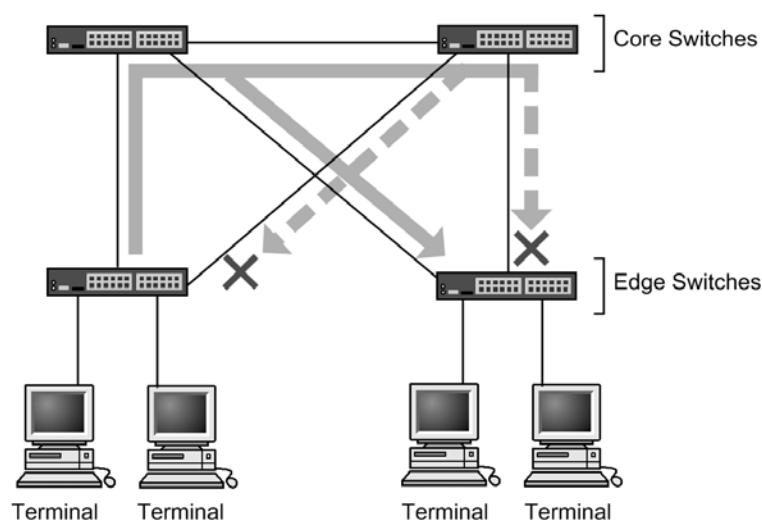
20.1 Overview of Spanning Tree Protocols

20.1.1 Overview

Spanning Tree Protocols are Layer 2 loop prevention protocols. Spanning Tree Protocols can be used to make Layer 2 networks redundant, and to prevent loops.

The following figure shows an overview of a network with a Spanning Tree Protocol applied.

Figure 20-1 Overview of a network with a Spanning Tree Protocol applied



Legend: × : Blocking status

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 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 the **Blocking** status.

20.1.2 Types of Spanning Tree Protocols

The Switches support 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 20-1 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 Switches allow the above Spanning Tree Protocols to be used as standalone or together. The following table describes which Spanning Tree combinations can be applied.

Table 20-2 Spanning Tree combinations and applicability

Tree building condition	Applicable topology calculation results
Standalone PVST+	A Spanning Tree Protocol is applied to each VLAN for which PVST+ is running. The Spanning Tree Protocol is not applied to other VLANs. PVST+ runs by default on port VLANs for the Switches.
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 is applied to each VLAN 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.

20.1.3 Spanning Tree Protocols and rapid Spanning Tree Protocol

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 the **Blocking** status (communication is not possible), switches to multiple statuses, and then puts the port in the **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 are the same as for IEEE 802.1w. The following table describes the status transitions for each protocol, and their corresponding required times.

Table 20-3 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 status transitions to Blocking as soon as the port becomes available.	--

Status	Status overview	Transition to the next status
Bl ocki ng	Status in which communication is not possible. In this status, MAC address learning is not performed. This is the status of a port put into Bl ocki ng after the topology stabilizes or just after link-up.	20 seconds (variable) or until BPDU reception
Li steni ng	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 transitions to Learni ng .	15 seconds (variable)
Learni ng	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 Forwardi ng .	15 seconds (variable)
Forwardi ng	Status in which communication is possible. In this case, the topology is stable.	--

Legend: --: Not applicable

Table 20-4 Status transitions for Rapid PVST+ and Rapid STP (Single Spanning Tree)

Status	Status overview	Transition to the next status
Di sabl e	Status in which a port cannot be used. This status transitions to Di scardi ng as soon as the port becomes available.	--
Di scardi ng	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 transitions to Learni ng .	Omitted or 15 seconds (variable)
Learni ng	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 Forwardi ng .	Omitted or 15 seconds (variable)
Forwardi ng	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 to enable high-speed topology changes.

When using rapid Spanning Tree Protocol, set it according to the conditions described below. If these conditions are not satisfied, **Di scardi ng** and **Learni ng** 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 *20.3.2 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.

20.1.4 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 20-5 Bridge role

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. This switch forwards 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 20-6 Port role

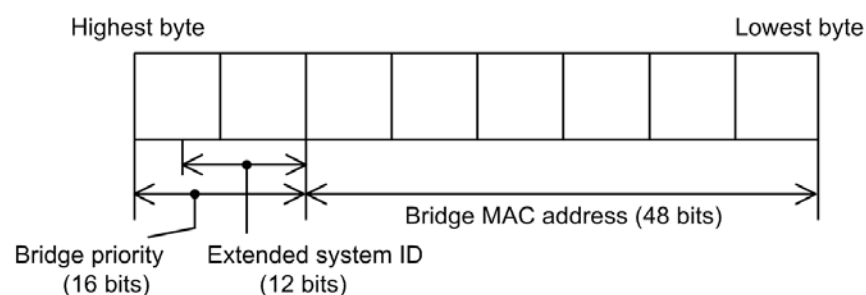
Port role	Overview
Root port	A port for a communication path from a designated bridge to the root bridge. This port allows communication.
Designated port	A port, other than the root port, for which communication is possible. It allows communication downstream from the root bridge to other ports in the 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 are 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 20-2 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 path with the lowest root path cost is used.

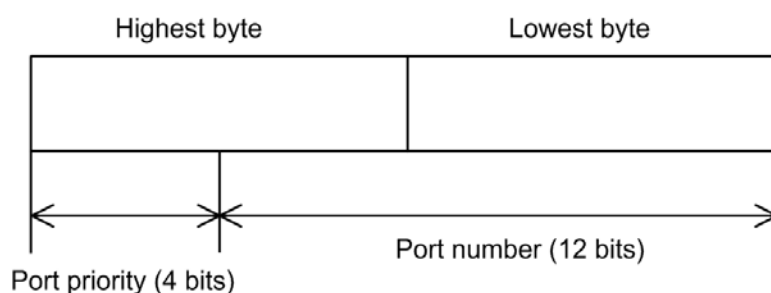
We recommend that a lower path cost be specified for a port that has a faster packet transmission speed (that is, the faster the port, the lower the specified path cost). The default value of the path cost corresponds to the speed of the port, but can also be changed in the configuration.

(5) Port ID

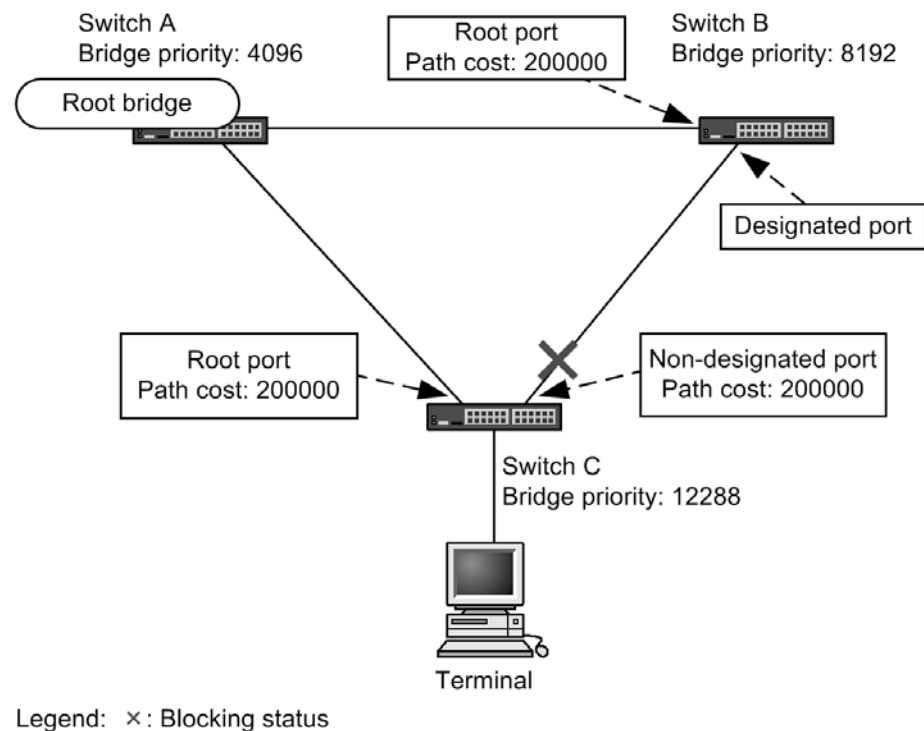
Each port in a switch is identified by a parameter called a port ID. Port IDs are used to select a communication path when two or more redundant connections exist between two switches and the path cost cannot be changed for each port. Note that when redundant connections are used between two switches, 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 20-3 Port ID

**20.1.5 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, and are placed to handle terminals as edge switches.

Figure 20-4 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 to 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 number of intermediate switches. To prioritize paths that have slow ports over paths that 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 the **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 the **Blocking** status. To change the port of Switch B to the **Blocking** status, set the path costs so that the root path cost of Switch B increases.

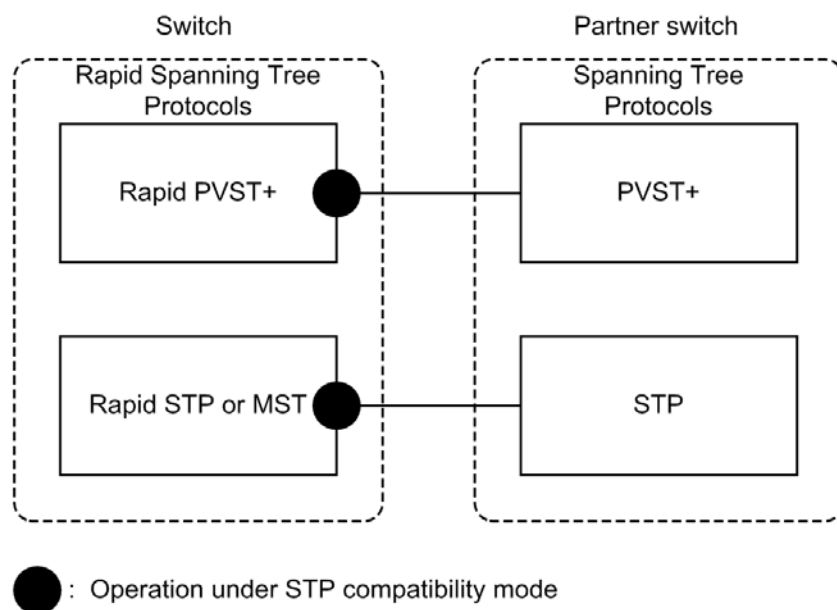
20.1.6 STP compatibility mode**(1) Overview**

If the Switch uses rapid Spanning Tree Protocols, and the partner switch uses Spanning Tree Protocols, the target port of the Switch runs in STP compatibility mode.

In STP compatibility mode operation, the target port of the Switch operates according to the partner switch. Therefore, high-speed transitions are not performed.

The following figure shows the combinations that can operate in STP compatibility mode.

Figure 20-5 Operation in STP compatibility mode



In STP compatibility mode operation, high-speed transitions can no longer be performed on the target port, requiring more time for communication to be restored.

Each Switch supports the automatic-restoration functionality and forced restoration functionality as restoration functionality for rapid Spanning Tree Protocols.

(2) Restoration functionality

(a) Automatic-restoration functionality

If the partner switch switches to rapid Spanning Tree Protocol during operation in STP compatibility mode, the automatic-restoration functionality allows the Switch to be automatically restored from STP compatibility mode and to operate as rapid Spanning Tree Protocol again.

- If the link type of the target port is point-to-point, the STP compatibility mode automatic-restoration functionality runs.
- If the target port is a non-designated port[#] running in STP compatibility mode, an RST BPDU or MST BPDU can be sent from the target port to disable STP compatibility mode.

#

For details about non-designated ports, see *Table 20-6 Port role*.

- If the link type of the target port is shared, the automatic-restoration functionality does not run, because automatic-restoration mode would not run correctly.

In addition, the target port and partner switch might continue to run in STP compatibility mode depending on the timing of restoration.

(b) Forced restoration functionality

The forced restoration functionality performs forced restoration for ports running in STP compatibility mode, allowing them to perform normal high-speed transition.

In this 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.

20.1.7 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 Switch, all VLANs temporarily go down.

20.2 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.

20.2.1 List of configuration commands

The following table describes the configuration commands for the Spanning Tree operating mode.

Table 20-7 List of configuration commands

Command name	Description
spanning-tree disable	Stops the Spanning Tree functionality.
spanning-tree mode	Sets the operating mode for the 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.

20.2.2 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.

Note that when **rapid-pvst** is specified for the operating mode, the Single Spanning Tree default is STP.

Table 20-8 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 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

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

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. Note 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.

20 Spanning Tree Protocols

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.

20.3 Description of PVST+

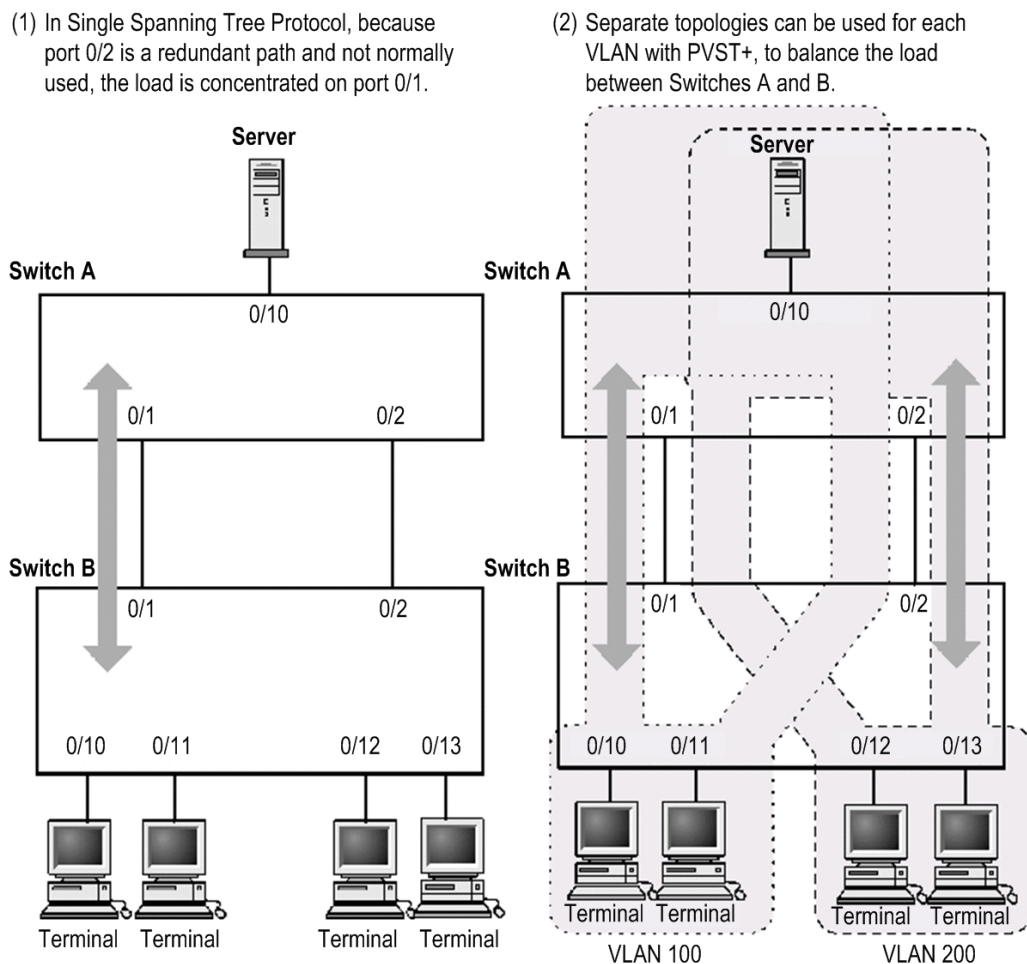
PVST+ builds a tree for each VLAN. These trees can be used for load balancing. In addition, access ports can be used to connect with switches running on Single Spanning Tree.

20.3.1 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 0/1 than port 0/2, whereas the port priority for VLAN 200 is set higher for port 0/2 than port 0/1, allowing access from each terminal to the server to be load-balanced for each VLAN.

Figure 20-6 Using PVST+ to balance load



20.3.2 PVST+ for access ports

(1) Description

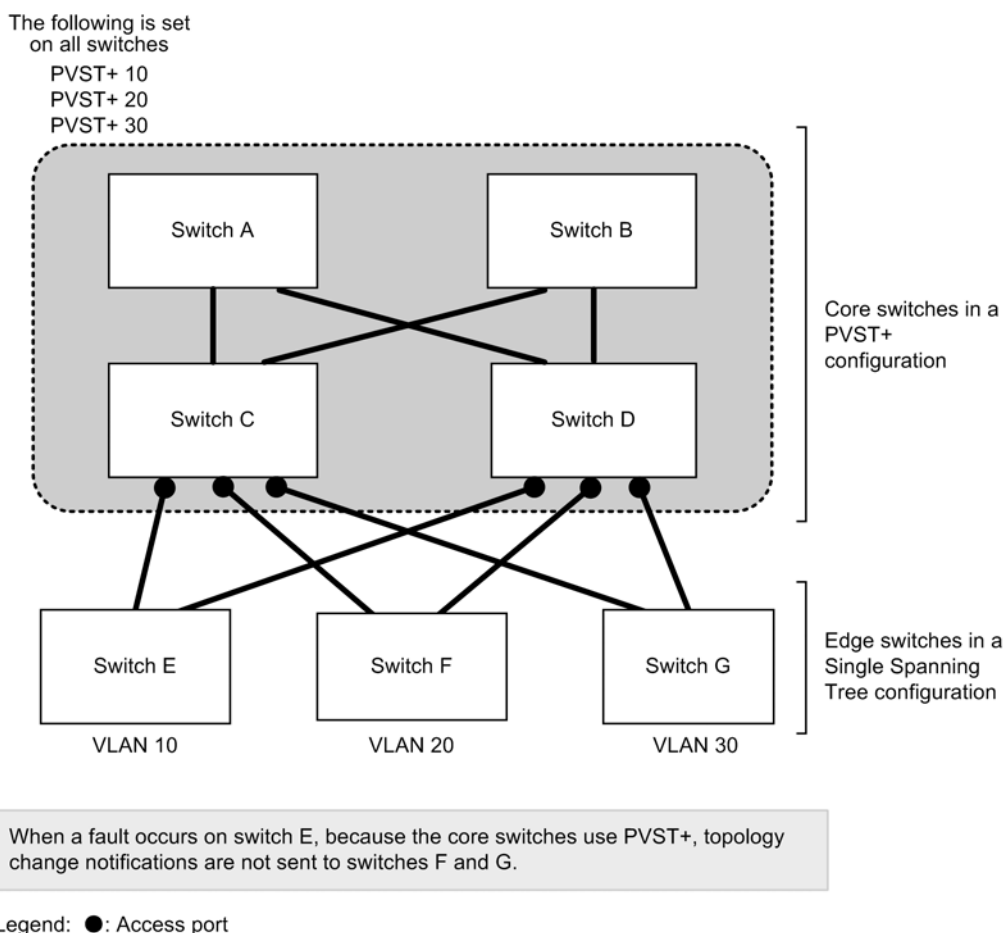
A network can be built using switches that use Single Spanning Tree and switches that support Single Spanning Tree functionality for one tree (abbreviated hereafter simply as Single Spanning Tree) and PVST+. Switches running on Single Spanning Tree are used as

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 do 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 20-7 Connecting to Single Spanning Tree



(2) When PVST+ and Single Spanning Tree are used together on access ports

When PVST+ and Single Spanning Tree are used together, 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).

20.3.3 Notes on PVST+ usage

(1) Notes on use with other functionality

For details, see *16.3 Compatibility between Layer 2 switch functionality and other functionality*.

(2) VLAN 1 (default VLAN) PVST+ and Single Spanning Tree

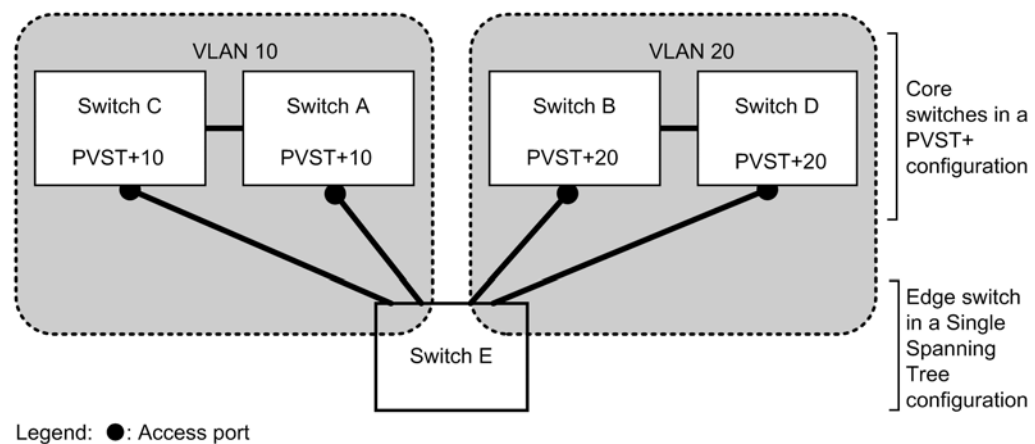
Single Spanning Tree and VLAN 1 PVST+ cannot run at the same time. When Single Spanning Tree runs, VLAN 1 PVST+ stops.

(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 20-8 Example prohibited configuration with Single Spanning Tree



Because switch E does not consist of one Spanning Tree, the topology is invalid.

20.4 PVST+ configuration

20.4.1 List of configuration commands

The following table describes the configuration commands for PVST+.

Table 20-9 List of configuration commands

Command name	Description
<code>spanning-tree cost</code>	Sets the path cost for each port.
<code>spanning-tree pathcost method</code>	Sets the margin of values used for path costs for a port.
<code>spanning-tree port-priority</code>	Sets the port priority for each port.
<code>spanning-tree vlan</code>	Sets PVST+ starting and stopping operation.
<code>spanning-tree vlan cost</code>	Sets the path cost value for a VLAN.
<code>spanning-tree vlan forward-time</code>	Sets the time required for port status transitions.
<code>spanning-tree vlan hello-time</code>	Sets the sending interval for BPDUs.
<code>spanning-tree vlan max-age</code>	Sets the maximum enabled time for sent BPDUs.
<code>spanning-tree vlan pathcost method</code>	Sets the margin of values used for path costs for a VLAN.
<code>spanning-tree vlan port-priority</code>	Sets the port priority for a VLAN.
<code>spanning-tree vlan priority</code>	Sets the bridge priority.
<code>spanning-tree vlan transmission-limit</code>	Sets the maximum number of BPDUs that can be sent per hello-time interval.

20.4.2 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` configuration command is used to stop operation.

To prevent PVST+ operation for a newly created VLAN, use the `no spanning-tree vlan` configuration command to set 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` configuration 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.

20.4.3 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. 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 20-10 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

Port speed	Default path cost value	
	short (16-bit value)	long (32-bit value)
10 Gbit/s	2	2000

Command examples

1. `(config)# interface gigabitethernet 0/1`

```
(config-if)# spanning-tree cost 100
```

```
(config-if)# exit
```

Sets the path cost of port 0/1 to 100.

2. `(config)# spanning-tree pathcost method long`

```
(config)# interface gigabitethernet 0/1
```

```
(config-if)# spanning-tree vlan 10 cost 200000
```

```
(config-if)# exit
```

Sets **long** (32-bit value) path costs to be used, and then changes port 0/1 for VLAN 10 to have a cost value of 200000. The path cost is 200000 on port 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.

(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 connected partner 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 0/1`

```
(config-if)# spanning-tree port-priority 64
```

```
(config-if)# exit
```

Sets the port priority for port 0/1 to 64.

2. `(config)# interface gigabitethernet 0/1`

```
(config-if)# spanning-tree vlan 10 port-priority 144
```

```
(config-if)# exit
```

Changes the port priority of port 0/1 for VLAN 10 to 144. For port 0/1, only VLAN 10 has a port priority of 144, with other VLANs running at 64.

20.4.4 Configuring PVST+ parameters

Each parameter must be set to satisfy the following relationship: $2 \times (\text{forward-time} - 1) \geq \text{max-age} \geq 2 \times (\text{hello-time} + 1)$. 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

If 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 Protocol 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 the value back to the default value.

(2) Setting the maximum number of BPDUs to be sent

To prevent an increase in CPU load for the 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 problem 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 the 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 VLAN 10 PVST+.

(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 PVST+ mode, it transitions from **Blocking** to **Listening**, **Learning**, and then **Forwarding**, and for 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 for a quicker transition 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: $2 \times (\text{forward-time} - 1) \geq \text{max-age} \geq 2 \times (\text{hello-time} + 1)$.

Command examples

1. `(config)# spanning-tree vlan 10 forward-time 10`

Sets the status transition time to 10 seconds for VLAN 10 PVST+.

20.5 PVST+ operation

20.5.1 List of operation commands

The following table describes the operation commands for PVST+.

Table 20-11 List of operation commands

Command name	Description
<code>show spanning-tree</code>	Shows Spanning Tree information.
<code>show spanning-tree statistics</code>	Shows Spanning Tree statistics.
<code>clear spanning-tree statistics</code>	Clears Spanning Tree statistics.
<code>clear spanning-tree detected-protocol</code>	Forces recovery of STP compatible mode for Spanning Tree Protocols.
<code>show spanning-tree port-count</code>	Shows the numbers handled by Spanning Tree Protocols.

20.5.2 Checking PVST+ statuses

PVST+ information is displayed in the execution results of the `show spanning-tree` operation command. 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 20-9 Results of executing show spanning-tree

```
> show spanning-tree vlan 4094

Date 2010/08/14 11:22:22 UTC
VLAN 4094 PVST+ Spanning Tree: Enabled Mode: PVST+
  Bridge ID      Priority: 36862    MAC Address: 00ed.f010.0001
  Bridge Status: Designated
  Root Bridge ID Priority: 36862    MAC Address: 0012.e2c4.2772
  Root Cost: 19
  Root Port: 0/20
Port Information
  0/17    Down Status: Disabled Role: -      LoopGuard
  0/18    Down Status: Disabled Role: -      LoopGuard
  0/19    Down Status: Disabled Role: -      LoopGuard
  0/20    Up    Status: Forwarding Role: Root   PortFast
  0/21    Down Status: Disabled Role: -      -
  0/22    Up    Status: Blocking Role: Alternate -
  ChGr: 8 Down Status: Disabled Role: -      RootGuard

>
```

20.6 Description of Single Spanning Tree

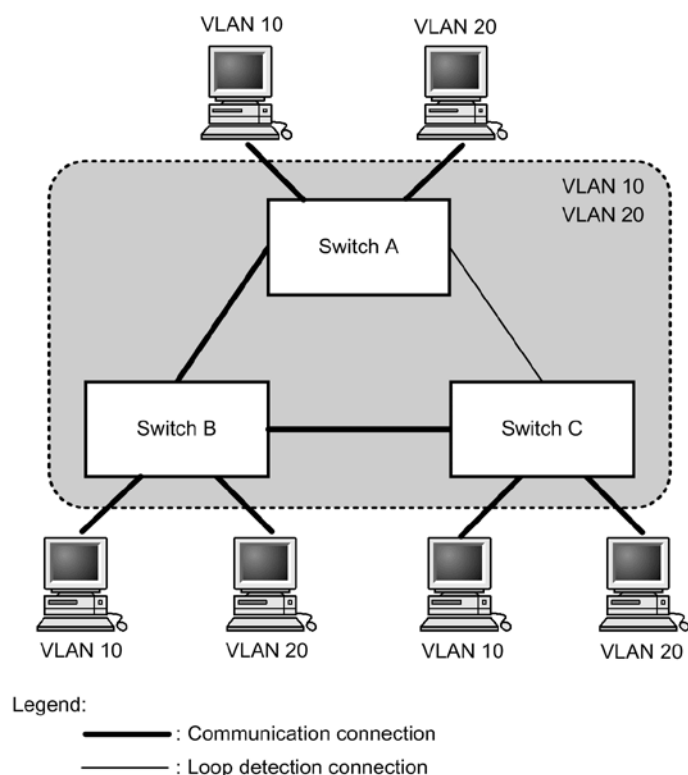
Single Spanning Tree creates topologies in which all switches are targets.

20.6.1 Overview

Single Spanning Tree 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 in order to apply Single Spanning Tree. A single topology is used for all VLANs for communication.

Figure 20-10 Network configuration based on Single Spanning Tree



20.6.2 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 the Single Spanning Tree when Single Spanning Tree is used with a PVST+.

Table 20-12 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 <code>no spanning-tree vlan</code> configuration command)
	Default VLANs (port VLANs with VLAN ID 1)
	Protocol VLANs
	MAC VLANs

20.6.3 Notes on Single Spanning Tree usage

(1) Notes on use with other functionality

For details, see *16.3 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, VLAN 1 PVST+ stops.

20.7 Configuration of Single Spanning Tree

20.7.1 List of configuration commands

The following table describes the configuration commands for Single Spanning Tree.

Table 20-13 List of configuration commands

Command name	Description
<code>spanning-tree cost</code>	Sets the path cost for each port.
<code>spanning-tree pathcost method</code>	Sets the margin of values used for the path costs for a port.
<code>spanning-tree port-priority</code>	Sets the port priority for each port.
<code>spanning-tree single</code>	Starts or stops Single Spanning Tree.
<code>spanning-tree single cost</code>	Sets the path cost value for Single Spanning Tree.
<code>spanning-tree single forward-time</code>	Sets the time required for port status transitions.
<code>spanning-tree single hello-time</code>	Sets the sending interval for BPDUs.
<code>spanning-tree single max-age</code>	Sets the maximum enabled time for sent BPDUs.
<code>spanning-tree single pathcost method</code>	Sets the margin of values used for the path costs for Single Spanning Tree.
<code>spanning-tree single port-priority</code>	Sets the port priority for Single Spanning Tree.
<code>spanning-tree single priority</code>	Sets the bridge priority.
<code>spanning-tree single transmission-limit</code>	Sets the maximum number of BPDUs that can be sent per hello-time interval.

20.7.2 Configuring Single Spanning Tree

Points to note

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, VLAN 1 PVST+ stops.

Command examples

1. `(config)# spanning-tree single`

Runs Single Spanning Tree. This setting stops VLAN 1 PVST+, making VLAN 1 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.

20.7.3 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 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.

Command examples

1. `(config)# spanning-tree single priority 4096`
Sets the bridge priority for the 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. 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 20-14 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

Command examples

1. `(config)# interface gigabitethernet 0/1`

```
(config-if)# spanning-tree cost 100
(config-if)# exit
```

Sets the path cost of port 0/1 to 100.

2.

```
(config)# spanning-tree pathcost method long
(config)# interface gigabitethernet 0/1
(config-if)# spanning-tree single cost 200000
(config-if)# exit
```

Sets **long** (32-bit value) path costs to be used, and then changes the port 0/1 for Single Spanning Tree to have a cost value of 200000. The path cost is 200000 on port 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.

(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 for making connections between two switches redundant, but use this functionality when a Spanning Tree Protocol is needed for redundancy because the connected partner 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 0/1
(config-if)# spanning-tree port-priority 64
(config-if)# exit
```

Sets the port priority for port 0/1 to 64.
2.

```
(config)# interface gigabitethernet 0/1
(config-if)# spanning-tree single port-priority 144
(config-if)# exit
```

Changes the port priority of port 0/1 for Single Spanning Tree to 144. For port 0/1, only Single Spanning Tree has a port priority of 144, with PVST+ instances using the same port running at 64.

20.7.4 Configuring Single Spanning Tree parameters

Each parameter must be set to satisfy the following relationship: $2 \times (\text{forward-time} - 1) \geq \text{max-age} \geq 2 \times (\text{hello-time} + 1)$. 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 (two 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 seconds 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: $2 \times (\text{forward-time} - 1) \geq \text{max-age} \geq 2 \times (\text{hello-time} + 1)$.

Command examples

1. `(config)# spanning-tree single forward-time 10`

Sets the status transition time to 10 seconds for Single Spanning Tree.

20.8 Operation for Single Spanning Tree

20.8.1 List of operation commands

The following table describes the operation commands for Single Spanning Tree.

Table 20-15 List of operation commands

Command name	Description
<code>show spanning-tree</code>	Shows Spanning Tree information.
<code>show spanning-tree statistics</code>	Shows Spanning Tree statistics.
<code>clear spanning-tree statistics</code>	Clears Spanning Tree statistics.
<code>clear spanning-tree detected-protocol</code>	Forces recovery of STP compatible mode for Spanning Tree Protocols.
<code>show spanning-tree port-count</code>	Shows the numbers handled by Spanning Tree Protocols.

20.8.2 Checking Single Spanning Tree statuses

Use the `show spanning-tree` operation 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 20-11 Information about Single Spanning Tree

```
> show spanning-tree single
```

```
Date 2010/08/10 11:38:40 UTC
```

```
Single Spanning Tree: Enabled Mode: STP
```

```
Bridge ID Priority: 32768 MAC Address: 00ed.f010.0001
```

```
Bridge Status: Root
```

```
Root Bridge ID Priority: 32768 MAC Address: 00ed.f010.0001
```

```
Root Cost: 0
```

```
Root Port: -
```

```
Port Information
```

```
0/1 Up Status: Learning Role: Designated RootGuard
0/2 Down Status: Disabled Role: - RootGuard
0/3 Down Status: Disabled Role: - -
0/4 Down Status: Disabled Role: - -
0/5 Down Status: Disabled Role: - -
0/6 Down Status: Disabled Role: - -
0/7 Down Status: Disabled Role: - RootGuard
0/8 Down Status: Disabled Role: - RootGuard
0/11 Down Status: Disabled Role: - LoopGuard
0/12 Up Status: Blocking Role: Alternate LoopGuard
0/14 Down Status: Disabled Role: - PortFast
0/16 Down Status: Disabled Role: - PortFast
0/17 Down Status: Disabled Role: - LoopGuard
0/18 Down Status: Disabled Role: - LoopGuard
0/19 Down Status: Disabled Role: - LoopGuard
0/20 Up Status: Forwarding Role: Designated PortFast
```

```
:
:
```

```
>
```

20.9 Description of Multiple Spanning Tree

20.9.1 Overview

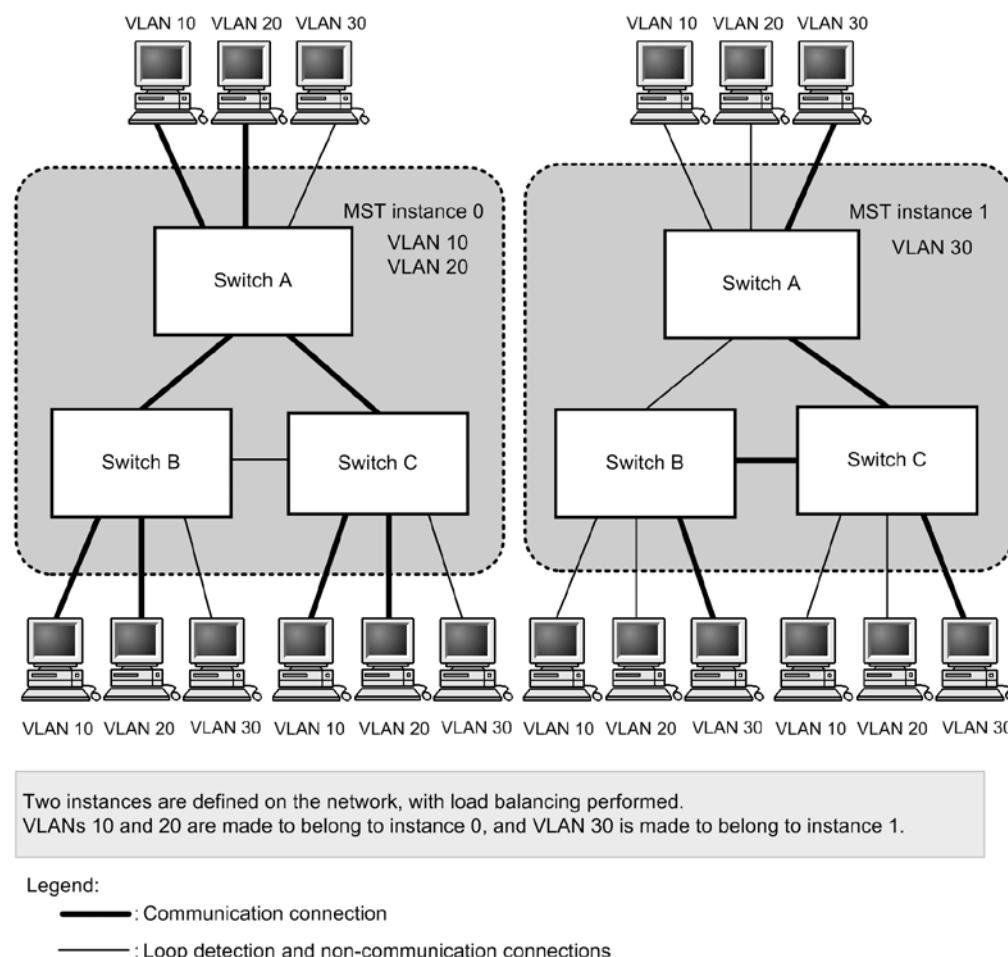
The following explains the features of Multiple Spanning Tree. MST instances can be used to perform load balancing. MST regions can be used to divide large network configurations into smaller configurations, to simplify network design. The following gives a functional overview of how Multiple Spanning 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 20-12 Example MST instance setup



(2) MST regions

Multiple Spanning Tree allows multiple switches to be grouped and handled as an MST region. To assign switches to the same MST region, settings for region name, revision number, and MST instance IDs, and mapping VLANs to MST instance IDs need to be matched between the switches. 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

A 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.

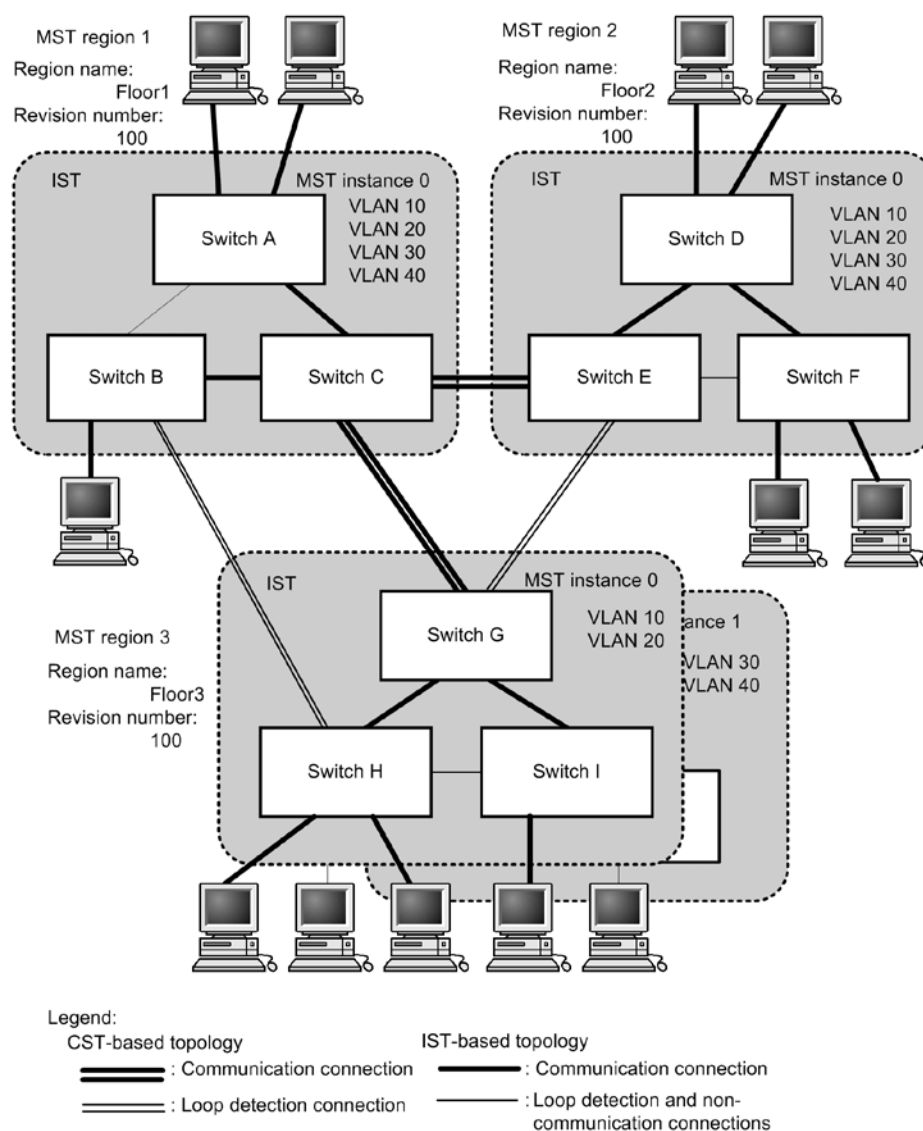
- IST

An 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

A Common and Internal Spanning Tree (CIST) refers to a topology that combines ISTs and CSTs.

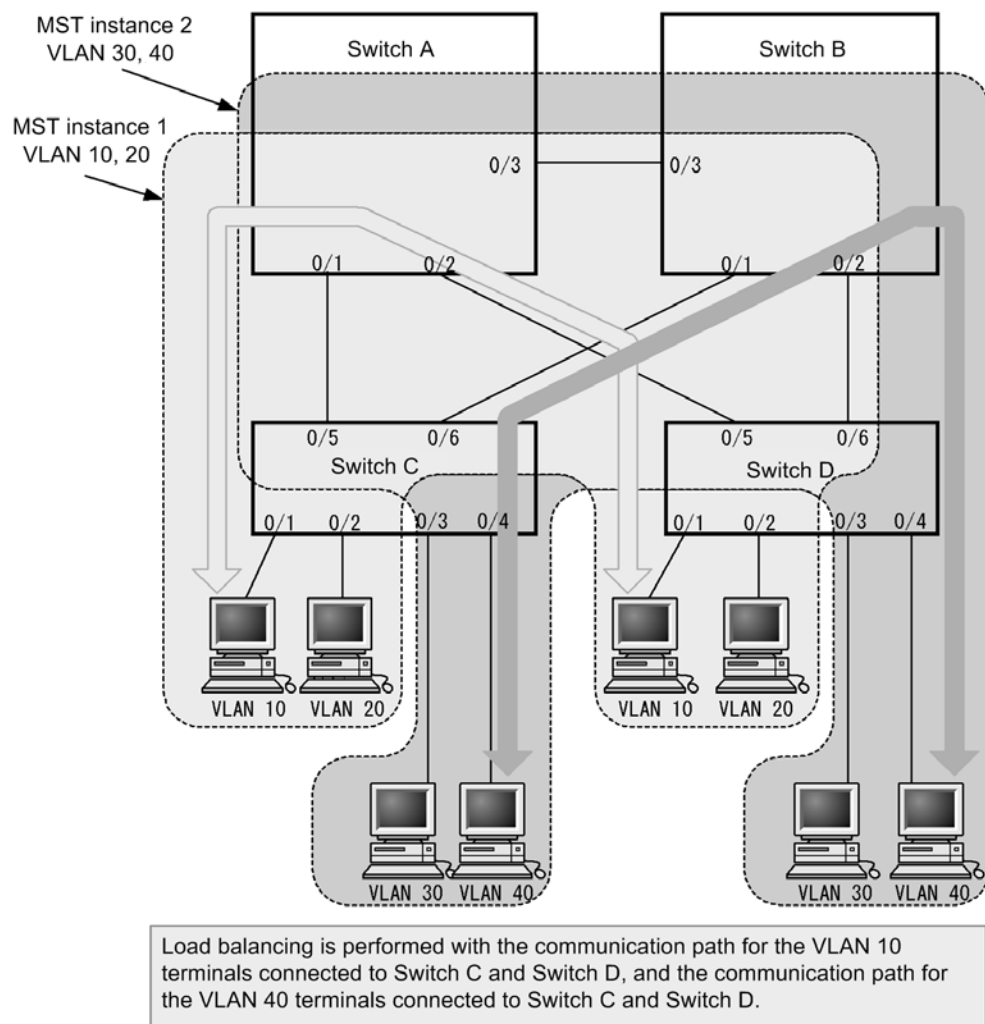
The following figure shows an overview of Multiple Spanning Tree.

Figure 20-13 Overview of Multiple Spanning Tree

20.9.2 Designing networks for Multiple Spanning Tree

(1) Configuring load balancing for each MST instance

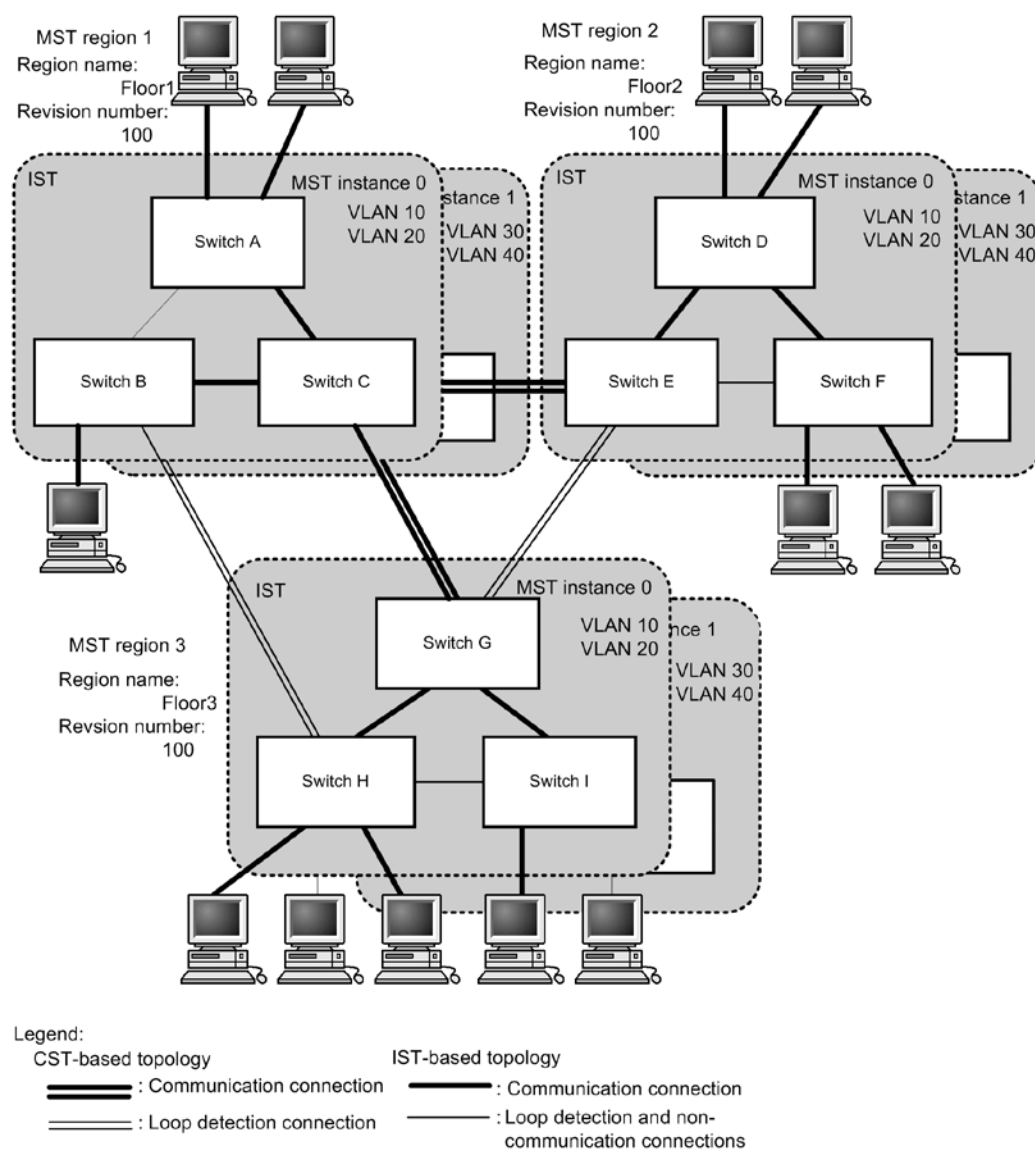
Multiple Spanning Tree allows load balancing to be performed for each MST instance. The figure below shows an example configuration for load balancing. In this example, VLANs 10 and 20 are set for MST instance 1, and VLANs 30 and 40 are set for MST instance 2, for load balancing in two parts. As shown in this example, Multiple Spanning Tree can enable load balancing by managing four VLANs with just two trees.

Figure 20-14 Load balancing configuration for Multiple Spanning Tree

(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 20-15 Network configuration by MST region

20.9.3 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.

20.9.4 Notes on Multiple Spanning Tree usage

(1) Notes on use with other functionality

For details, see *16.3 Compatibility between Layer 2 switch functionality and other functionality*.

(2) MST regions

The range of VLANs that can be handled by other switches might differ from that of the Switches. 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 20-16 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 subsequent instances	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 subsequent instances	Corresponding MST instance
Other cases	When the Switch stops	CIST root bridge	CIST
		Root bridge on MST instance 0 (IST)	CIST
		Root bridge on MST instance 1 and subsequent instances	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 subsequent instances	Corresponding MST instance

20.10 Configuration of Multiple Spanning Tree

20.10.1 List of configuration commands

The following table describes the configuration commands for Multiple Spanning Tree.

Table 20-17 List of configuration commands

Command name	Description
<code>i n s t a n c e</code>	Sets the VLANs that will participate in an MST instance of Multiple Spanning Tree.
<code>n a m e</code>	Sets a string that identifies the region of Multiple Spanning Tree.
<code>r e v i s i o n</code>	Sets a revision number for identifying a region of Multiple Spanning Tree.
<code>s p a n n i n g - t r e e c o s t</code>	Sets the path cost for each port.
<code>s p a n n i n g - t r e e m o d e</code>	Sets the operating mode for the Spanning Tree functionality.
<code>s p a n n i n g - t r e e m s t c o n f i g u r a t i o n</code>	Sets the information required to form MST regions in Multiple Spanning Tree.
<code>s p a n n i n g - t r e e m s t c o s t</code>	Sets the path cost for each MST instance for Multiple Spanning Tree.
<code>s p a n n i n g - t r e e m s t f o r w a r d - t i m e</code>	Sets the time required for port status transitions.
<code>s p a n n i n g - t r e e m s t h e l l o - t i m e</code>	Sets the sending interval for BPDUs.
<code>s p a n n i n g - t r e e m s t m a x - a g e</code>	Sets the maximum enabled time for sent BPDUs.
<code>s p a n n i n g - t r e e m s t m a x - h o p s</code>	Sets the maximum number of hops within an MST region.
<code>s p a n n i n g - t r e e m s t p o r t - p r i o r i t y</code>	Sets the port priority for each MST instance in Multiple Spanning Tree.
<code>s p a n n i n g - t r e e m s t r o o t p r i o r i t y</code>	Sets the bridge priority for each MST instance.
<code>s p a n n i n g - t r e e m s t t r a n s m i s s i o n - l i m i t</code>	Sets the maximum number of BPDUs that can be sent per hello-time interval.
<code>s p a n n i n g - t r e e p o r t - p r i o r i t y</code>	Sets the port priority for a port.

20.10.2 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` configuration 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
```

```
(config-mst)# exit
```

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).

20.10.3 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 20-18 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

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 0/1`
`(config-if)# spanning-tree cost 2000`

Sets MST instances 10, 20, and 30, and sets the path cost of port 0/1 to 2000. This means the path cost of port 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`
`(config-if)# exit`

Changes the path cost of port 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.

(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 for making connections between two switches redundant, but use this functionality when a Spanning Tree Protocol is needed for redundancy because the connected partner 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 0/1
(config-if)# spanning-tree port-priority 64
(config-if)# exit
```

Sets the port priority for port 0/1 to 64.

2.

```
(config)# interface gigabitethernet 0/1
(config-if)# spanning-tree mst 20 port-priority 144
(config-if)# exit
```

Sets the port priority of port 0/1 for instance 20 to 144. For port 0/1, only instance 20 has a port priority of 144, with other instances running at 64.

20.10.4 Configuring Multiple Spanning Tree parameters

Each parameter must be set to satisfy the following relationship: $2 \times (\text{forward-time} - 1) \geq \text{max-age} \geq 2 \times (\text{hello-time} + 1)$. 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 the value 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 hops 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 seconds.

(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: $2 \times (\text{forward-time} - 1) \geq \text{max-age} \geq 2 \times (\text{hello-time} + 1)$.

Command examples

1. **(config) # spanning-tree mst forward-time 10**

Sets the status transition time for BPDUs in Multiple Spanning Tree to 10 seconds.

20.11 Operation for Multiple Spanning Tree

20.11.1 List of operation commands

The following table describes the operation commands for Multiple Spanning Tree.

Table 20-19 List of operation commands

Command name	Description
<code>show spanning-tree</code>	Shows Spanning Tree information.
<code>show spanning-tree statistics</code>	Shows Spanning Tree statistics.
<code>clear spanning-tree statistics</code>	Clears Spanning Tree statistics.
<code>clear spanning-tree detected-protocol</code>	Forces recovery of STP compatible mode for Spanning Tree Protocols.
<code>show spanning-tree port-count</code>	Shows the numbers handled by Spanning Tree Protocols.

20.11.2 Checking Multiple Spanning Tree statuses

Use the `show spanning-tree` operation 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 results of executing `show spanning-tree`.

Figure 20-16 Results of executing show spanning-tree

```
> show spanning-tree mst instance 4095

Date 2010/08/14 13:04:05 UTC
Multiple Spanning Tree: Enabled
Revision Level: 0      Configuration Name:
MST Instance 4095
VLAN Mapped: 4094
Regional Root Priority: 36863      MAC      : 00ed.f010.0001
Internal Root Cost      : 0        Root Port: -
Bridge ID      Priority: 36863      MAC      : 00ed.f010.0001
Regional Bridge Status : Root
Port Information
0/17      Down Status: Disabled Role: -      -
0/18      Down Status: Disabled Role: -      -
0/19      Down Status: Disabled Role: -      -
0/20      Up   Status: Forwarding Role: Designated PortFast
0/21      Down Status: Disabled Role: -      -
0/22      Up   Status: Forwarding Role: Designated -
ChGr: 8    Down Status: Disabled Role: -      RootGuard

>
```

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.

20.12 Description of common Spanning Tree functionality

20.12.1 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.

The PortFast functionality runs depending on the PortFast settings and the type of port. The following table describes the operating conditions for the PortFast functionality.

Table 20-20 Operating conditions for the PortFast functionality

Configuration definition		Port type	
Settings on a port (spanning-tree portfast)	Settings on a switch (spanning-tree portfast default)	Access port Protocol port MAC port	Trunk port
PortFast is set (trunk)	(The settings on the port have priority)	Y	Y
PortFast is disabled (disable)		N	N
Parameters are omitted		Y	N
The command is not set	The command is set	Y	N
	The command is not set	N	N

Legend

Y: Supported, N: Not supported

(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` operation command, to link up again with PortFast ports with the BPDU guard functionality applied, and resume communication.

20.12.2 BPDU filter

(1) Overview

On ports with the BPDU filter functionality applied, BPDU sending and reception is stopped. The BPDU filter functionality is applied to those 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.

20.12.3 Loop guards

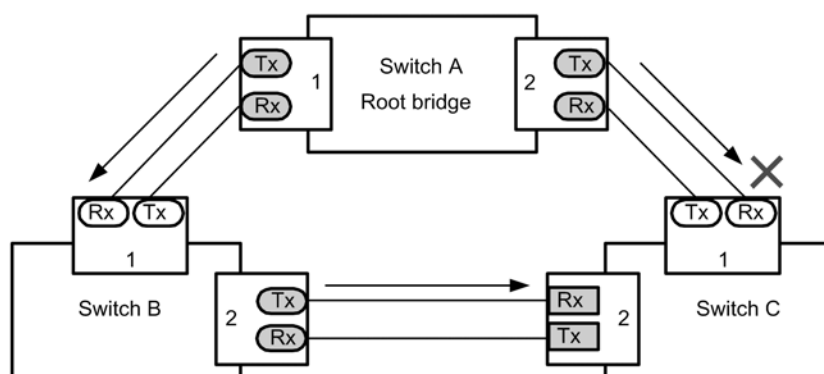
(1) Overview

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.

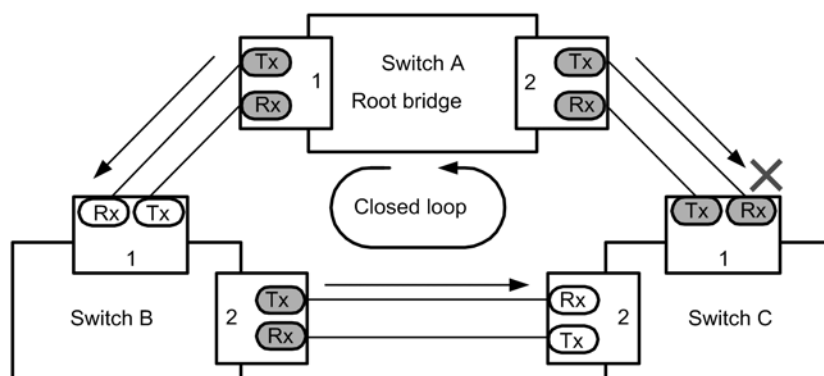
The following figure shows the problems that occur during unidirectional link faults.

Figure 20-17 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.

The loop guard functionality does not run on ports on which the root guard functionality is set, or when the PortFast functionality is set on a switch or port.

The following table summarizes the loop guard operating conditions.

Table 20-21 Loop guard operating conditions

PortFast functionality	Configuration definition		Loop guard operation
	Settings on a port (spanning-tree guard)	Settings on a switch (spanning-tree loopguard default)	
Enabled	Loop guard is set (loop)	(The settings on the port have priority)	N
	Guard is disabled (none)		N

PortFast functionality	Configuration definition		Loop guard operation
	Settings on a port (spanning-tree guard)	Settings on a switch (spanning-tree loopguard default)	
	Root guard is set (root)		N
	The command is not set	The command is set	N
		The command is not set	N
Disabled	Loop guard is set (loop)	(The settings on the port have priority)	Y
	Guard is disabled (none)		N
	Root guard is set (root)		N
	The command is not set	The command is set	Y
		The command is not set	N

Legend

Y: Supported, N: Not supported

(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.

- A switch starts
- A port goes up (including due to link aggregation)
- 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 changes so that the partner port becomes a designated port, in which case a BPDU timeout is detected on the partner port, and the loop guard operates. 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.

20.12.4 Root guards

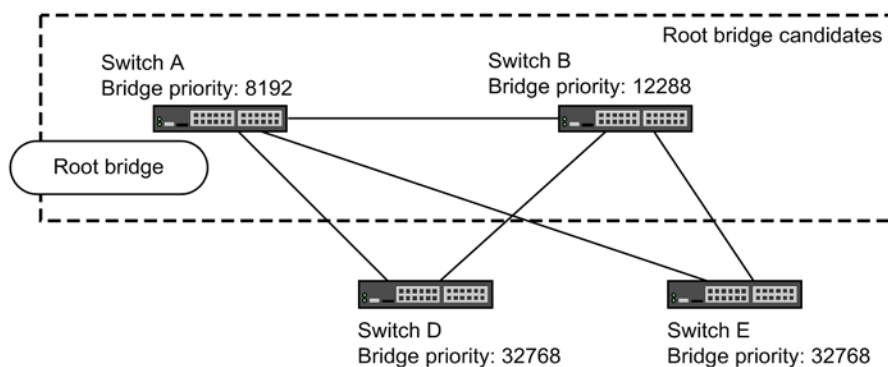
(1) Overview

Unintended topologies might occur if a switch is accidentally connected or a setting is changed somewhere 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.

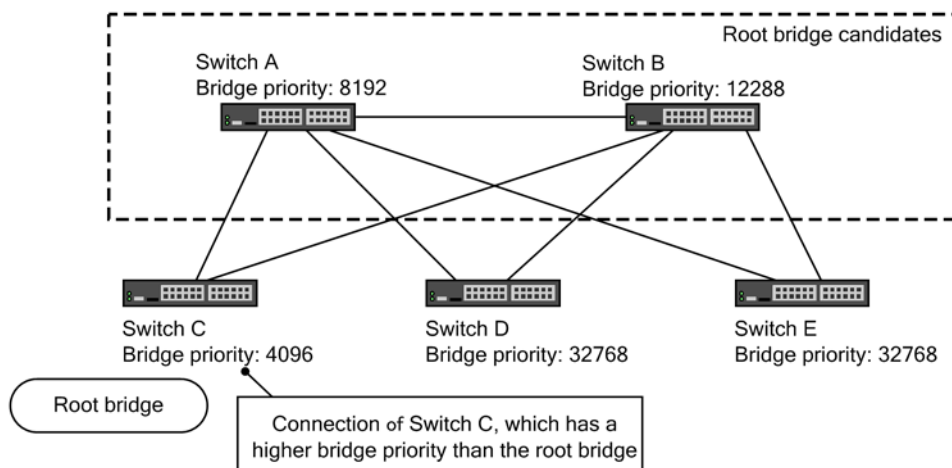
- Operation in which Switch A and Switch B run as root bridge candidates

Figure 20-18 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 20-19 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.

The following table describes the root guard operating conditions.

Table 20-22 Root guard operating conditions

Configuration definition		Root guard operation
Settings on a port (spanning-tree guard)	Settings on a switch (spanning-tree loopguard default)	
Loop guard is set (loop)	(The settings on the port have priority)	N
Guard is disabled (none)		N
Root guard is set (root)		Y
The command is not set	The command is set	N
	The command is not set	N

Legend

Y: Supported, N: Not supported

20.13 Configuration of the common Spanning Tree functionality

20.13.1 List of configuration commands

The following table describes the configuration commands for common Spanning Tree functionality.

Table 20-23 List of configuration commands

Command name	Description
<code>spanning-tree bpdupfilter</code>	Sets BPDU filter functionality for each port.
<code>spanning-tree guard</code>	Sets loop guard functionality and root guard functionality for each port.
<code>spanning-tree link-type</code>	Sets link types for ports.
<code>spanning-tree loopguard default</code>	Sets loop guard functionality to be used by default.
<code>spanning-tree portfast</code>	Sets PortFast functionality for each port.
<code>spanning-tree bpduguard</code>	Sets BPDU guard functionality for each port.
<code>spanning-tree portfast bpduguard default</code>	Sets BPDU guard functionality to be used by default.
<code>spanning-tree portfast default</code>	Sets PortFast functionality to be used by default.

20.13.2 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` configuration 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` configuration 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 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 0/1 (access port).

3. `(config)# interface gigabitethernet 0/3`
`(config-if)# switchport mode trunk`
`(config-if)# spanning-tree portfast trunk`
`(config-if)# exit`

Specifies port 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` configuration 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` configuration 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 0/1`
`(config-if)# spanning-tree bpduguard disable`
`(config-if)# exit`

Sets BPDU guard functionality to not be used on port 0/1 (access port). Normal PortFast functionality is applied to port 0/1.

3. `(config)# interface gigabitethernet 0/2`
`(config-if)# switchport mode trunk`
`(config-if)# spanning-tree portfast trunk`
`(config-if)# exit`

Sets PortFast functionality for port 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` configuration command.

20.13.3 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 0/1
(config-if)# spanning-tree bpdupfilter enable
(config-if)# exit
```

Sets the BPDU filter functionality for port 0/1.

20.13.4 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 t` 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 t
```

Sets that loop guard functionality is to be applied for all ports other than those with PortFast set.

2.

```
(config)# interface gigabitethernet 0/1
(config-if)# spanning-tree guard none
(config-if)# exit
```

Sets loop guards to be disabled on port 0/1 when loop guards are set to be applied by default.

3.

```
(config)# no spanning-tree loopguard default t
(config)# interface gigabitethernet 0/2
(config-if)# spanning-tree guard loop
(config-if)# exit
```

Deletes settings to apply loop guards by default, and applies loop guards by setting for each port, for port 0/2.

20.13.5 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 0/1
(config-if)# spanning-tree guard root
(config-if)# exit
```

Sets root guard functionality for port 0/1.

20.13.6 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 type, 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 0/1
(config-if)# spanning-tree link-type point-to-point
(config-if)# exit
```

Runs port 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 exist.

20.14 Operation for common Spanning Tree functionality

20.14.1 List of operation commands

The following table describes the operation command for common Spanning Tree functionality.

Table 20-24 List of operation commands

Command name	Description
<code>show spanning-tree</code>	Shows Spanning Tree information.

20.14.2 Checking the status of common Spanning Tree functionality

Use the `show spanning-tree detail` operation command to check information about Spanning Tree Protocols. The figure below shows an example for VLAN 4094 PVST+.

- The PortFast item can be checked to make sure that PortFast is set for port 0/20.
- The Loop Guard item can be checked to make sure that a loop guard is set for port 0/17.
- Root guards can be checked with the RootGuard item, and BPDU filters can be checked with the BPDUFilter item. (In this example, both items are displayed as OFF, meaning that neither functionality has been set.)
- The Link Type item for each port can be used to check the link type. (Because this example is for PVST+, - is displayed for the Link Type item.)

Figure 20-20 Spanning Tree information

```
> show spanning-tree vlan 4094 detail

Date 2010/08/14 11:26:46 UTC
VLAN 4094 PVST+ Spanning Tree: Enabled Mode: PVST+
Bridge ID
  Priority: 36862                      MAC Address: 00ed.f010.0001
  Bridge Status: Designated          Path Cost Method: Short
  Max Age: 20                        Hello Time: 2
  Forward Delay: 15
Root Bridge ID
  Priority: 36862                      MAC Address: 0012.e2c4.2772
  Root Cost: 19
  Root Port: 0/20
  Max Age: 20                        Hello Time: 2
  Forward Delay: 15
Port Information
Port: 0/17 Down
  Status: Disabled                    Role: -
  Priority: 128                       Cost: -
  Link Type: -                        Compatible Mode: -
  Loop Guard: ON(Blocking)            PortFast: OFF
  BPDUFilter: OFF                     RootGuard: OFF
Port: 0/20 Up
  Status: Forwarding                  Role: Root
  Priority: 128                       Cost: 19
  Link Type: -                        Compatible Mode: -
  Loop Guard: OFF                     PortFast: ON(BPDU received)
  BPDUFilter: OFF                     RootGuard: OFF
BPDU Parameters(2010/08/14 11:26:47):
  Designated Root
```


Priority: 36862	MAC address: 0012. e2c4. 2772
Designated Bridge	
Priority: 36862	MAC address: 0012. e2c4. 2772
Root Cost: 0	
Port ID	
Priority: 128	Number: 20
Message Age Timer: 2(0) /20	

>

21 . 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.

21.1	Overview of the Ring Protocol
21.2	Basic Ring Protocol principles
21.3	Overview of single ring operation
21.4	Overview of multi-ring operation
21.5	Multi-fault monitoring functionality for the Ring Protocol
21.6	Ring Protocol network design
21.7	Notes on Ring Protocol

21.1 Overview of the Ring Protocol

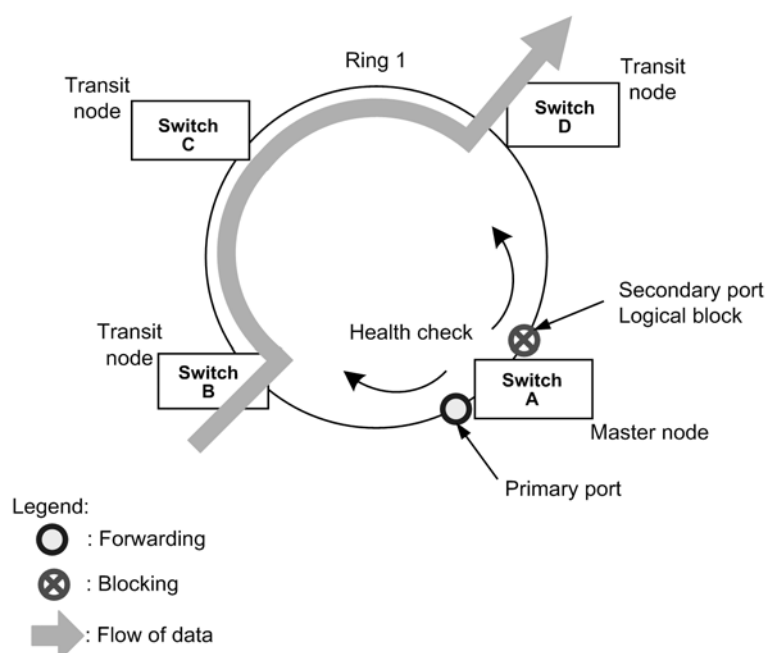
21.1.1 Overview

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 a ring topology, the need for transmission paths and interfaces is reduced when compared to a mesh topology.

The following figure shows an overview of a ring network based on the Ring Protocol.

Figure 21-1 Overview of the Ring Protocol



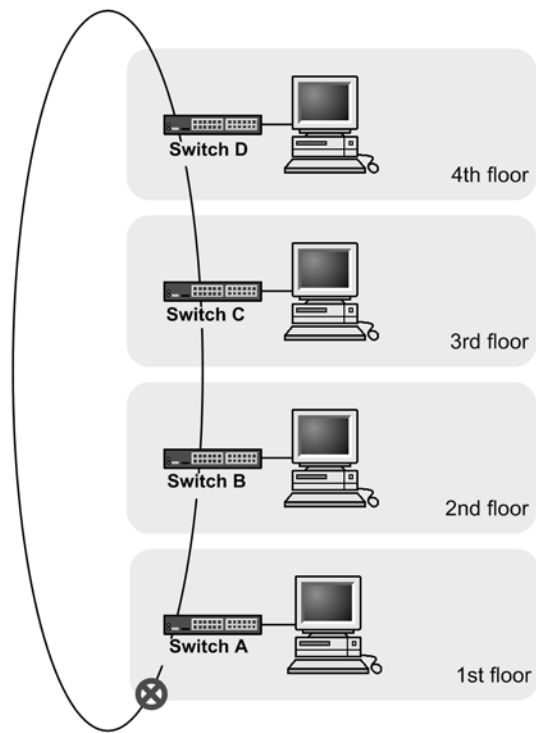
Of the nodes constituting a ring, one is the master node and the others are transit nodes. The two ports connecting each node are called ring ports, and the ring ports of the master node include a primary port and a secondary port. The master node can divide a ring configuration by applying a logical 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.

21.1.2 Features

(1) Ethernet-based ring networks

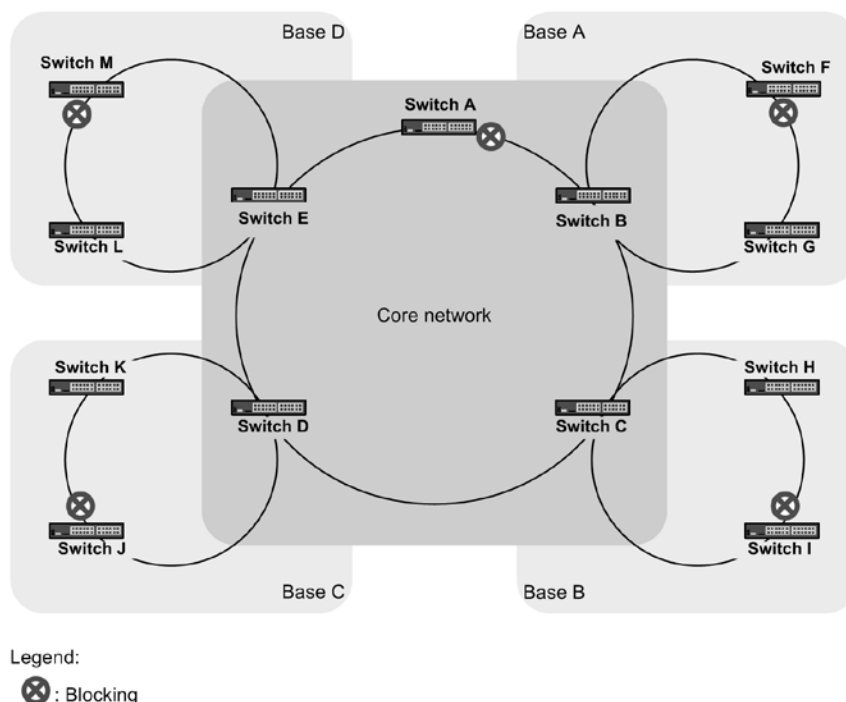
The Ring Protocol is an Ethernet-based network redundancy protocol. Whereas conventional ring networks typically use dual-link fiber optics such as FDDI, the Ring Protocol can be used to build ring networks using Ethernet.

The following figure shows an example Ring Protocol application.

Figure 21-2 Example Ring Protocol application (part 1)

Legend:

⊗ : Blocking

Figure 21-3 Example Ring Protocol application (part 2)**(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 are 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 for prompting 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.

21.1.3 Supported specifications

The following table describes the items and specifications supported by the Ring Protocol.

Table 21-1 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)
Node	Master nodes	Y
	Transit nodes	Y
	Shared nodes	Y
Maximum number of ring IDs per switch		51 If the Ring Protocol is used with Spanning Tree Protocols or if the multi-fault monitoring functionality is used, this value is 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
	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 50 ms increments
Fault monitoring time		500 to 300000 ms, in 50 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 50 ms increments
	Multi-fault monitoring time	1000 to 300000 ms, in 50 ms increments

Legend: Y: Supported; N: Not supported

21.2 Basic Ring Protocol principles

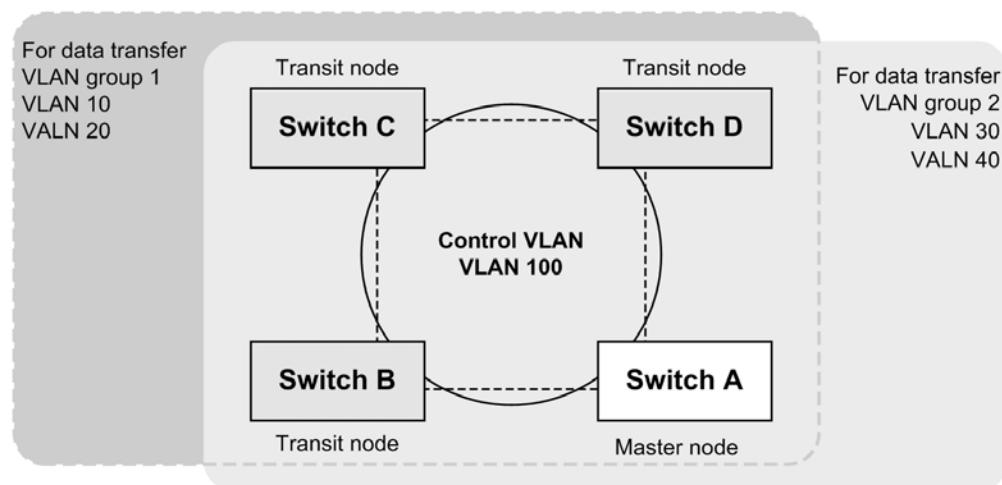
21.2.1 Network configuration

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.

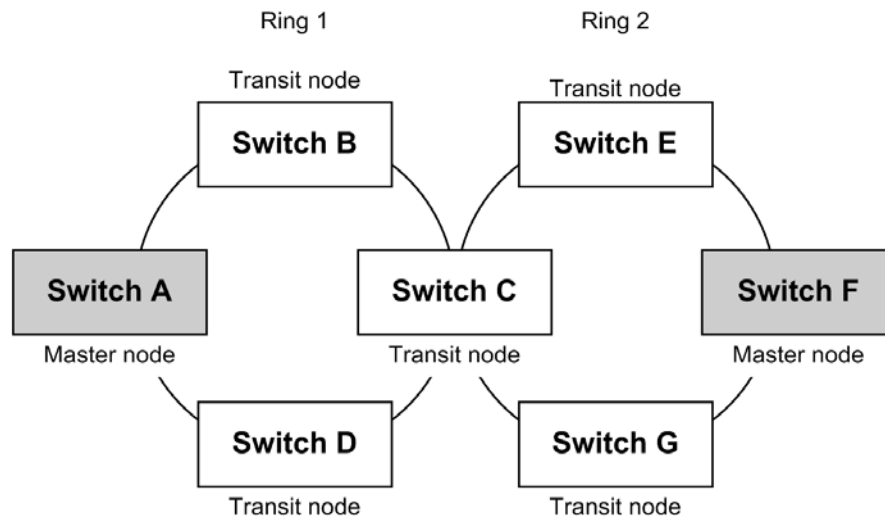
Figure 21-4 Single ring configuration



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

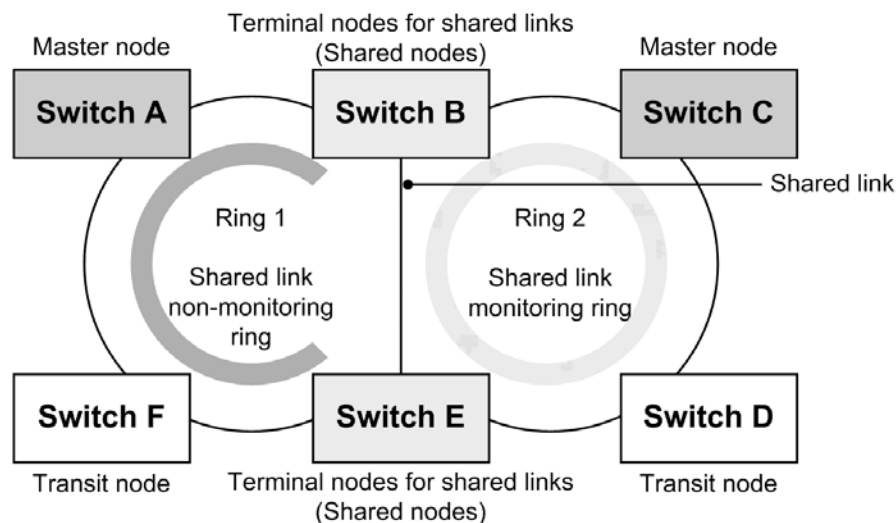
Of the possible multi-ring configurations, the following figure shows one in which a single node is the contact point for the neighboring ring.

Figure 21-5 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 21-6 Multi-ring configurations with shared links

Legend: : Monitoring path for ring 1 : Monitoring path for ring 2

When multiple single rings are connected by multiple nodes, links are shared by multiple rings. These links are called shared links, and a 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, this is called a multi-ring configuration without shared links because no shared links exist.

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.

21.2.2 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.

21.2.3 Fault monitoring methods

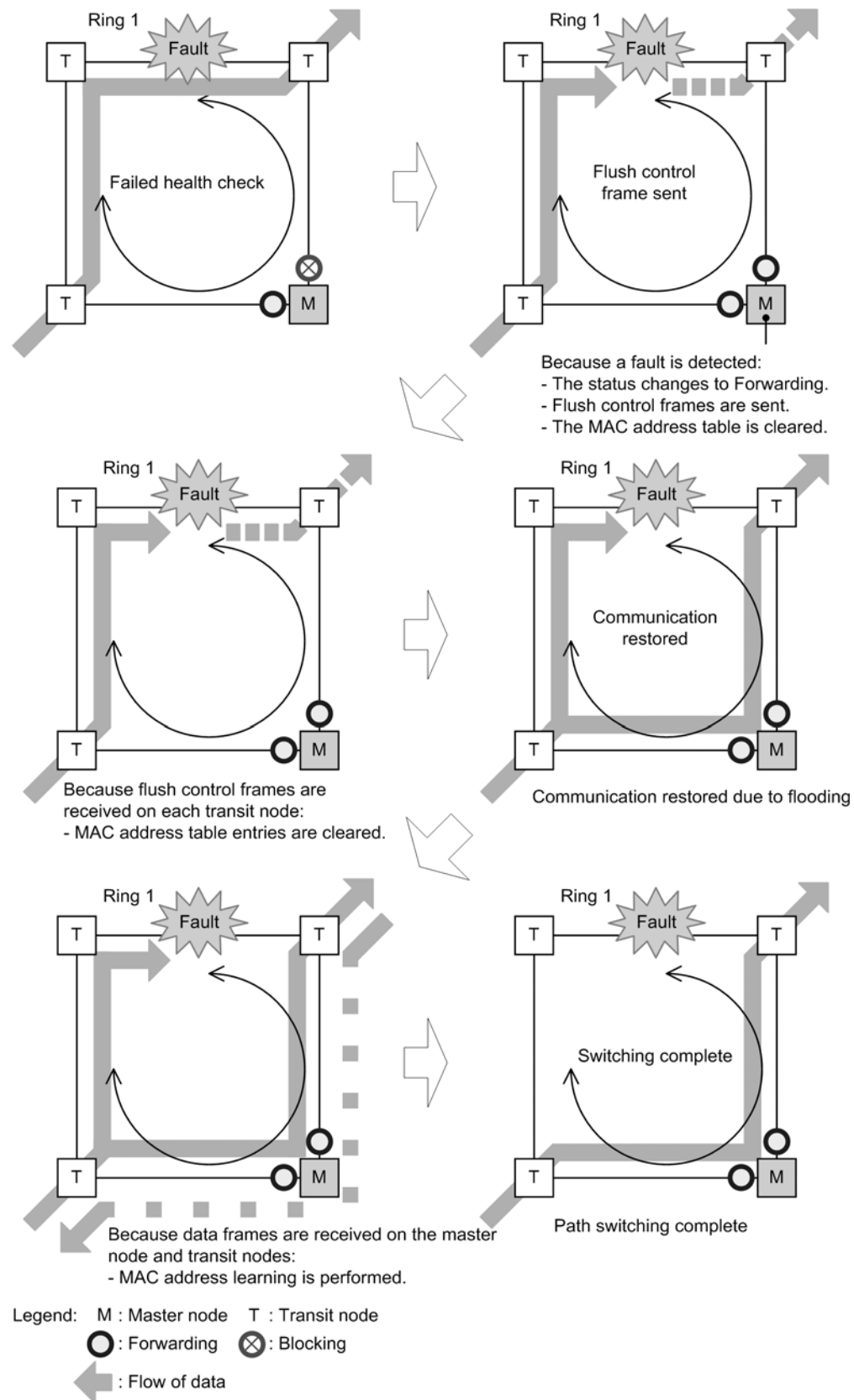
Ring faults are monitored under the Ring Protocol by having the master node regularly send control frames called health-check frames, and then monitor whether or not these health-check frames were received. When a health-check frame does not arrive within a fixed time, the master node determines that 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.

21.2.4 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 switch the path 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 21-7 Overview of path switching for the Ring Protocol**(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

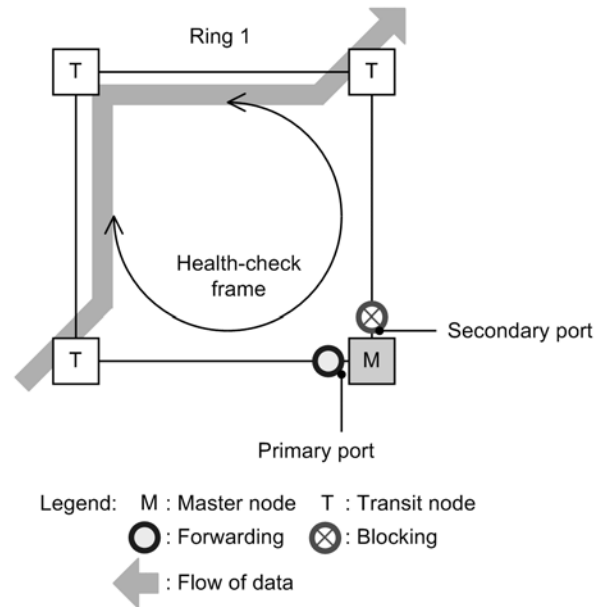
When a ring fault is detected on the master node, a control frame called a flush control frame is sent to other transit nodes in the ring of the same control VLAN to request that MAC address table entries be cleared. When this flush control frame is received, MAC address table entries are cleared for the ring port. Because of this, flooding is performed until MAC address learning is performed. MAC address learning occurs by sending and receiving frames on the new path, and communication path switching is completed.

21.3 Overview of single ring operation

21.3.1 Normal ring operation

The following figure shows normal operation for a single ring.

Figure 21-8 Normal ring operation



(1) Master node operation

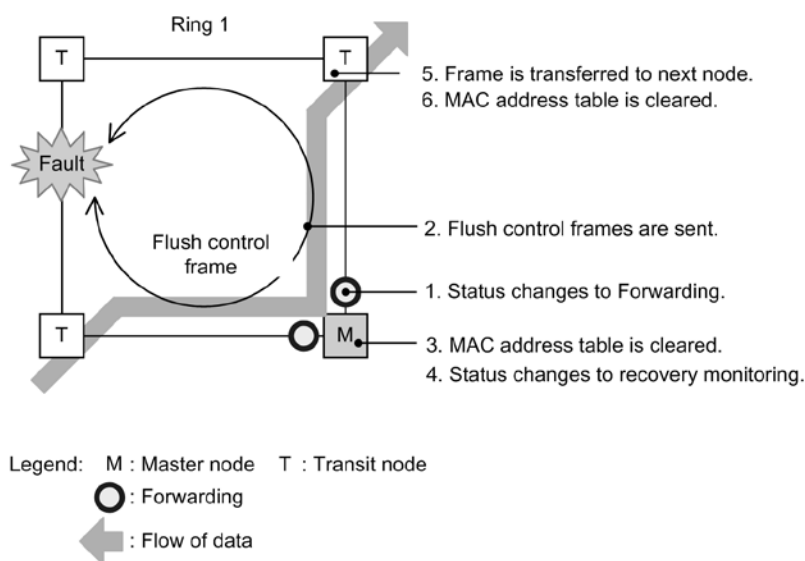
To prevent fault misdetection due to one-way link faults, health-check frames are sent from two ring ports. Monitoring is performed to check that health-check frames in both directions are received within the pre-determined time. Data frame transfer is performed on the primary port. Because the secondary 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.

21.3.2 Operation when a fault is detected

The following figure shows operation when a ring fault has been detected for a single ring.

Figure 21-9 Operation during a ring fault**(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 21-2 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 to an alternate path.

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.

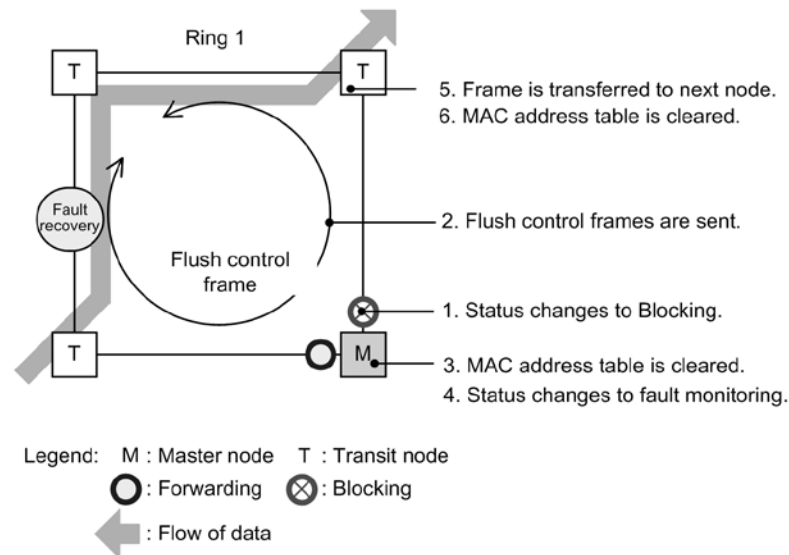
6. The MAC address table is cleared.

The MAC address table entries pertaining to the ring port are cleared. Clearing the MAC address table entries allows paths to be switched to an alternate path.

21.3.3 Operation when recovery is detected

The following figure shows operation when recovery from a ring fault is detected for a single ring.

Figure 21-10 Operation during fault recovery



(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 21-3 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 to a normal communication path.

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 to a normal communication path.

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** configuration command) of the ring port. The reception hold time for flush control frames (**forwarding-shift-time** configuration command) is set when recovery from a link fault on a ring port has occurred.

21.3.4 Operation when path switch-back is suppressed and cleared

When the path switchback 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:

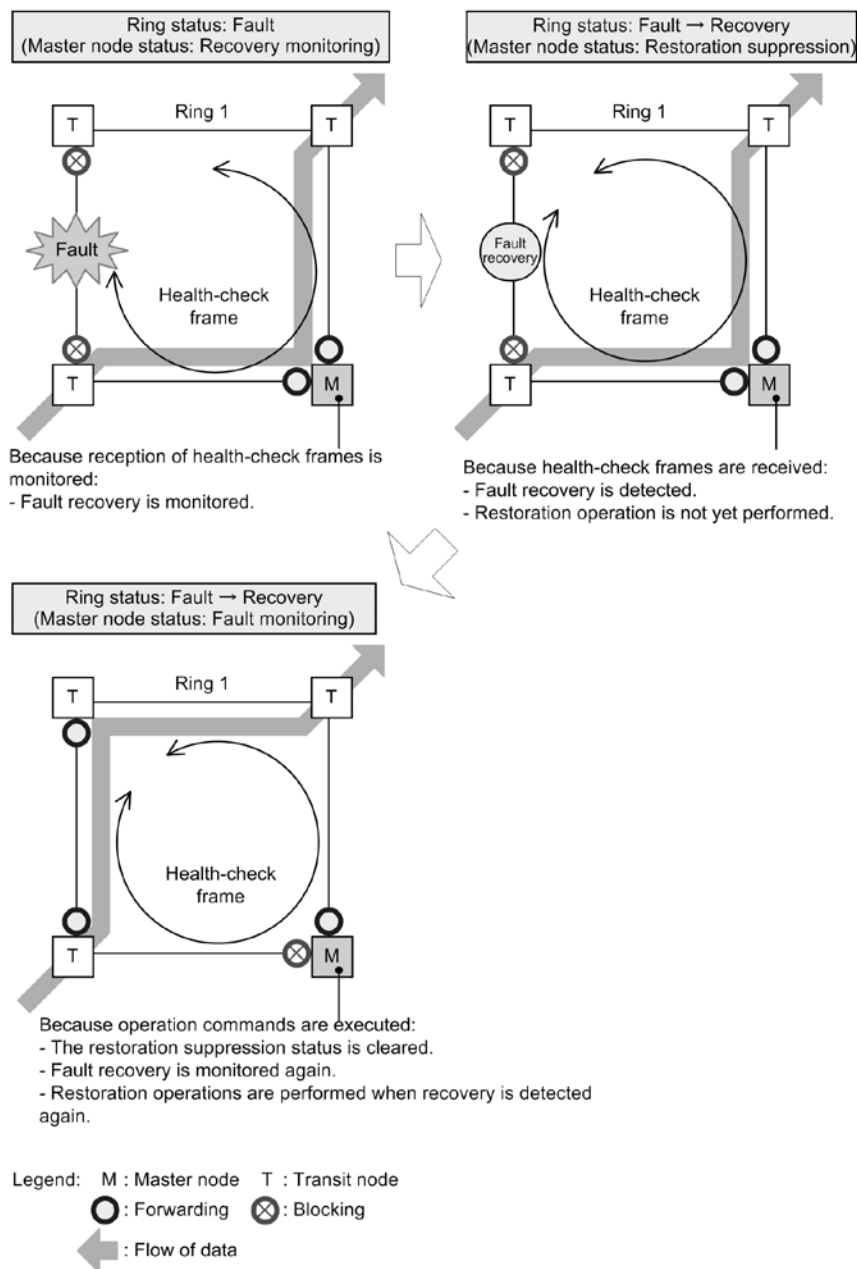
- Path switch-back suppression is cleared by executing the **clear axrp preempt-delay** operation command.
- The path switch-back suppression time specified by the **preempt-delay** configuration command elapses.
- The **preempt-delay** configuration command enabling path switch-back suppression functionality 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 21-11 Operation when operation commands are executed to clear path switch-back suppression



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).

21.4 Overview of multi-ring operation

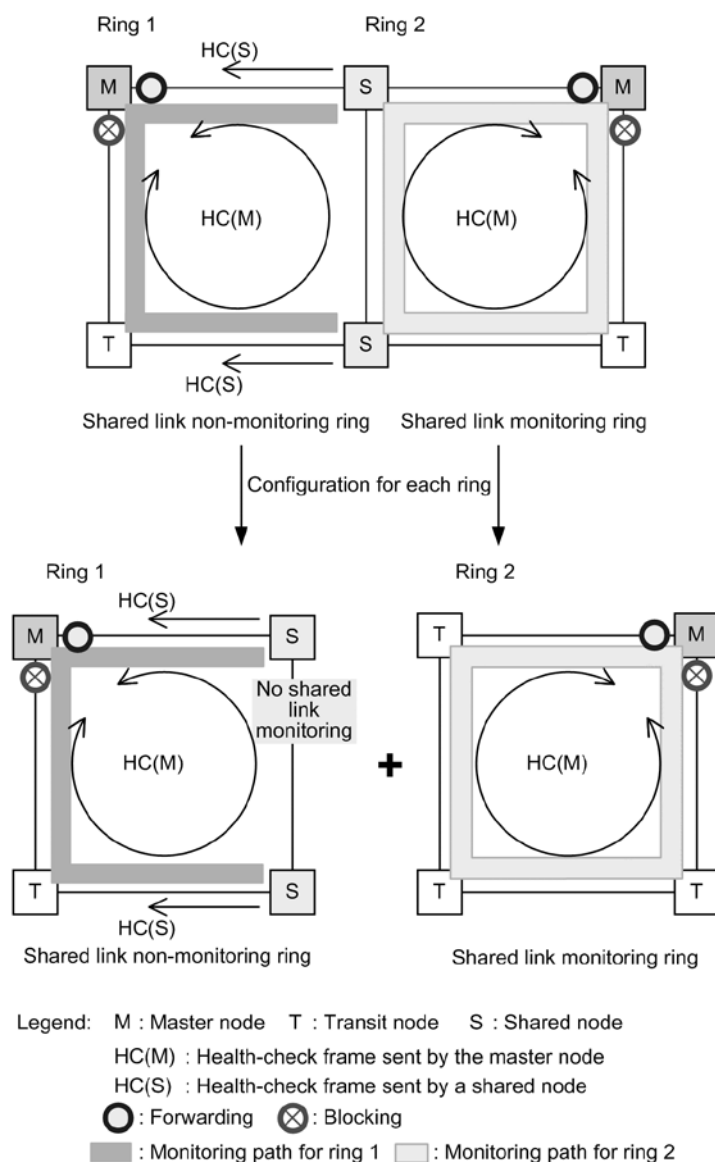
The following explains multi-ring configurations, focusing on those with shared links. For details about multi-ring configurations without shared links, because operation is the same as for single rings, see 21.3 *Overview of single ring operation*.

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.

21.4.1 Normal ring operation

The following figure shows normal operation for a multi-ring configuration with shared links.

Figure 21-12 Normal ring status

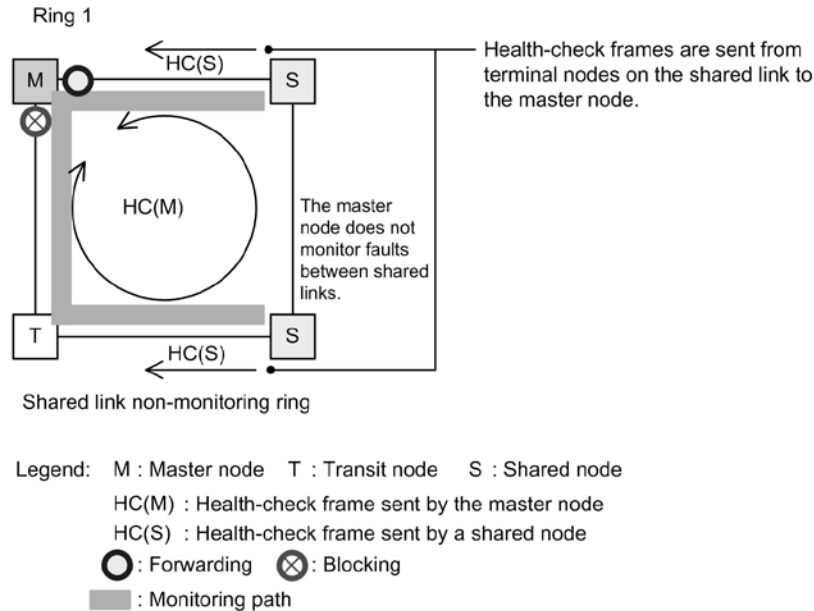


(1) Shared link non-monitoring rings

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 21-13 Normal operation for shared link non-monitoring rings



(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

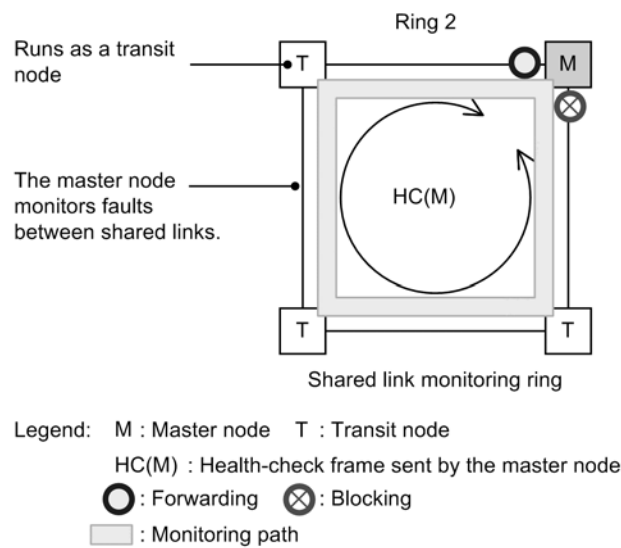
Transit node operation is the same as for single rings. Transit nodes do not monitor HC(M)s and HC(S)s. When an HC(M) or HC(S) is received, it is transferred to the next node in the ring. Data frame transfer is performed on both ring ports.

(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 from 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 for a single ring, as master nodes or transit nodes.

Figure 21-14 Normal operation for shared link monitoring rings**(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.

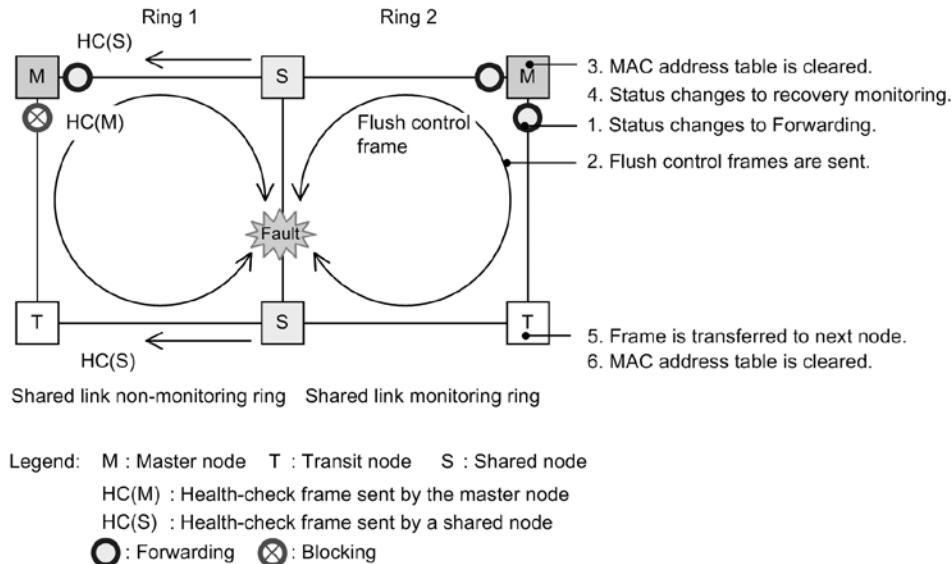
21.4.2 Operation for shared link faults and restoration

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 21-15 Operation during shared link faults



(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:

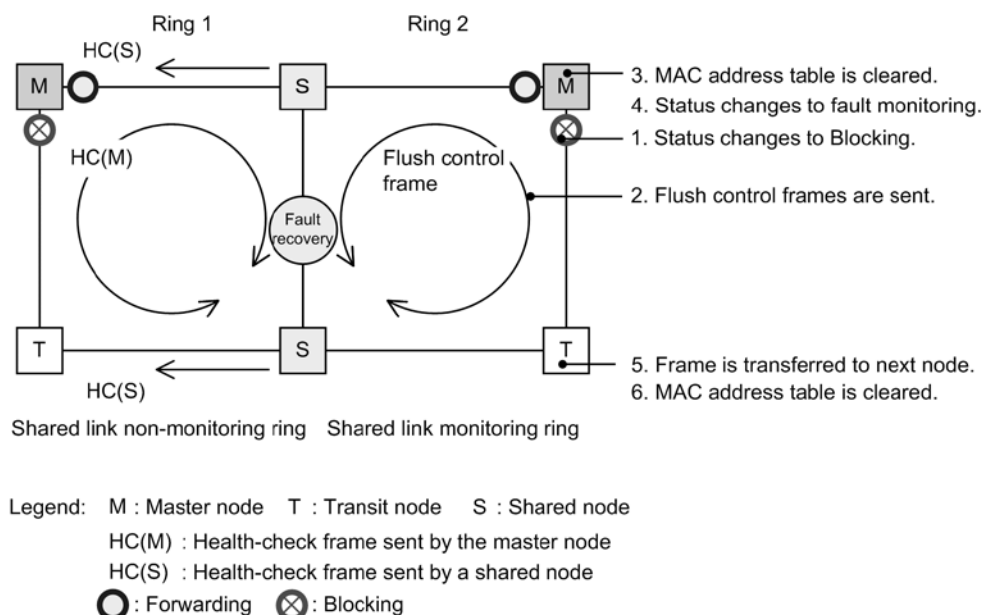
5. Flush control frames are transferred.
6. The MAC address table is cleared.

(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 21-16 Operation during shared link recovery**(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.

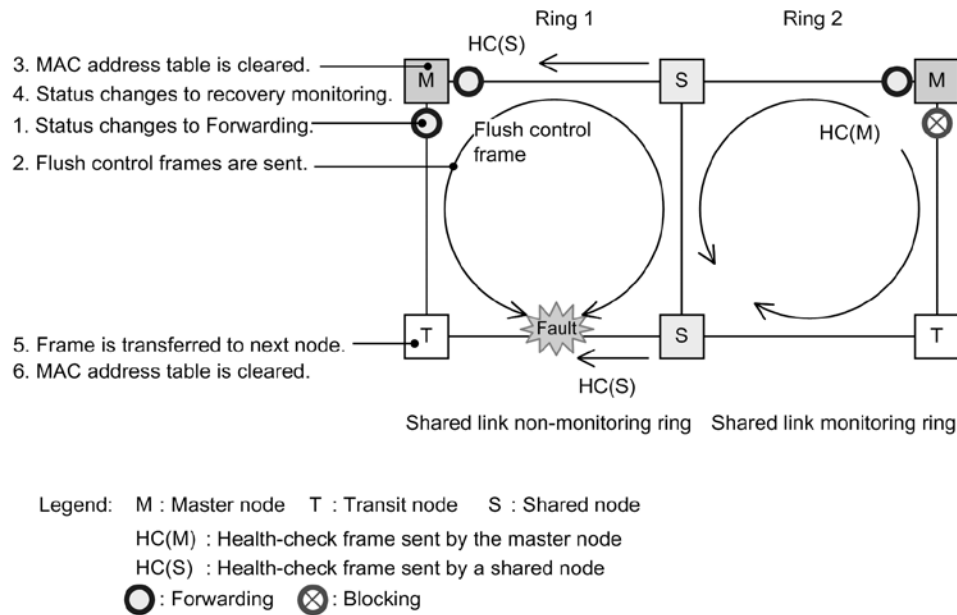
21.4.3 Operation for faults and restoration other than for shared links in a shared link non-monitoring ring

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 21-17 Operation during a ring fault other than for shared links on shared link non-monitoring rings



(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:

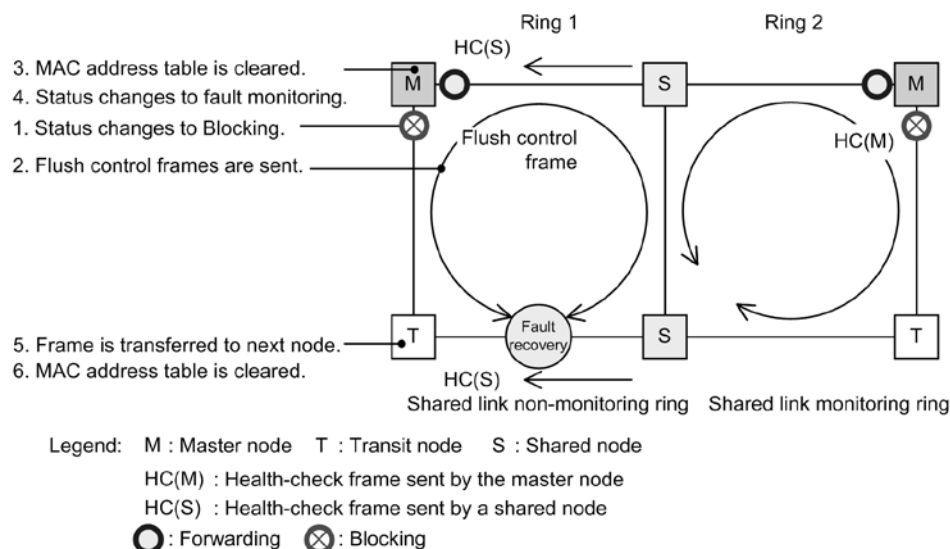
5. Flush control frames are transferred.
6. The MAC address table is cleared.

(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 21-18 Operation for recovery from a ring fault other than for shared links in a shared link non-monitoring ring**(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 is 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

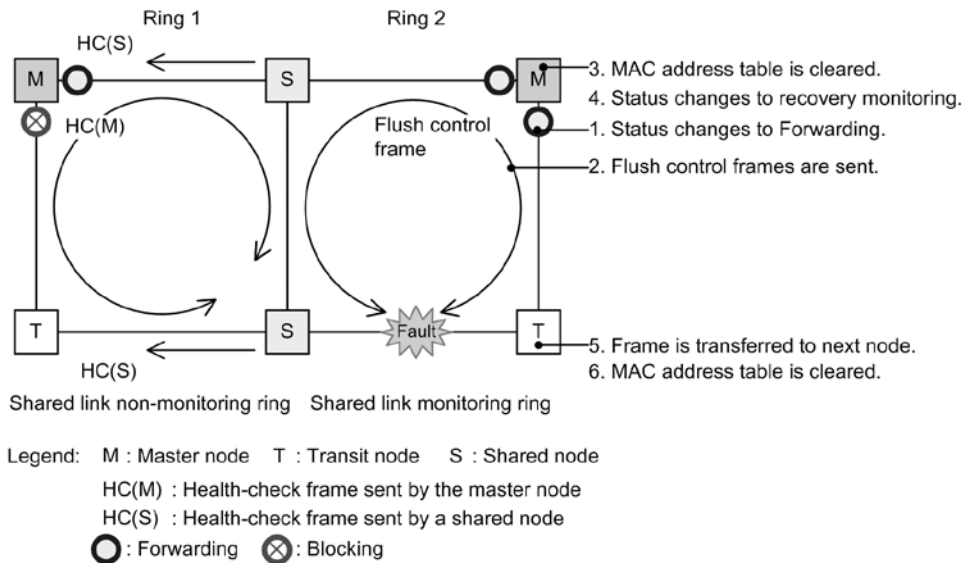
Because no faults occur within a shared link monitoring ring, restoration is not performed.

21.4.4 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 21-19 Operation during ring faults other than for shared links in a shared link monitoring ring**(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:

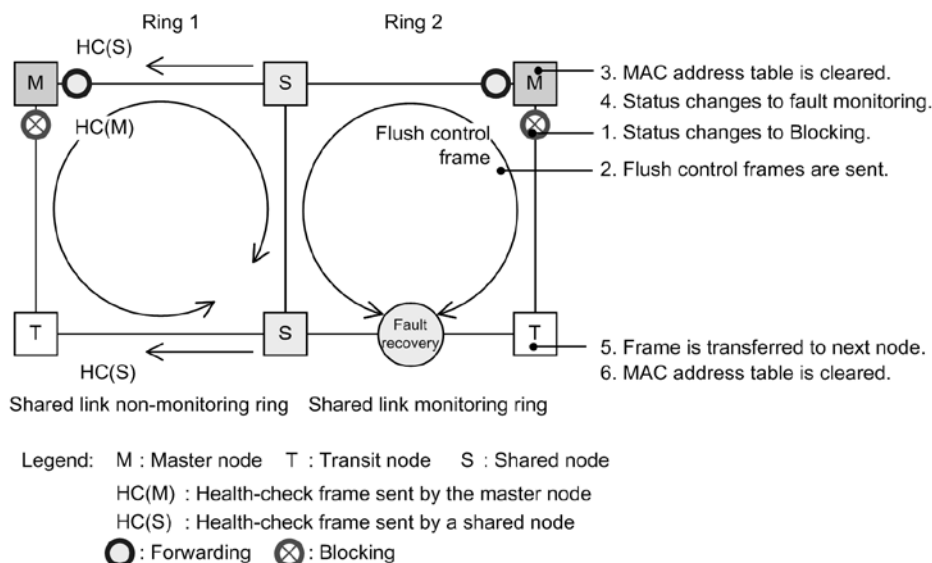
5. Flush control frames are transferred.
6. The MAC address table is cleared.

(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 21-20 Operation for recovery from a ring fault other than for shared links in a shared link monitoring ring**(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.

21.4.5 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 *21.3 Overview of single ring operation*.

21.5 Multi-fault monitoring functionality for the Ring Protocol

21.5.1 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 21-21 Example of a fault on a shared link monitoring ring

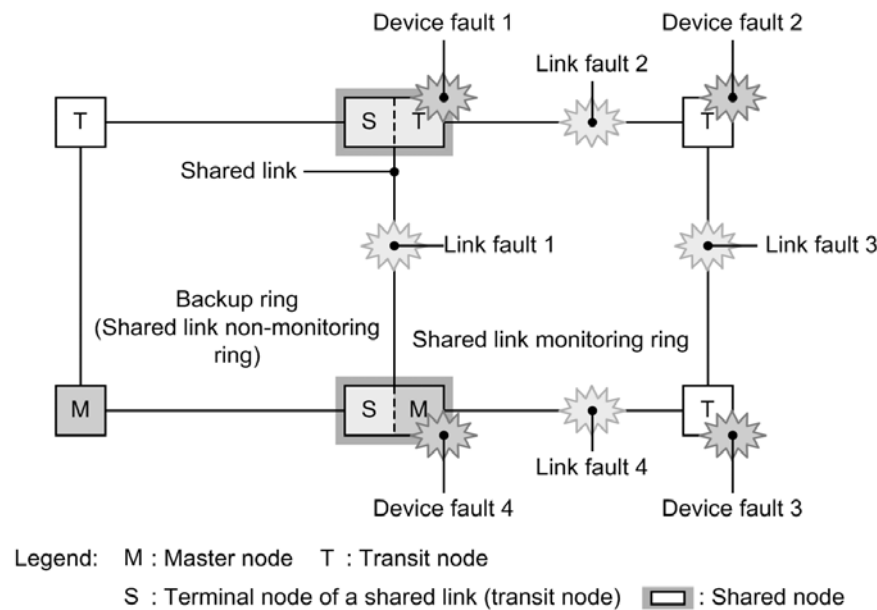


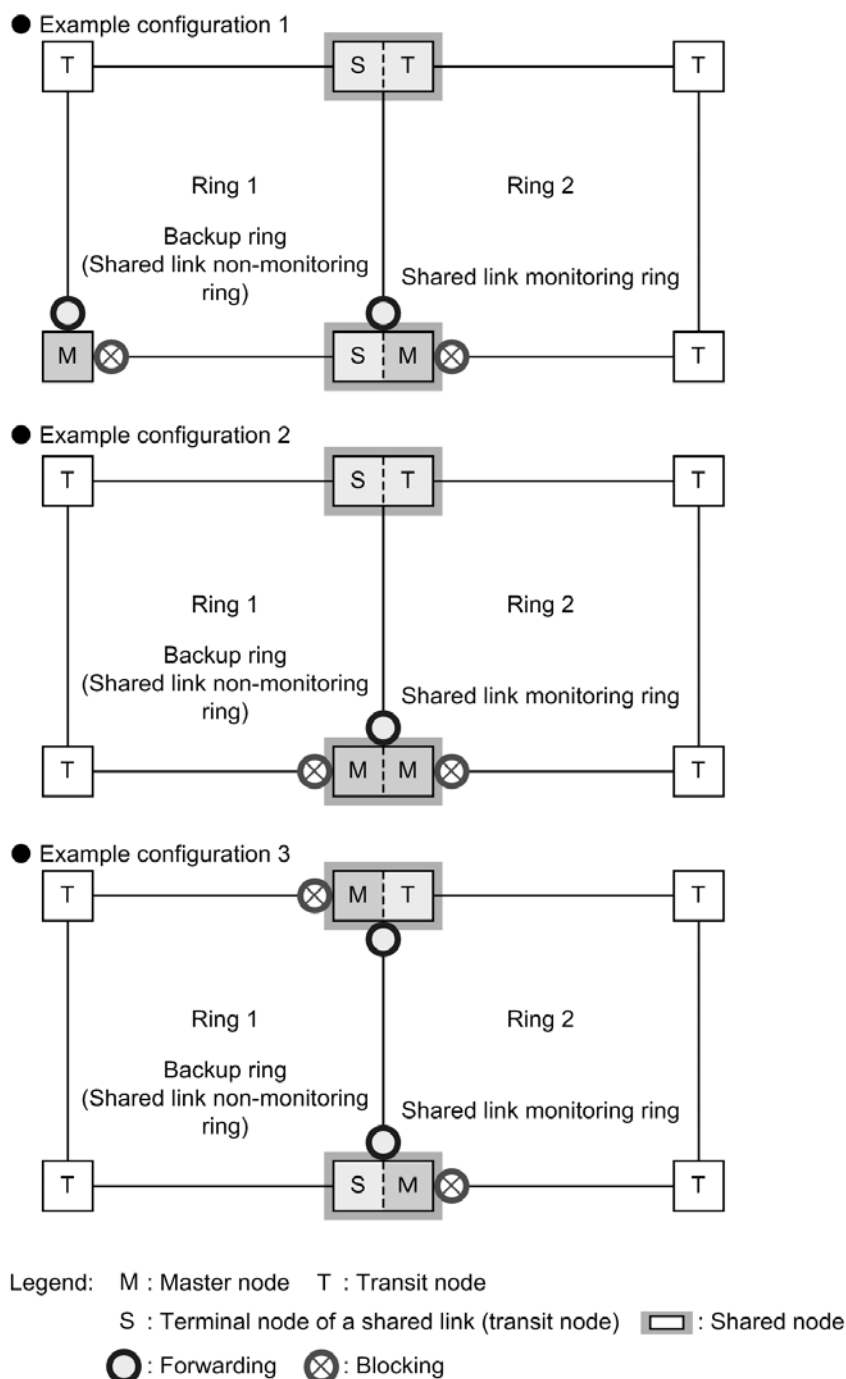
Table 21-4 Combinations of faults that can be detected by the multi-fault monitoring functionality

Fault 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)

21.5.2 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 21-22 Basic configuration example for the multi-fault monitoring functionality



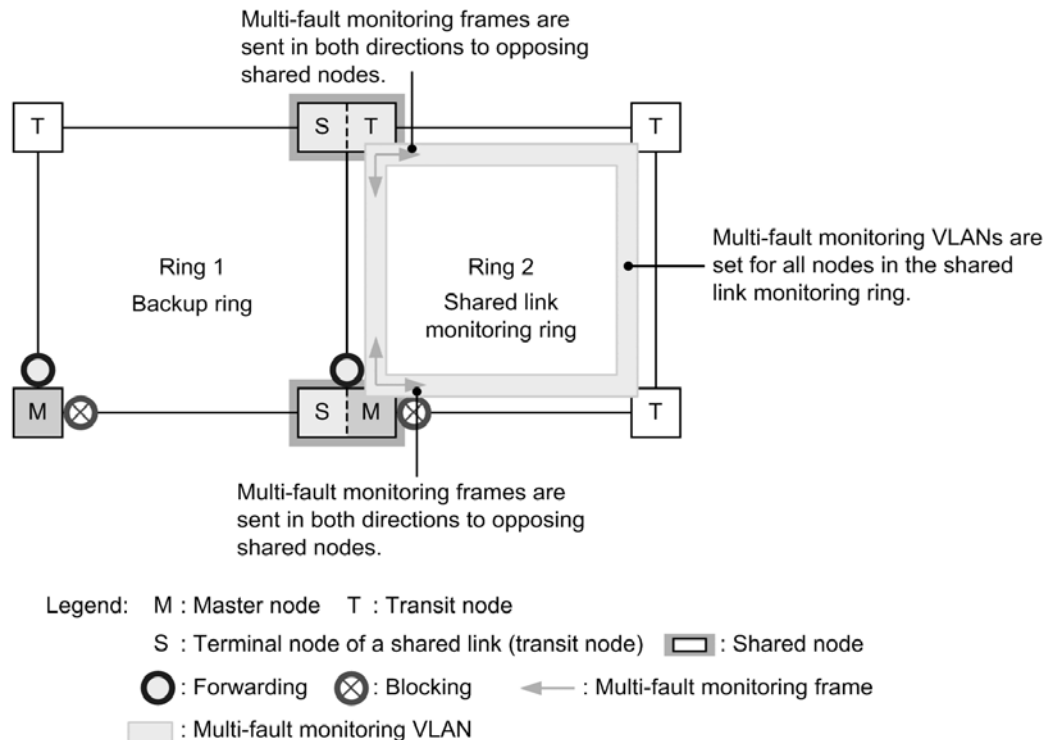
21.5.3 Overview of operation for multi-fault monitoring

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 shows an overview of multi-fault monitoring operation.

Figure 21-23 Overview of multi-fault monitoring operation



(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 21.4.1(2) *Shared link monitoring ring*.

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

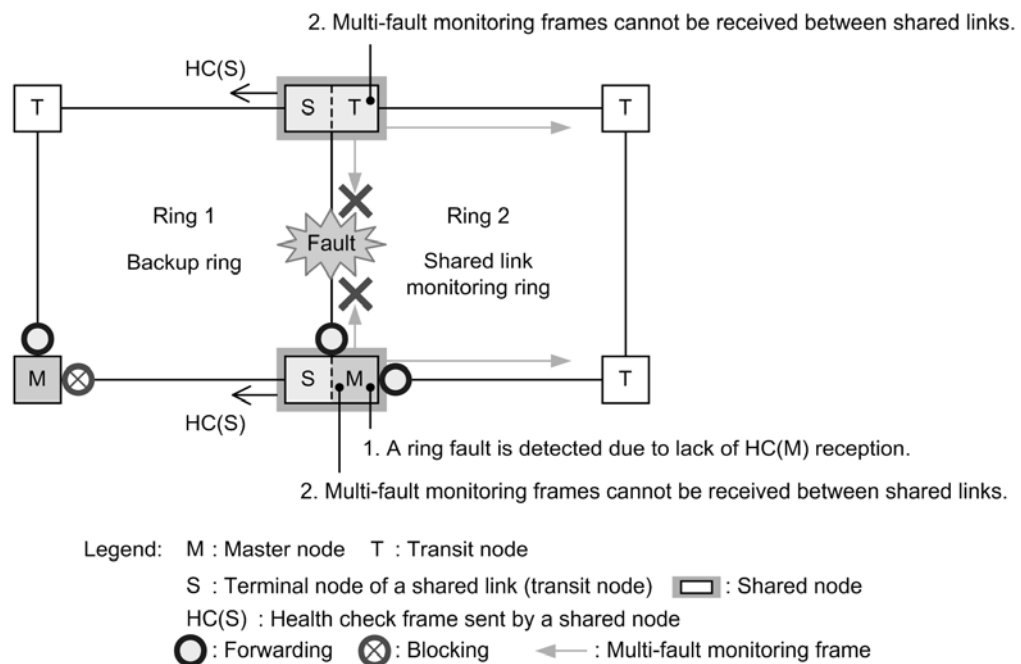
For details about the operation for master nodes and transit nodes in a backup ring, because operation is the same as that for multi-rings, see 21.4.1(1) *Shared link non-monitoring ring*.

21.5.4 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 21-24 Operation during shared link faults**(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 21.4.2(1) *Operation when a fault is detected*.

2. Multi-fault monitoring frames cannot be received between shared links.

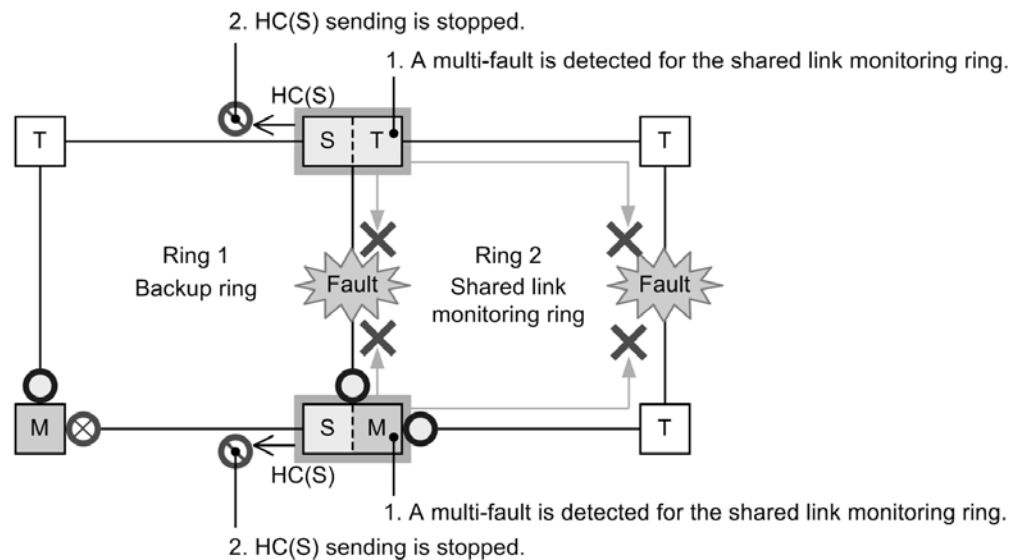
Shared nodes can no longer receive multi-fault monitoring frames between shared links, but because reception is still possible on the other ring port, multi-fault monitoring continues.





(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 21-25 Operation when multi-faults occur

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.

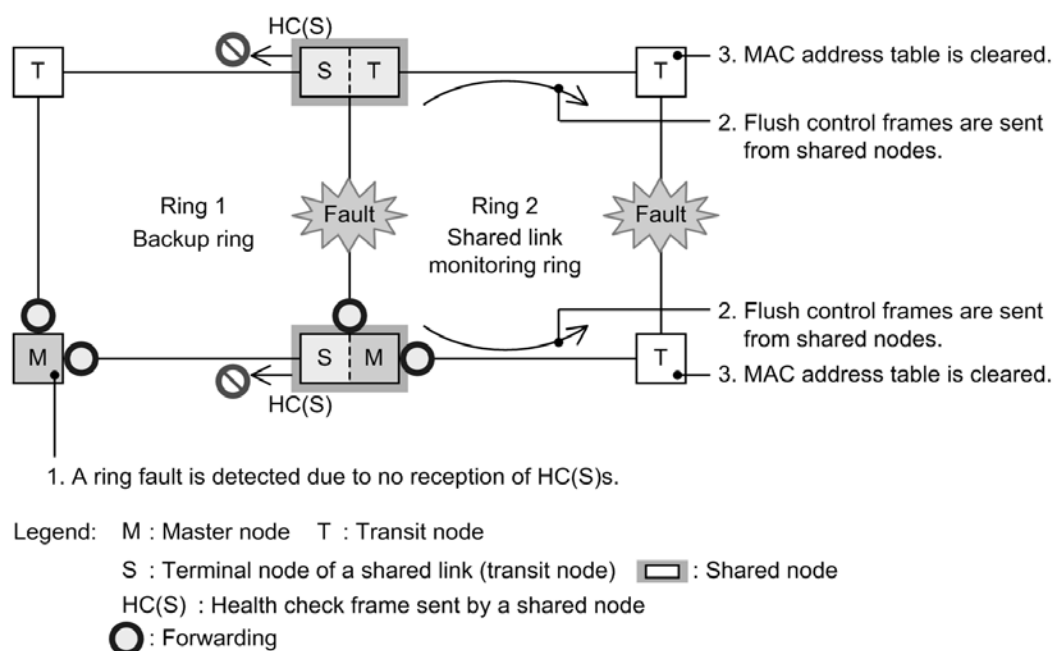
(b) Operation for each node in a backup ring

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 21-26 Operation for switching to the backup ring**(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 21.4.3(1) *Operation when a fault is detected*.

(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.

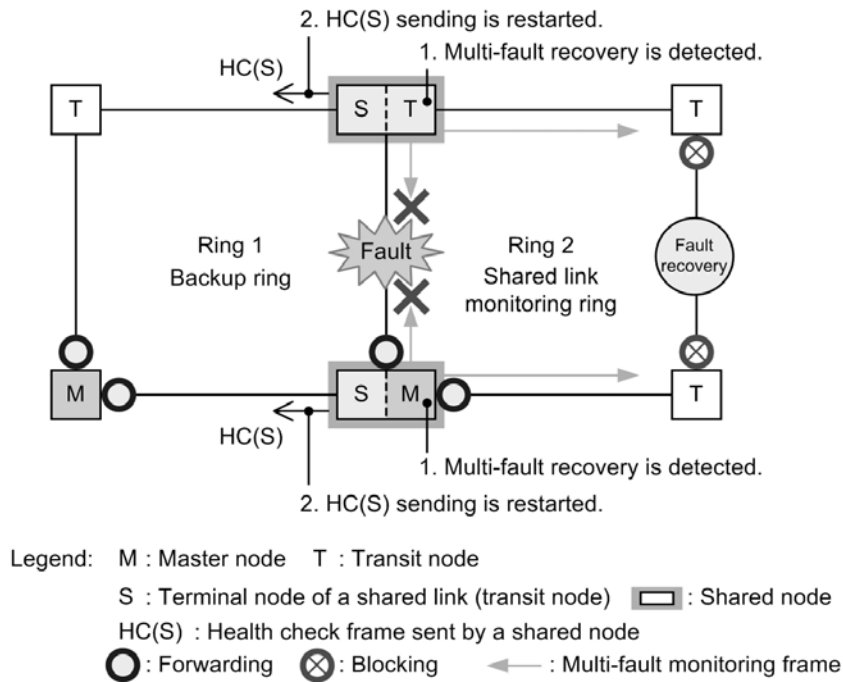
Transit nodes receive flush control frames sent from shared nodes, and clear the MAC address table.

21.5.5 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 21-27 Operation during partial recovery from a multi-fault**(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.

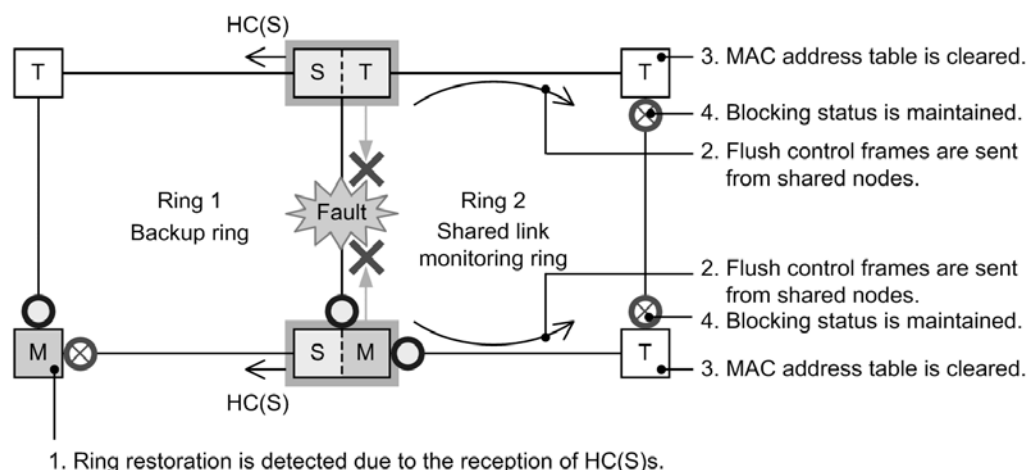
(b) Operation for each node in a backup ring

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 21-28 Switch-back operation from backup rings

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 21.4.3(2) *Operation when recovery is detected*.

(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. MAC address table is cleared.

Transit nodes receive flush control frames sent from shared nodes, and clear the MAC address table.

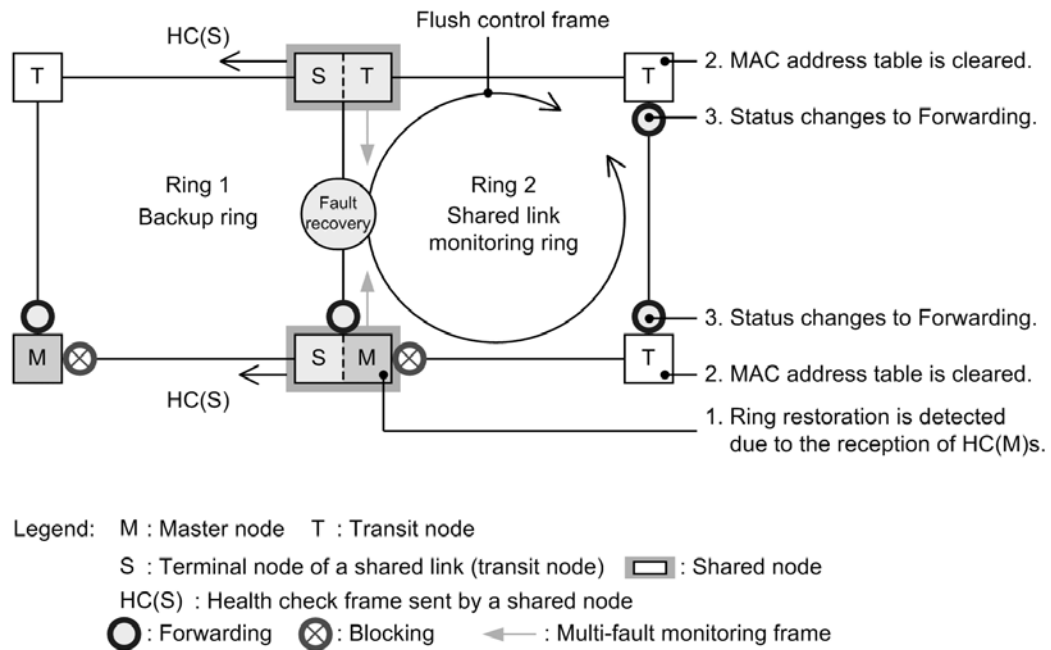
4. The **Blocking** status is maintained.

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 21.7(18) *Communication during partial multi-fault recovery*.

(3) Operation during recovery from a shared link fault

The following figure shows operation during shared link fault restoration.

Figure 21-29 Operation during recovery from a shared link fault**(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 21.4.2(2) *Operation when recovery is detected*.

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 **Forwardi ng**.

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 **Forwardi ng**.

21.6 Ring Protocol network design

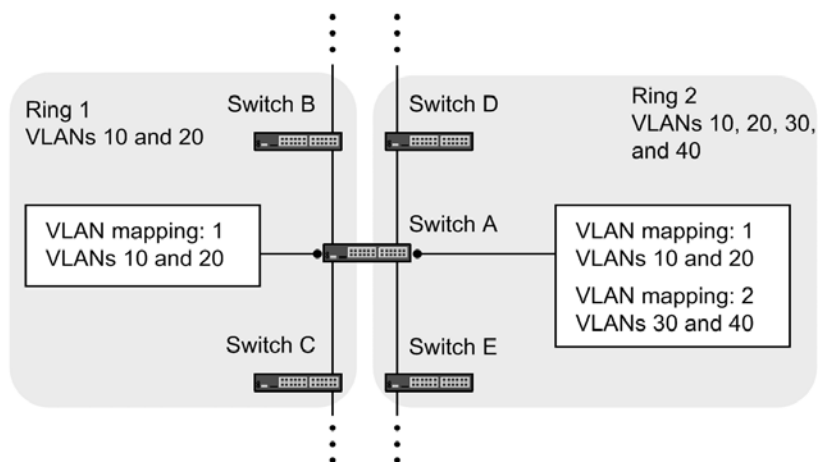
21.6.1 Using VLAN mappings

(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 a 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 21-30 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+.

21.6.2 Using forwarding-delay-time for control VLANs

When the Ring Protocol runs from the initial state during device startup for a transit node, data transfer VLANs are logically blocked. Transit nodes remove the logical block when they receive a flush control frame sent from the master node. However, when the fault monitoring time (`health-check holdtime` configuration command) for the master node is long during device 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` configuration command) 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` parameter of the `control-vlan` configuration command) is set for the control VLAN, this kind of case can be avoided.

1. The transit node logically blocks the control VLAN immediately after device startup.
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` parameter of the

`control-vlan` configuration command) 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` parameter of the `control-vlan` configuration command) and fault monitoring time (`health-check holdtime` configuration command) for control VLANs

For the forwarding transition time (`forwarding-delay-time` parameter of the `control-vlan` configuration command) of a control VLAN, set a value greater than that of the fault monitoring time (`health-check holdtime` configuration command). For the forwarding transition time of a control VLAN (`forwarding-delay-time` parameter of the `control-vlan` configuration command), we recommend setting a value around twice that of the fault monitoring time (`health-check holdtime` configuration command). If a value less than that of the fault monitoring time (`health-check holdtime` configuration command) 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.

21.6.3 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 21-5 Primary port selection method (VLAN group #1)

Ring port #1	Ring port #2	Prioritized port
Physical port	Physical port	The port with the smaller port number runs as the primary port.
Physical port	Channel group	The physical port runs as the primary port.
Channel group	Physical port	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 21-6 Primary port selection method (VLAN group #2)

Ring port #1	Ring port #2	Prioritized port
Physical port	Physical port	The port with the larger port number runs as the primary port.
Physical port	Channel group	The channel group runs as the primary port.
Channel group	Physical port	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.

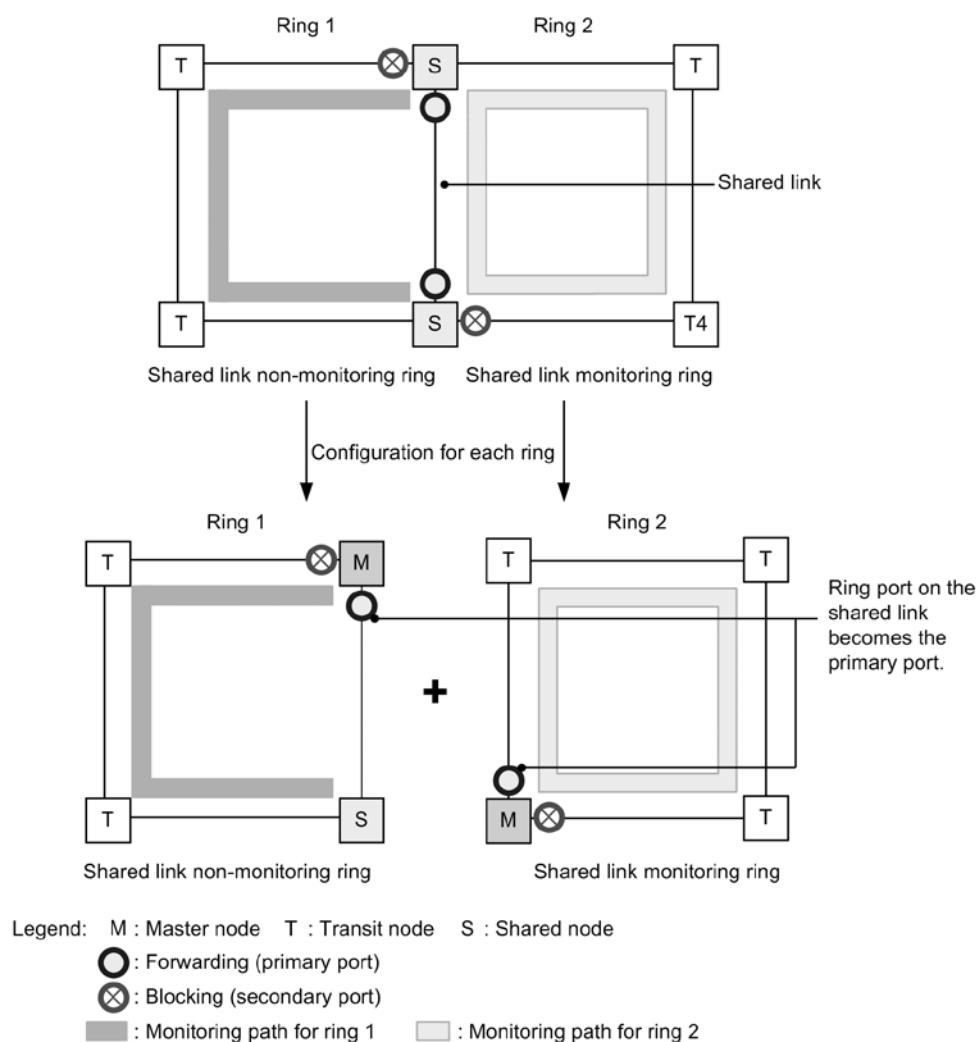
21.6.4 Configurations with mixed node types within the same device

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.

21.6.5 Configurations with mixed node types for shared nodes

In a multi-ring configuration with shared links, nodes placed 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 21-31 Port status when a shared node is used as the master node



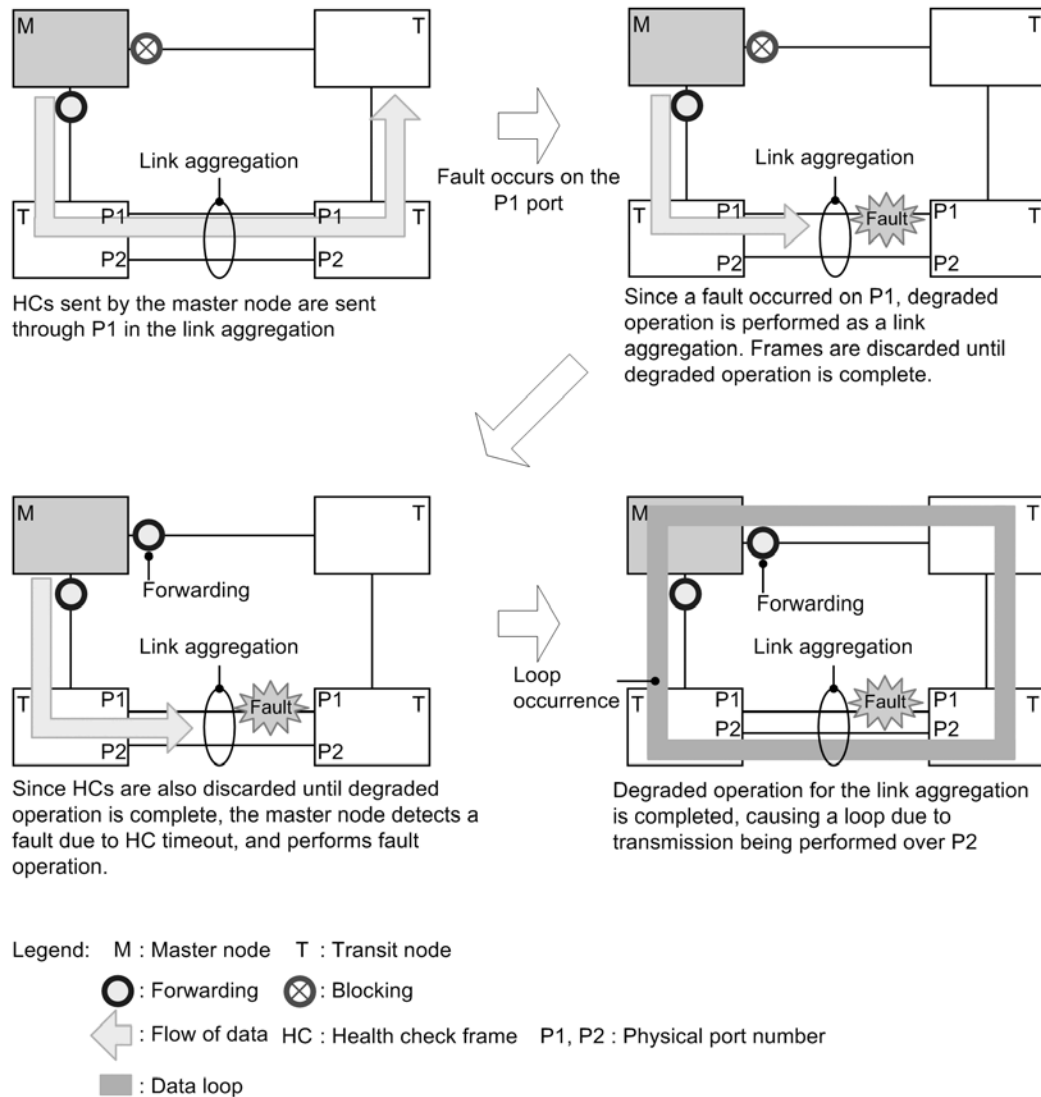
21.6.6 Setting fault monitoring times when link aggregation is used

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` configuration command) 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 21-32 Fault detection when link aggregation is used



21.6.7 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.

21.6.8 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 *14.2.6 Configuring the link-down detection timer* and *14.2.7 Configuring the link-up detection timer*.

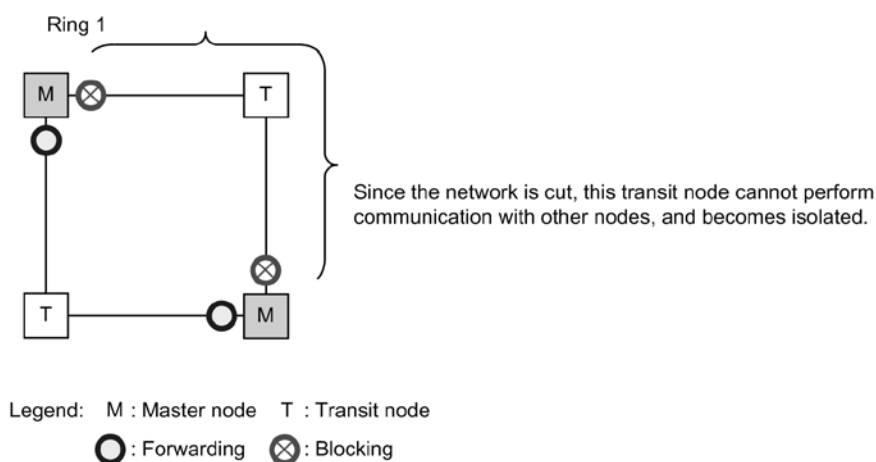
21.6.9 Prohibited Ring Protocol configurations

The following describes prohibited network configurations when the Ring Protocol is used.

(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.

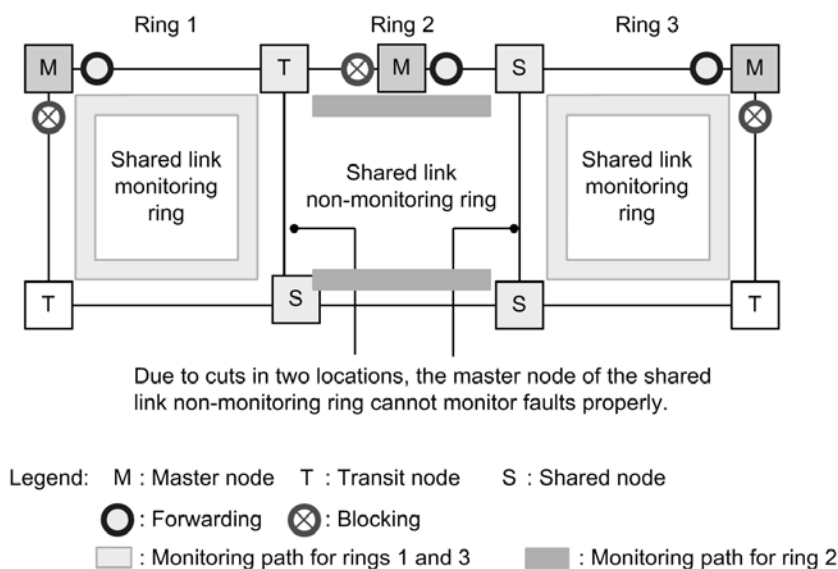
Figure 21-33 Setting multiple master nodes in the same ring



(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.

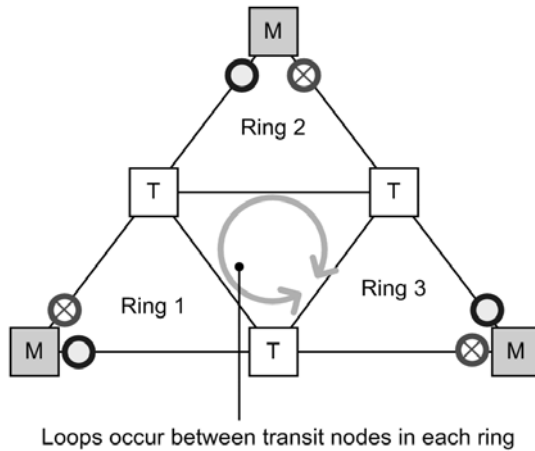
Figure 21-34 Configuration with multiple shared link monitoring rings



(3) Example of a looped multi-ring configuration

For multi-ring configurations such as that in the following figure, loops form between transit nodes.

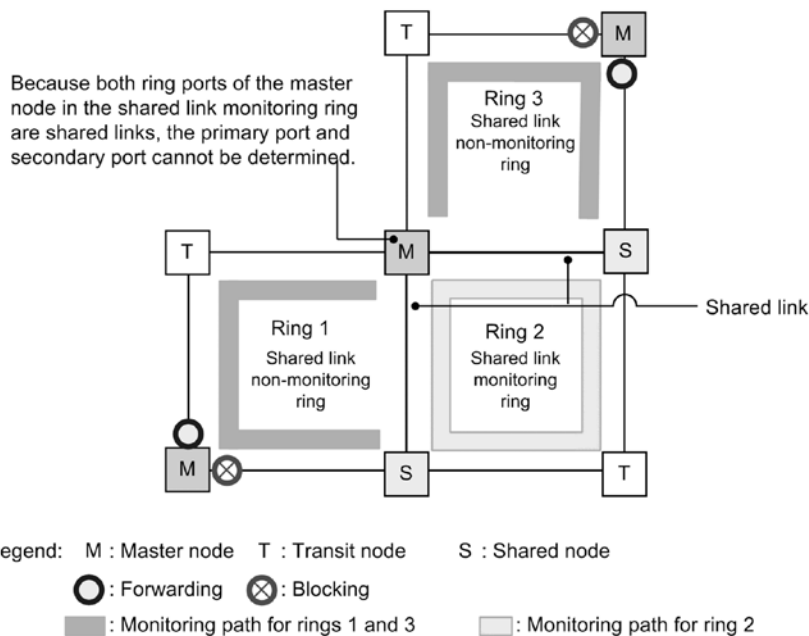
Figure 21-35 Looped multi-ring configuration



(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 21-36 Configuration in which the master node's primary port cannot be determined



21.6.10 Prohibited configurations for the multi-fault monitoring functionality

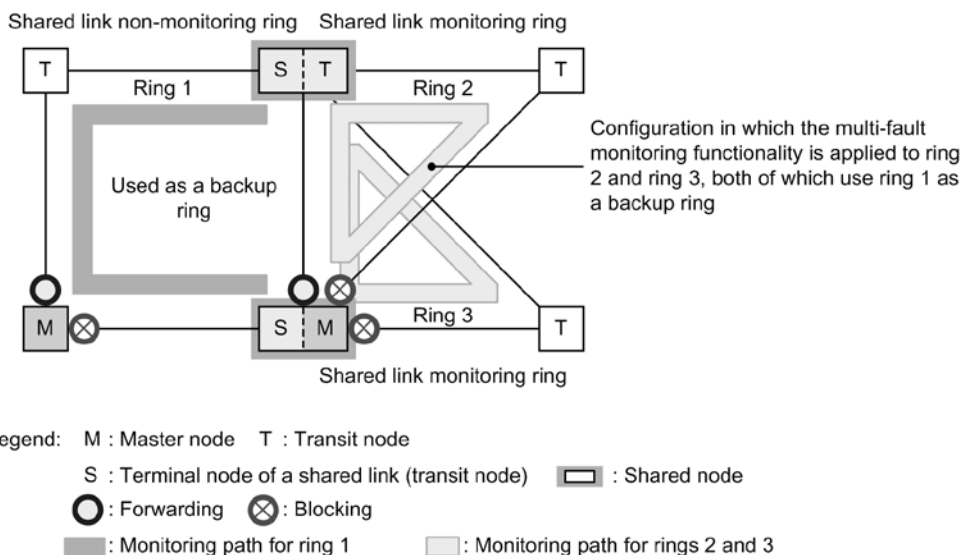
The prohibited configurations when the multi-fault monitoring functionality is used are as follows.

(1) Configurations 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 21-37 Configuration in which multiple shared link monitoring rings use the same backup ring

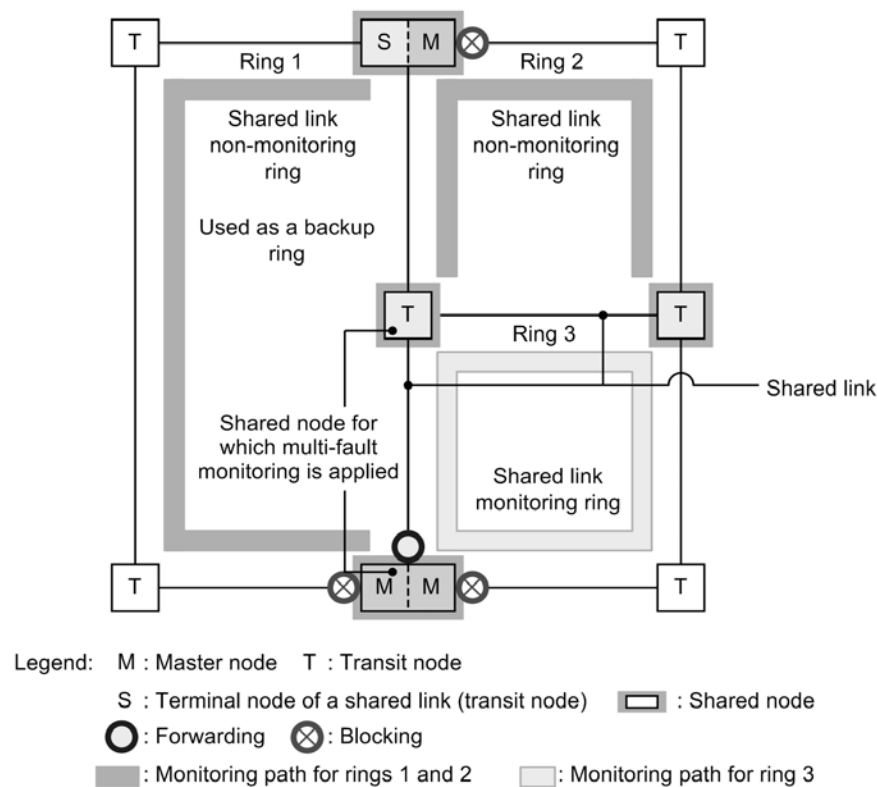


(2) Configuration in which multi-faults are monitored on shared nodes within shared links

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.

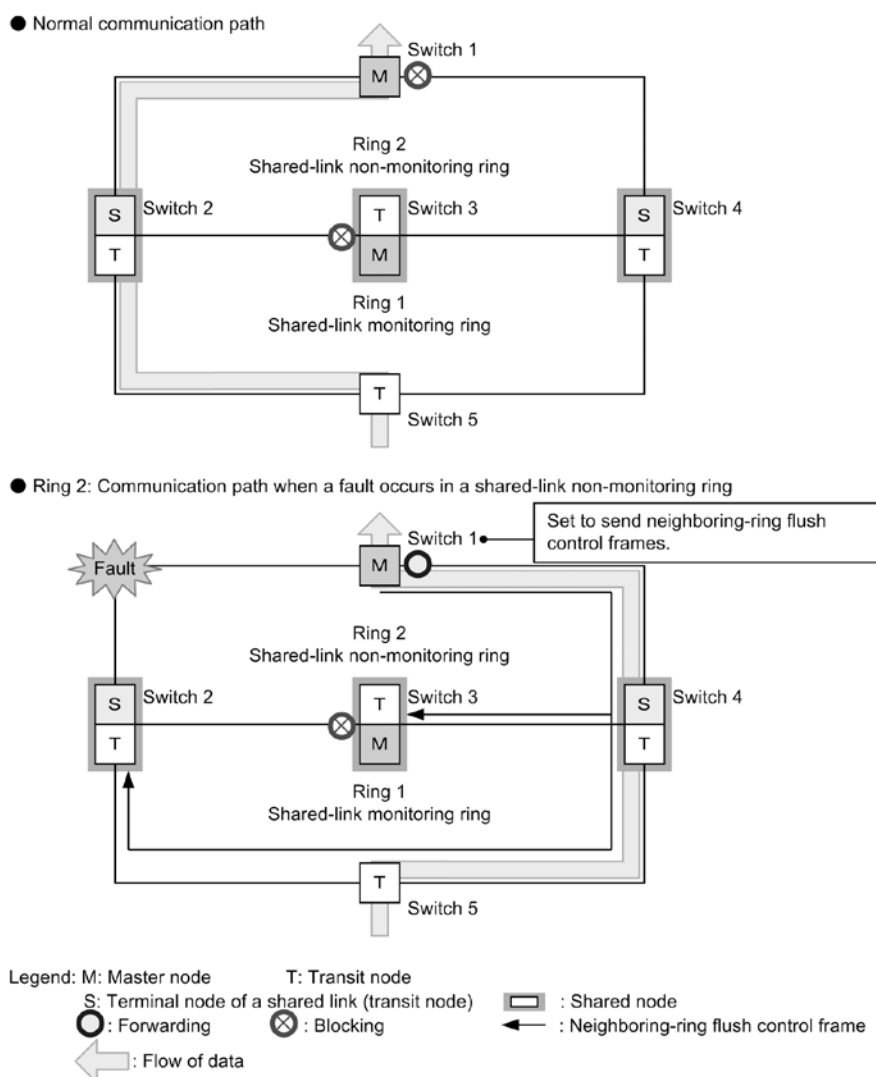
Figure 21-38 Configuration in which multi-faults are monitored on shared nodes within shared links



21.6.11 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 21-39 Example configuration in which both ring ports of a master node are shared links

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.

21.7 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 *16.3 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.

Note that the default VLAN (VLAN ID = 1) cannot be set.

(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 for flush control frames (`forwarding-shift-time` configuration command) times out. When the reception hold time for flush control frames (`forwarding-shift-time` configuration command) is shorter than the health check sending interval of the master node (`health-check-interval` configuration command), 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` configuration command) to a value greater than the health check sending interval (`health-check-interval` configuration command).

(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 the **Blocking** status, and are no longer able to communicate.

(6) Building networks when the Ring Protocol is used

Networks using the Ring Protocol basically have a looped configuration. Therefore, build such networks as follows to avoid loops.

- When configuring the Ring Protocol, set **shut down** for the ring port (physical port or channel group) of the ring configuration node to take it down beforehand.
- Clear **shut down** for the ring port when the Ring Protocol has been set for all network devices.

(7) Health-check frame sending interval and fault monitoring times

Set the fault monitoring time (**health-check hold time** configuration command) to a value greater than the sending interval (**health-check interval** configuration command). 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 *21.5 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.

(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 vl an- mappi ng`
- `axrp- ri ng- port`
- `axrp- pri mary- port`
- `axrp vi rtual - li nk`

Note that for VLAN mapping (`axrp vl an- mappi ng` configuration 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 `Bl ocki ng`. The corresponding ring port changes to the `Forwardi ng` status and communication is restored after the reception hold time for flush control frames (`forwardi ng- shi ft- ti me` configuration command) 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).

(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** configuration command) for flush control frames for the transit node, or specify a value greater than the path switch-back suppression time (**preempt-delay** configuration command). 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** configuration command) 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 (**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** configuration command before shutting down the channel group of the link aggregation by using the **shutdown** configuration command.

If you bring up the channel group using the **no shutdown** configuration command, make sure to shut down all physical ports belonging to the channel group by using the **shutdown** configuration command.

22. Settings and Operation for Ring Protocol

This chapter describes example settings for the Ring Protocol.

22.1 Configuration

22.2 Operation

22.1 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.

22.1.1 List of configuration commands

The following table describes the configuration commands for the Ring Protocol.

Table 22-1 List of configuration commands

Command name	Description
<code>axrp</code>	Set the ring ID.
<code>axrp vlan-mapping</code>	Sets the VLAN mapping and VLANs participating in the mapping.
<code>axrp-primary-port</code>	Sets the primary port.
<code>axrp-ring-port</code>	Sets the ring port.
<code>control-vlan</code>	Sets the VLAN to be used as the control VLAN.
<code>disable</code>	Disables the Ring Protocol functionality.
<code>flush-request-count</code>	Sets the number of times flush control frames are sent.
<code>flush-request-transmit-vlan</code>	Sets a VLAN that sends flush control frames for neighboring rings to devices in the neighboring ring.
<code>forwarding-shift-time</code>	Sets the reception hold time for flush control frames.
<code>health-check holdtime</code>	Sets the hold time for health-check frames.
<code>health-check interval</code>	Sets the sending interval for health-check frames.
<code>mode</code>	Sets the operating mode for a ring.
<code>multi-fault-detection holdtime</code>	Sets the reception hold time for multi-fault monitoring frames.
<code>multi-fault-detection interval</code>	Sets the sending interval for multi-fault monitoring frames.
<code>multi-fault-detection mode</code>	Sets the monitoring mode for multi-fault monitoring.
<code>multi-fault-detection vlan</code>	Sets the VLAN used as the multi-fault monitoring VLAN.
<code>name</code>	Sets the name for identifying the ring.
<code>preempt-delay</code>	Enables the path switch-back suppression functionality and sets the suppression time.

Command name	Description
<code>vlan-group</code>	Sets the VLAN group for which to run the Ring Protocol functionality, and the VLAN mapping ID.

22.1.2 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 *20 Spanning Tree Protocols*.

(2) Setting 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

22.1.3 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.

22.1.4 Configuring control VLANs

(1) Setting control VLANs

Points to note

Specify the VLAN to be used as the control VLAN. Note that the following VLANs cannot be set.

- VLANs used as data transfer VLANs
- VLAN IDs that are the same as VLAN IDs used for different rings
- Default VLAN (VLAN = 1)

Command examples

1. `(config)# axrp 1`

Switches to axrp configuration mode for ring ID 1.

2. `(config-axrp)# control-vlan 2`

`(config-axrp)# exit`

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`

`(config-axrp)# exit`

Sets the forwarding transition time for the control VLAN to 10 seconds.

22.1.5 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, additions applying to multiple rings 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, deletions applying to multiple rings 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.

22.1.6 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.

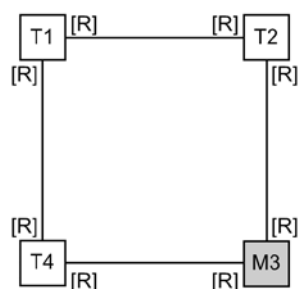
Command examples

1. `(config) # axrp 1`
`(config-axrp) # vlan-group 1 vlan-mapping 1`
`(config-axrp) # exit`

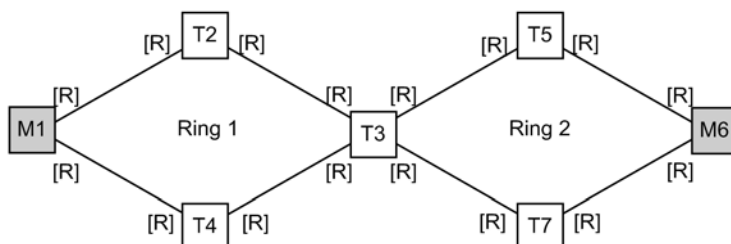
Sets VLAN mapping ID 1 for VLAN group 1.

22.1.7 Configuring modes and ring ports (for single rings and multi-ring configurations without shared links)

Figure 22-1 Single ring configuration shows a single ring configuration, and *Figure 22-2 Multi-ring configuration without shared links* shows a multi-ring configuration without shared links.

Figure 22-1 Single ring configuration

Legend: M : Master node T : Transit node
[R] : Ring port

Figure 22-2 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 a 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 22-1 Single ring configuration* and the M1 and M6 nodes in *Figure 22-2 Multi-ring configuration without shared links* correspond to this setting.

Command examples

1. `(config)# axrp 2`

```
(config-axrp)# mode master
```

```
(config-axrp)# exit
```

Sets the operation mode for ring ID 2 to master mode.

2. `(config)# interface gigabitethernet 0/1`

```
(config-if)# axrp-ring-port 2
```

```
(config-if)# exit
```

```
(config)# interface gigabitethernet 0/2
```

```
(config-if)# axrp-ring-port 2
```

```
(config-if)# exit
```

Switches to the interface mode for ports 0/1 and 0/2, and sets the target interface as the ring port for ring ID 2.

(2) Transit nodes

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 22-1 Single ring configuration*, and the T2, T3, T4, T5, and T7 nodes in *Figure 22-2 Multi-ring configuration without shared links* correspond to this setting.

Command examples

1. `(config)# axrp 2`

```
(config-axrp)# mode transit
```

```
(config-axrp)# exit
```

Sets the operating mode for ring ID 2 to transit mode.

2. `(config)# interface gigabitethernet 0/1`

```
(config-if)# axrp-ring-port 2
```

```
(config-if)# exit
```

```
(config)# interface gigabitethernet 0/2
```

```
(config-if)# axrp-ring-port 2
```

```
(config-if)# exit
```

Switches to the interface mode for ports 0/1 and 0/2, and sets the target interface as the ring port for ring ID 2.

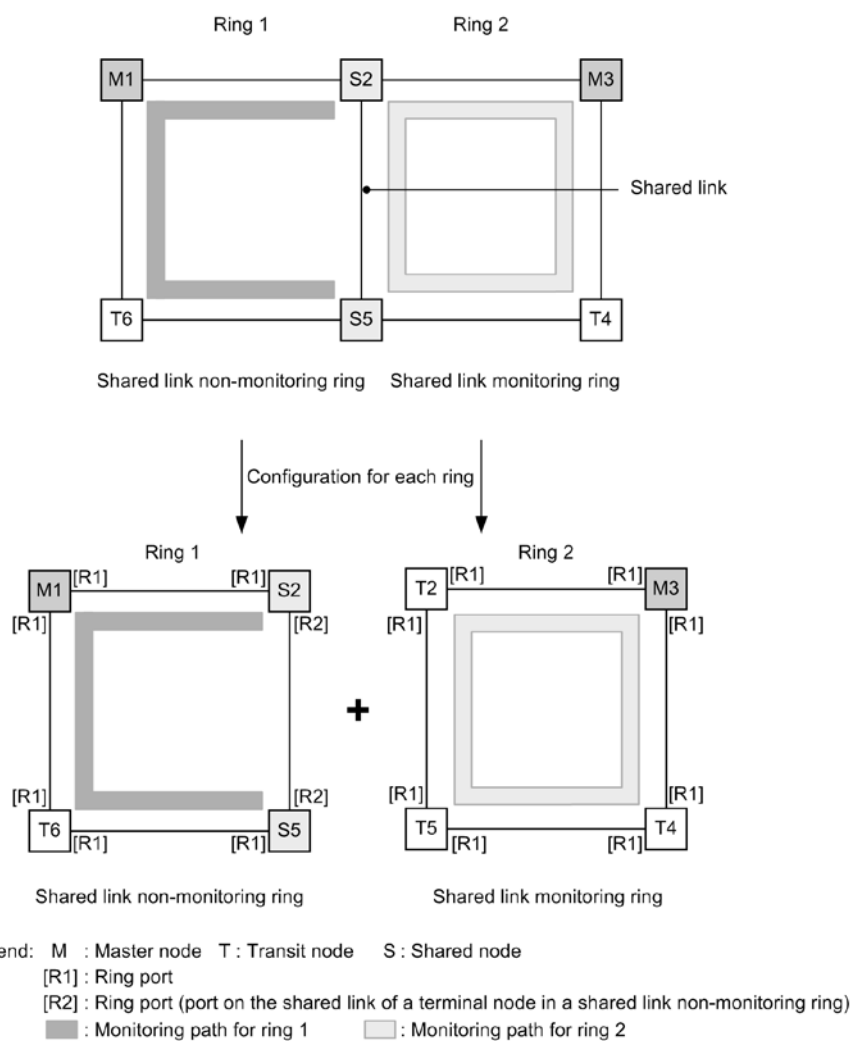
22.1.8 Configuring modes and ring ports (for multi-ring configurations with shared links)

This section describes 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 22-3 Multi-ring configuration with shared links (basic configuration)



(a) Master nodes for shared link monitoring rings

This is the same as the master node for a single ring. For details, see 22.1.7(1) *Master nodes*. The M3 node in *Figure 22-3 Multi-ring configuration 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 22.1.7(2) *Transit nodes*. The T2, T4, and T5 nodes in *Figure 22-3 Multi-ring configuration 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 22-3 Multi-ring configuration with shared links (basic configuration)* corresponds to this setting.

Command examples

1.

```
(config) # axrp 1
(config-axrp) # mode master ring-attribute rift-ring
(config-axrp) # exit
```

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 0/1
(config-if) # axrp-ring-port 1
(config-if) # exit
(config) # interface gigabitethernet 0/2
(config-if) # axrp-ring-port 1
(config-if) # exit
```

Switches to the interface mode for ports 0/1 and 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 22.1.7(2) *Transit nodes*. The T6 node in *Figure 22-3 Multi-ring configuration 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 22-3 Multi-ring configuration 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 22-3 Multi-ring configuration 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
(config-axrp) # exit
```
2.

```
(config) # interface gigabitethernet 0/1
(config-if) # axrp-ring-port 1
(config-if) # exit
```

```
(config)# interface gigabitethernet 0/2
(config-if)# axrp-ring-port 1 shared-edge
(config-if)# exit
```

Switches to the interface mode for ports 0/1 and 0/2, and sets the target interface as the ring port for ring ID 1. The **shared-edge** parameter is also set to port 0/2 as a shared link.

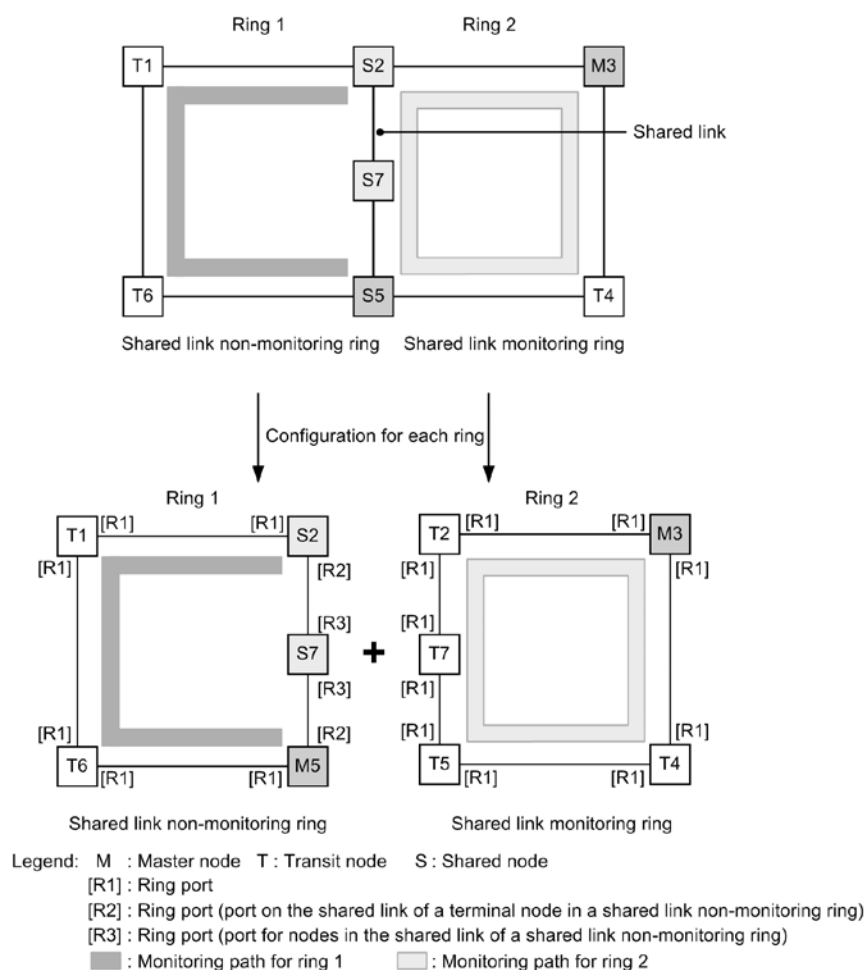
Notes

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 22-4 Multi-ring configuration with shared links (extended configuration)



(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 22-4 Multi-ring configuration 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 22-4 Multi-ring configuration 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
```

```
(config-axrp) # exit
```

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 0/1`

```
(config-if) # axrp-ring-port 1
```

```
(config-if) # exit
```

```
(config) # interface gigabitethernet 0/2
```

```
(config-if) # axrp-ring-port 1 shared-edge
```

```
(config-if) # exit
```

Switches to the interface mode for ports 0/1 and 0/2, and sets the target interface as the ring port for ring ID 1. The **shared-edge** parameter is also set to port 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 22-4 Multi-ring configuration 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 22-4 Multi-ring configuration with shared links (extended configuration)* corresponds to this setting.

Command examples

1. `(config) # axrp 1`

```
(config-axrp) # mode transit
```

```
(config-axrp) # exit
```

Sets the operating mode for ring ID 1 to transit mode.

2. `(config) # interface gigabitethernet 0/1`

```
(config-if) # axrp-ring-port 1 shared
```

```
(config-if) # exit
```

```
(config) # interface gigabitethernet 0/2
```

```
(config-if) # axrp-ring-port 1 shared
```

```
(config-if)# exit
```

Switches to the interface mode for ports 0/1 and 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.

22.1.9 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
(config-axrp)# exit
```

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
(config-axrp)# exit
```

Sets the health-check frame sending interval 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`
`(config-axrp)# exit`

Sets the health-check frame reception hold time 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`
`(config-axrp)# exit`

Sets the flush-control frame reception hold time 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 (`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 node 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`
`(config-if)# exit`

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`
`(config-axrp)# exit`
 Switches to configuration mode for ring ID 1, and sets the path switch-back suppression time to `infinity`.

22.1.10 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`
`(config-axrp)# multi-fault-detection vlan 20`
`(config-axrp)# exit`
 Switches to the configuration mode for ring ID 1, and then 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`
`(config-axrp)# multi-fault-detection mode monitor-enable backup-ring 2`
`(config-axrp)# exit`
 Switches to the configuration mode for ring ID 1, sets the monitoring mode for multi-fault monitoring to `monitor-enable`, and sets 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`
`(config-axrp)# multi-fault-detection mode transport-only`
`(config-axrp)# exit`

Switches to the configuration mode for ring ID 1, and then 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 configuration is ignored if performed for other nodes.

Command examples

1. `(config)# axrp 1`
`(config-axrp)# multi-fault-detection interval 1000`
`(config-axrp)# exit`

Switches to the configuration mode for ring ID 1, and then 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`
`(config-axrp)# exit`

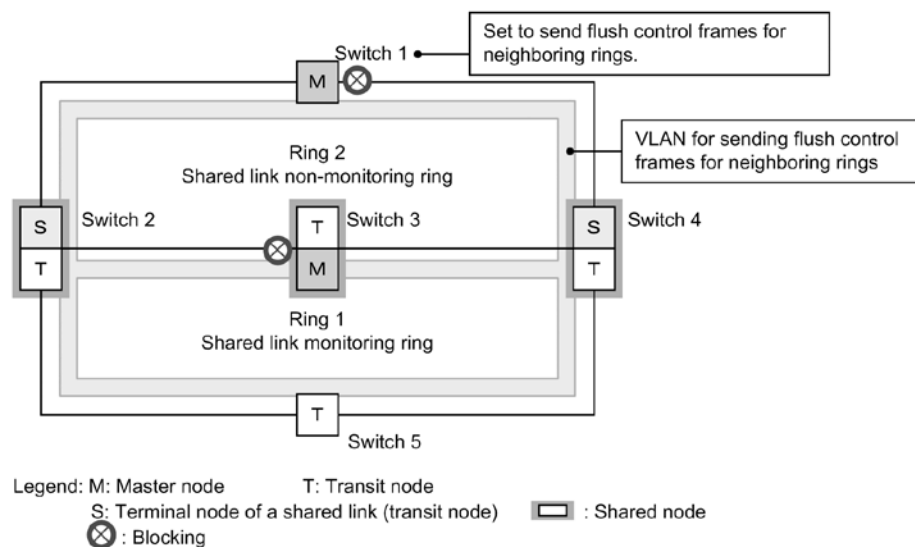
Switches to the configuration mode for ring ID 1, and then sets the reception hold time for multi-fault monitoring frames to 3000 ms.

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).

22.1.11 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 22-5 Configurations in which both ring ports of a master node are shared links**Points to note**

In a multi-ring configuration shown in *Figure 22-5 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`
`(config-axrp)# exit`

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.

22.2 Operation

22.2.1 List of operation commands

The following table describes the operation commands for the Ring Protocol.

Table 22-2 List of operation commands

Command name	Description
<code>show axrp</code>	Shows Ring Protocol information.
<code>clear axrp</code>	Clears Ring Protocol statistics.
<code>clear axrp preempt-delay</code>	Clears the path switch-back suppression status for a ring.
<code>show port</code> ^{#1}	Shows the usage status of the Ring Protocol for a port.
<code>show vlan</code> ^{#2}	Shows the usage status of the Ring Protocol for a VLAN.

#1

For details, see *13 Ethernet* in the manual *Operation Command Reference*.

#2

For details, see *16 VLAN* in the manual *Operation Command Reference*.

22.2.2 Checking Ring Protocol statuses

(1) Checking the configuration settings and operation statuses

The `show axrp` operation 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>` operation command can be used to check the status information for each ring.

The information displayed differs depending on the contents of the **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 status indicates that the required configuration command has not been obtained. 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` operation command and `show axrp detail` operation command.

Figure 22-6 Results of executing the show axrp command

```
> show axrp
```

```
Date 2012/03/02 17:08:17 UTC
```

```
Total Ring Counts: 3
```

```
Ring ID: 5
```

```
Name:
```

```
Oper State: enable
```

```
Mode: Transit
```

```
Attribute: rift-ring-edge(2)
```

```
Shared Edge Port: 64(ChGr)
```

VLAN Group ID	Ring Port	Role/State	Ring Port	Role/State
1	0/40	- /down	64(ChGr)	- /-
2	-	- /-	-	- /-

22 Settings and Operation for Ring Protocol

```
Ring ID: 10
Name:
Oper State: enable          Mode: Master      Attribute: -

VLAN Group ID  Ring Port  Role/State          Ring Port  Role/State
1              0/1        secondary/forwarding 64(ChGr)   primary/down
2              -         -/-                  -          -/-

Ring ID: 11
Name:
Oper State: enable          Mode: Transit   Attribute: rift-ring-edge(2)
Shared Edge Port: 64(ChGr)

VLAN Group ID  Ring Port  Role/State          Ring Port  Role/State
1              0/30      -/forwarding        64(ChGr)   -/-
2              -         -/-                  -          -/-

>
```

The `show axrp detail` operation command can be used to check detailed information about the ring status.

Figure 22-7 Results of executing the show axrp detail command

```
> show axrp detail

Date 2012/03/02 17:08:24 UTC
Total Ring Counts: 3

Ring ID: 5
Name:
Oper State: enable          Mode: Transit   Attribute: rift-ring-edge(2)
Shared Edge Port: 64(ChGr)
Control VLAN ID: 5
Health Check Interval (msec): 500
Forwarding Shift Time (sec): 10
Last Forwarding: flush request receive

VLAN Group ID: 1
VLAN ID: 50-99
Ring Port: 0/40            Role: -          State: down
Ring Port: 64(ChGr)       Role: -          State: -

VLAN Group ID: 2
VLAN ID: -
Ring Port: -               Role: -          State: -
Ring Port: -               Role: -          State: -

Ring ID: 10
Name:
Oper State: enable          Mode: Master      Attribute: -
Control VLAN ID: 10        Ring State: fault
Health Check Interval (msec): 200
Health Check Hold Time (msec): 500
Flush Request Counts: 3

VLAN Group ID: 1
VLAN ID: 50-99
Ring Port: 0/1            Role: secondary   State: forwarding
Ring Port: 64(ChGr)       Role: primary     State: down

VLAN Group ID: 2
```

```

VLAN ID: -
Ring Port: -           Role: -           State: -
Ring Port: -           Role: -           State: -

```

Last Transition Time: 2012/03/02 17: 07: 45

Fault Counts	Recovery Counts	Total	Flush Request Counts
32	31	327	

Ring ID: 11

Name:

Oper State: enable Mode: Transit Attribute: rift-ring-edge(2)

Shared Edge Port: 64(ChGr)

Control VLAN ID: 11

Health Check Interval (msec): 500

Forwarding Shift Time (sec): 10

Last Forwarding: flush request receive

VLAN Group ID: 1

VLAN ID: 50-99

Ring Port: 0/30 Role: - State: forwarding

Ring Port: 64(ChGr) Role: - State: -

VLAN Group ID: 2

VLAN ID: -

Ring Port: - Role: - State: -

Ring Port: - Role: - State: -

>

When the multi-fault monitoring functionality is applied, the **show axrp detail** operation command can be used to check information about the multi-fault monitoring status.

Figure 22-8 Results of executing the show axrp detail operation command when the multi-fault monitoring functionality is applied

> show axrp 10 detail

Ring ID: 10

Name:

Oper State: enable Mode: Master Attribute: -

Control VLAN ID: 10 Ring State: fault

Health Check Interval (msec): 200

Health Check Hold Time (msec): 500

Flush Request Counts: 3

VLAN Group ID: 1

VLAN ID: 50-99

Ring Port: 0/1 Role: secondary State: forwarding

Ring Port: 64(ChGr) Role: primary State: down

VLAN Group ID: 2

VLAN ID: -

Ring Port: - Role: - State: -

Ring Port: - Role: - State: -

Last Transition Time: 2012/03/02 17: 09: 45

Fault Counts	Recovery Counts	Total	Flush Request Counts
32	31	347	

Multi Fault Detection State: fault

Mode: monitoring Backup Ring ID: 11

Control VLAN ID: 999

Multi Fault Detection Interval (msec): 2000

Multi Fault Detection Hold Time (msec): 6000

>

23. Using the Ring Protocol with Spanning Tree Protocols/GSRP

This chapter describes how to use the Ring Protocol on the same device as a Spanning Tree Protocol or GSRP.

23.1 Using the Ring Protocol with

23.2 Using the Ring Protocol with GSRP

23.3 Virtual link configuration

23.4 Virtual link operation

23.1 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 *16.3 Compatibility between Layer 2 switch functionality and other functionality*. For details about the Ring Protocol, see *21 Description of the Ring Protocol*.

23.1.1 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 show examples of the Ring Protocol being used with Spanning Tree Protocols for a single ring configuration and a multi-ring configuration. Switches A/G/I, B/F/J, and C/D/K each comprise a Spanning Tree topology. The Ring Protocol and Spanning Tree Protocols are used at the same time for Switches A to D and F to G.

Figure 23-1 Example using the Ring Protocol and Spanning Tree Protocols together (single ring configuration)

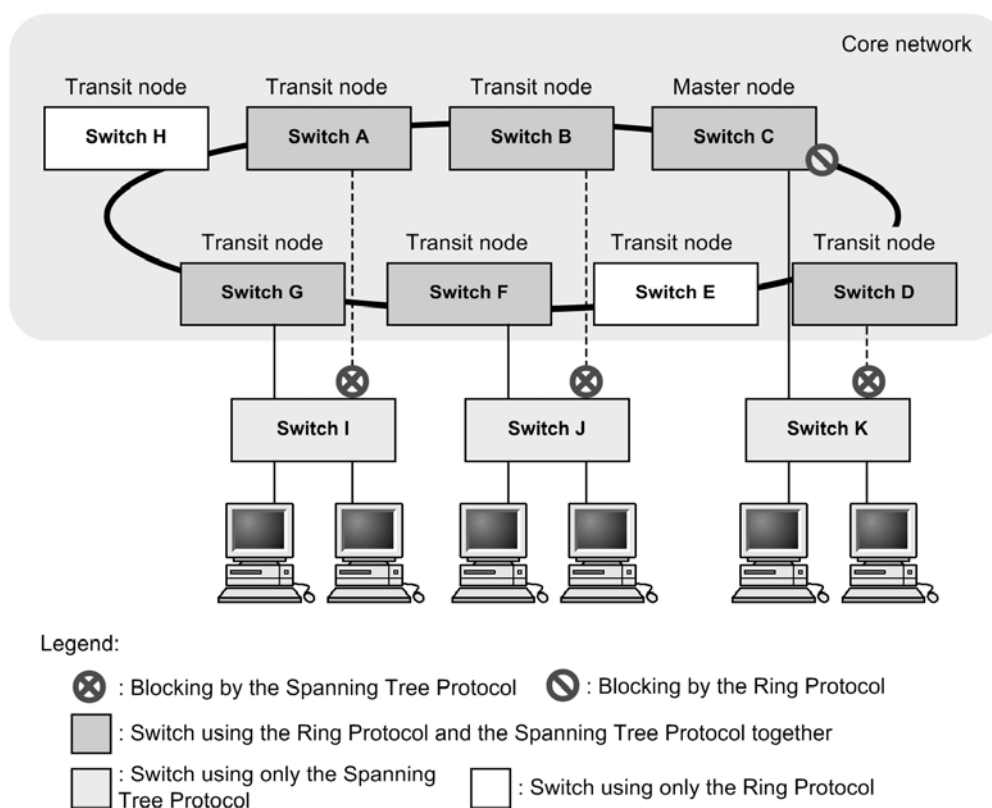
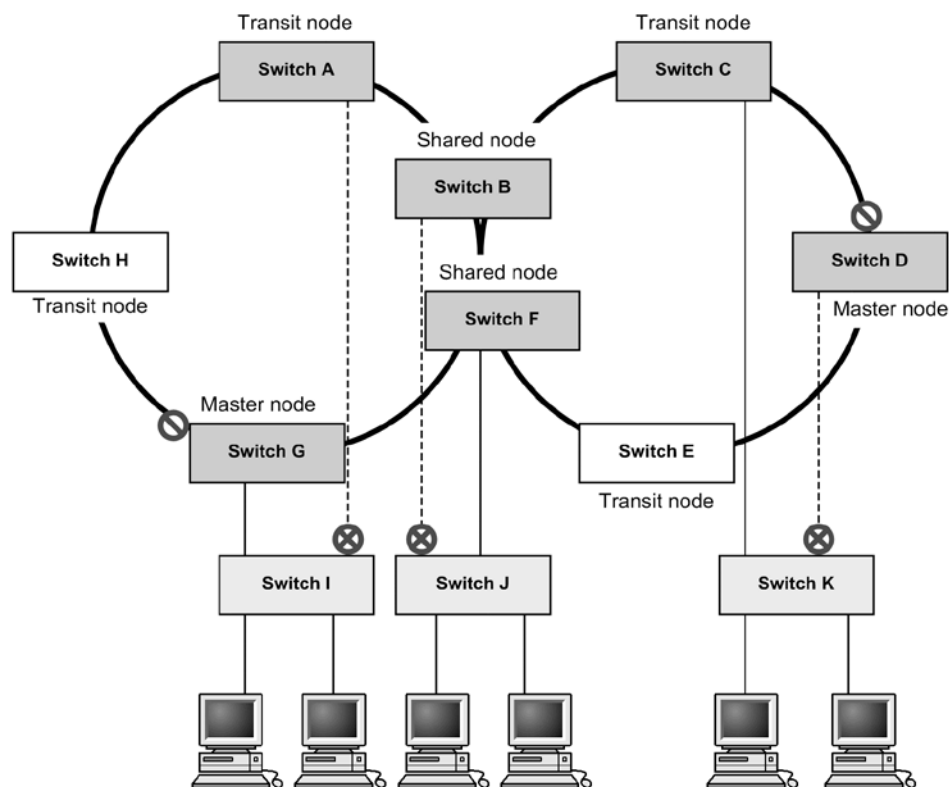







Figure 23-2 Example using the Ring Protocol and Spanning Tree Protocols together (multi-ring configuration)



Legend:

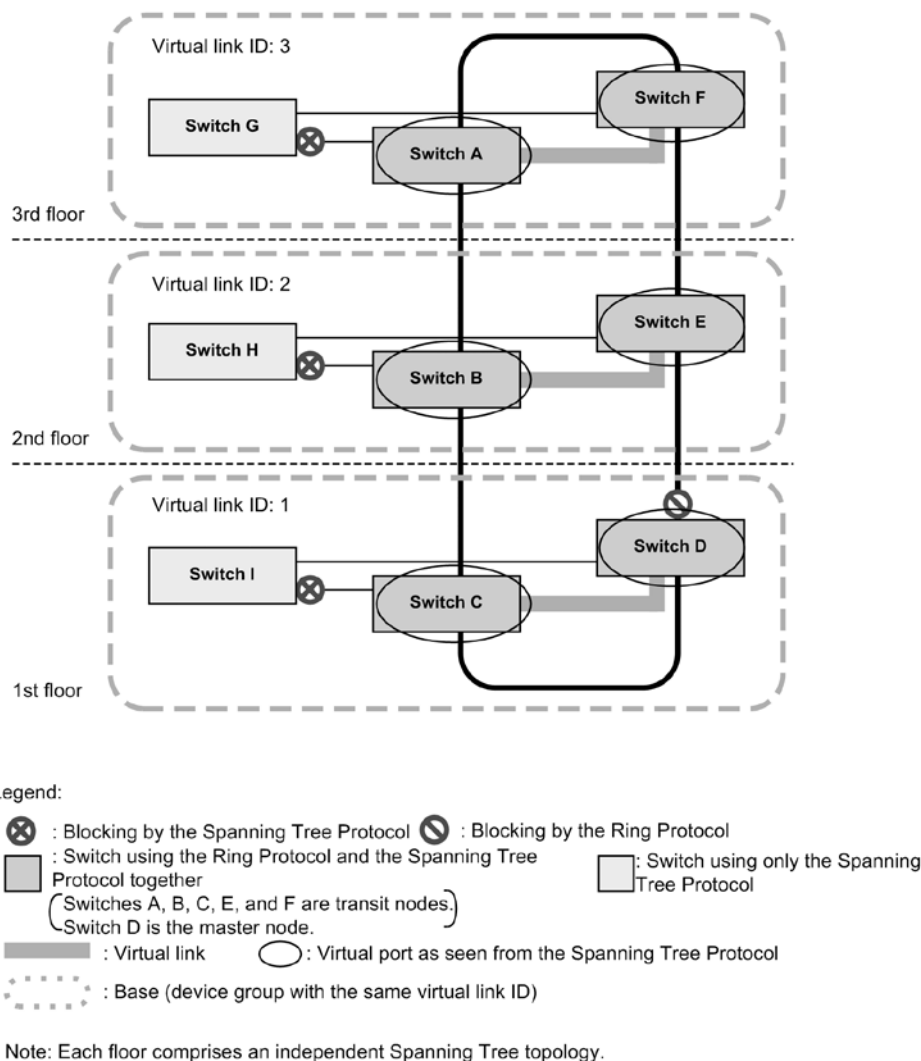
-  : Blocking by the Spanning Tree Protocol  : Blocking by the Ring Protocol
 : Switch using the Ring Protocol and the Spanning Tree Protocol together
 : Switch using only the Spanning Tree Protocol  : Switch using only the Ring Protocol

23.1.2 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 shows an overview of virtual links.

Figure 23-3 Overview of virtual links

(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 23-1 Value set for bridge priority

Configuration items	Related configuration	Initial value
Bridge priority	<code>spanning-tree single priority</code> <code>spanning-tree vlan priority</code> <code>spanning-tree mst root priority</code>	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 23-2 Value set for virtual link ports

Configuration items	Related configuration	Initial value
Link type	<code>spanning-tree link-type</code>	<code>point-to-point</code>
Port priority	<code>spanning-tree single priority</code> <code>spanning-tree vlan priority</code> <code>spanning-tree mst root priority</code>	0
Path cost	<code>spanning-tree cost</code> <code>spanning-tree single cost</code> <code>spanning-tree vlan cost</code> <code>spanning-tree mst cost</code>	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 the `Blocking` status.

- Switch startup (including restarting of the switch)

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, the

Switch temporarily sets 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 23-3 Settings when ports other than ring ports are temporarily in the Blocking status

Configuration items	Related configuration	Initial values
Reception hold time for Ring Protocol flush control frames	<code>forwarding-shift-time</code>	10 seconds or less (default value of 10 seconds)
Spanning Tree control frame sending interval	<code>spanning-tree single hello-time</code> <code>spanning-tree vlan hello-time</code> <code>spanning-tree mst hello-time</code>	2 seconds or less (default value of 2 seconds)

23.1.3 Compatibility with various Spanning Tree Protocols

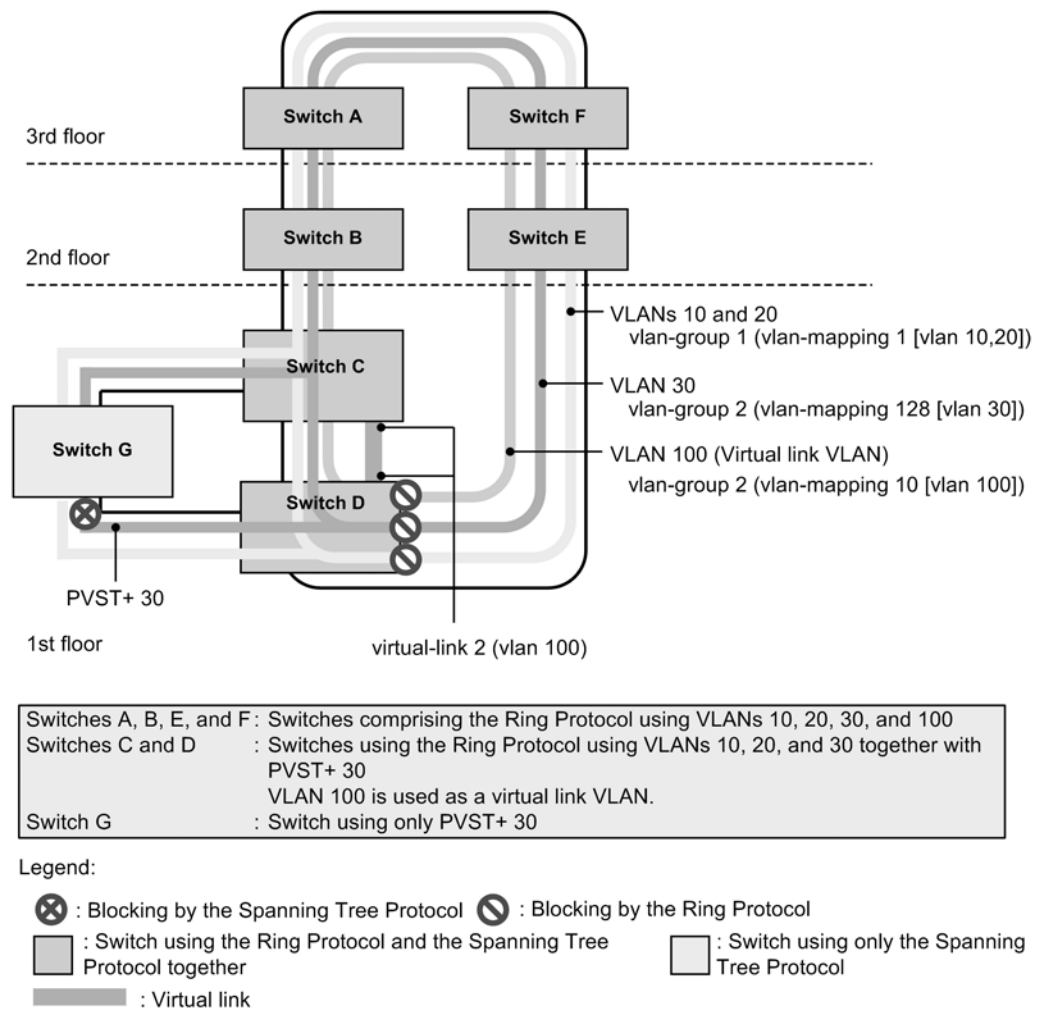
(1) Compatibility with PVST+

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 blocking 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.

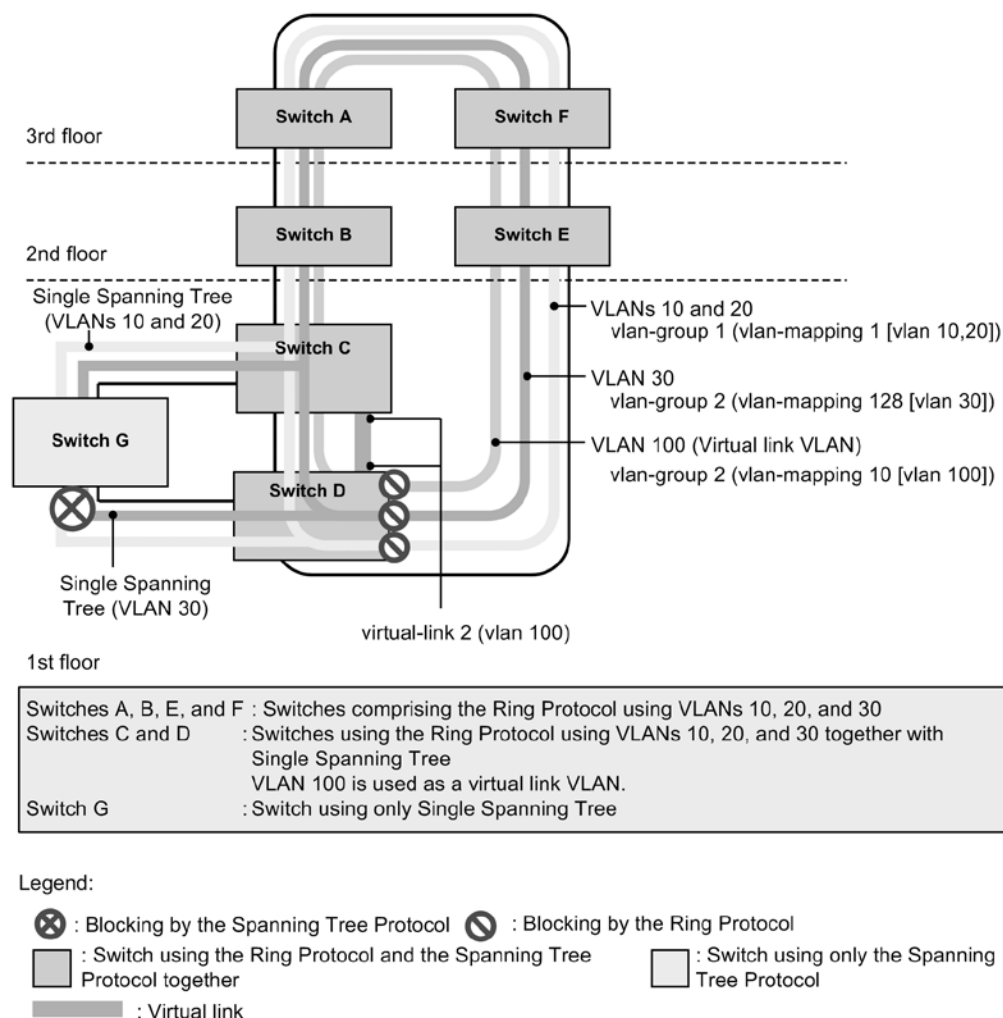
Figure 23-4 Configuration using PVST+ and the Ring Protocol together

(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.

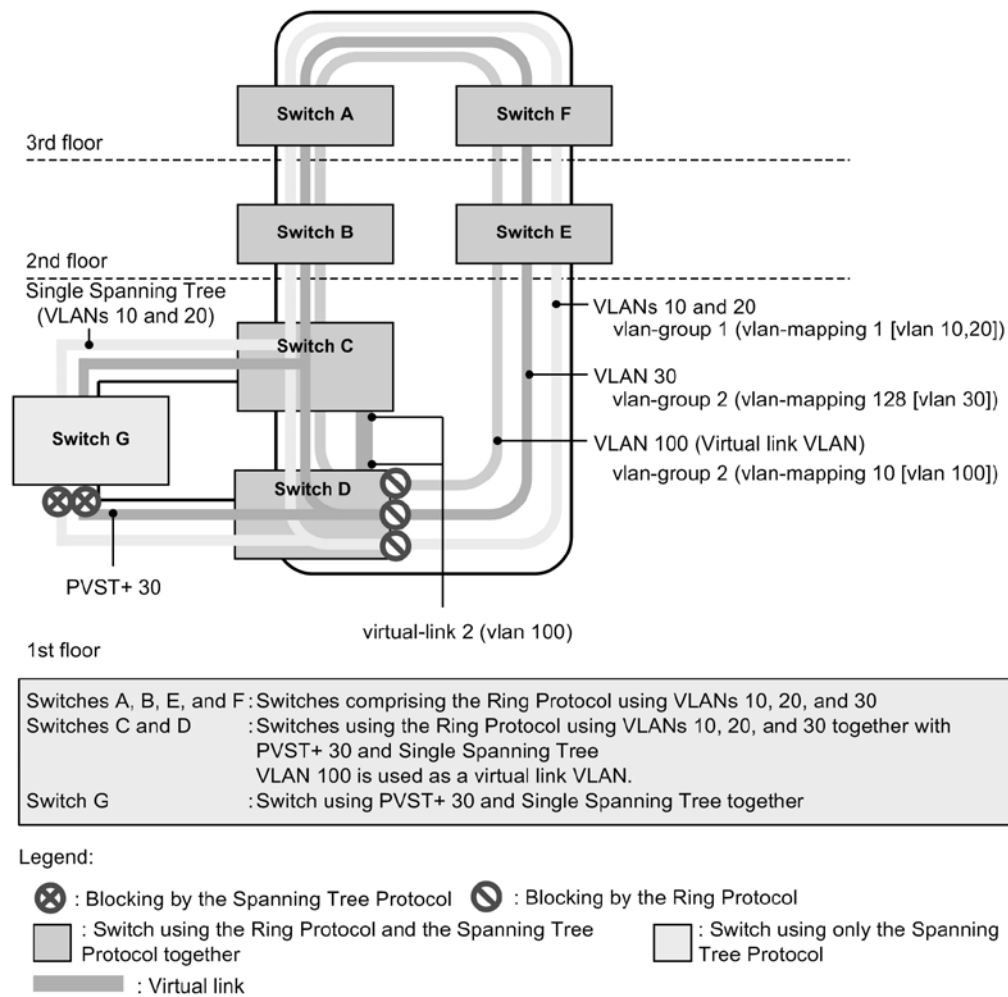
The figure below shows a configuration in which Single Spanning Tree and the Ring Protocol are used together. In the figure, Single Spanning Tree is set for switches C, D, and G, and two VLAN groups for the Ring Protocol are set for switches A, B, C, D, E, and F. Each topology for Single Spanning Tree 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 23-5 Configuration using Single Spanning Tree and the Ring Protocol together

(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 23-6 Configuration using Single Spanning Tree, PVST+, and the Ring Protocol together

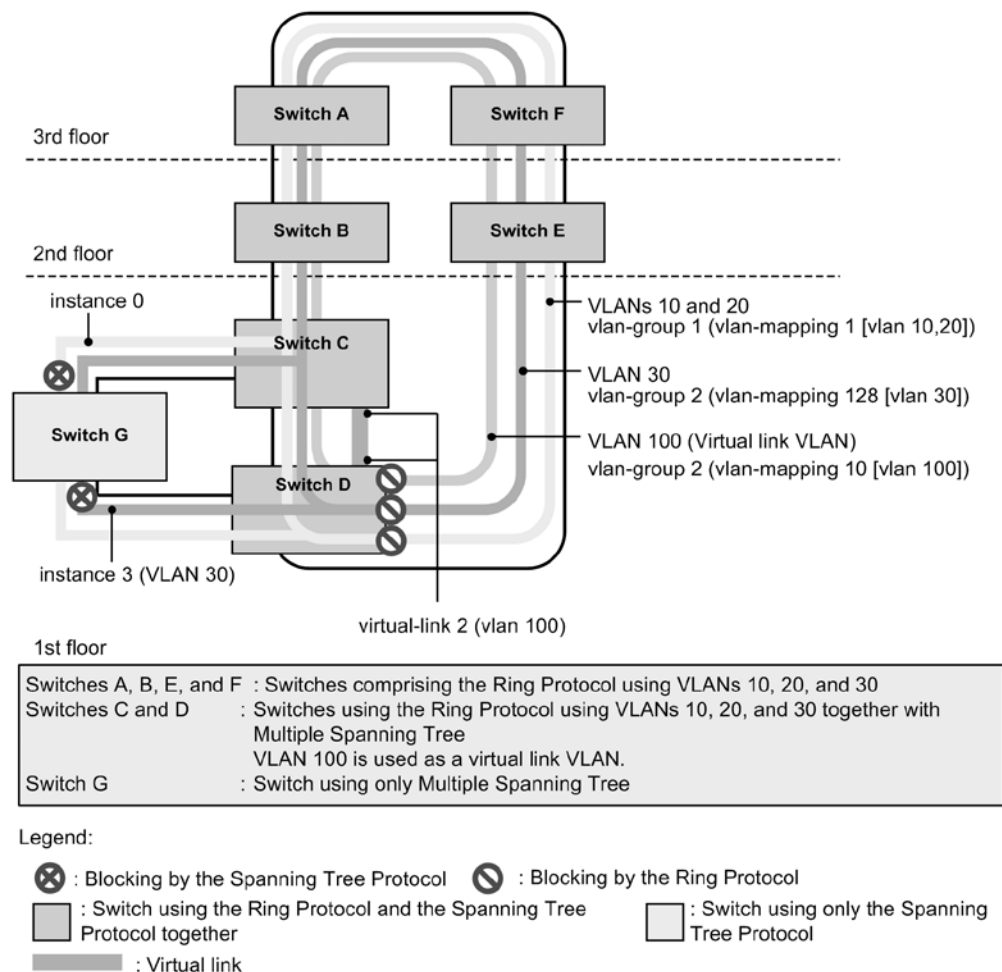
(4) Compatibility with Multiple Spanning Tree

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 23-7 Configuration using Multiple Spanning Tree and the Ring Protocol together

(5) VLANs that cannot be run together

1. 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.

2. 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.

3. 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.

4. 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.

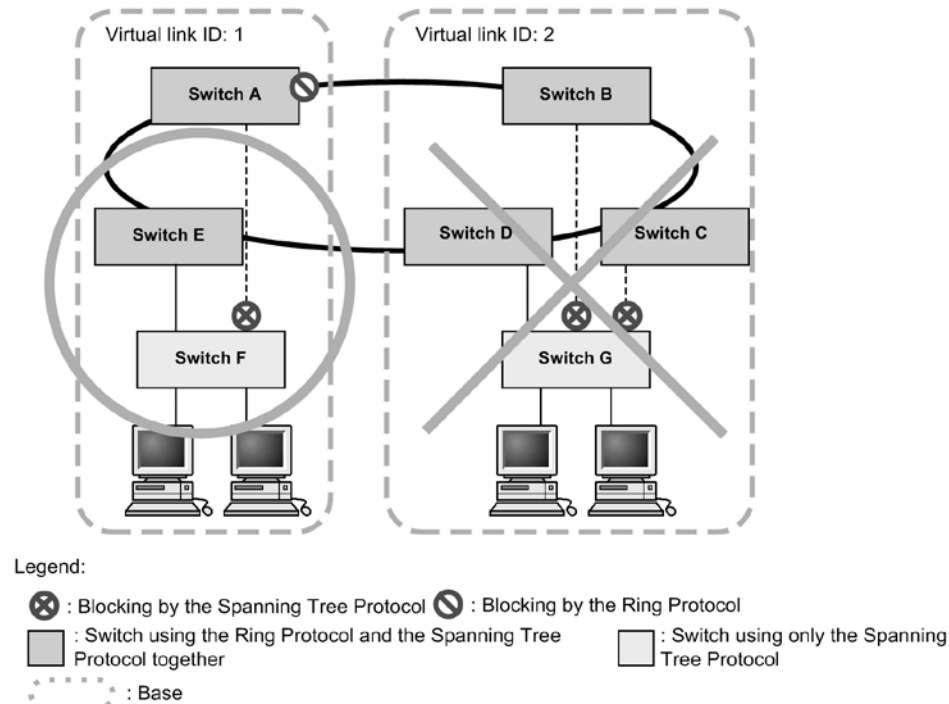
23.1.4 Prohibited configurations

(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 23-8 Prohibited configuration for virtual links



23.1.5 Notes on using 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 blocking 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 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 switch restart on transit nodes

When restarting the switch, 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 the `Blocking` status, preventing communication.

23.2 Using the Ring Protocol with GSRP

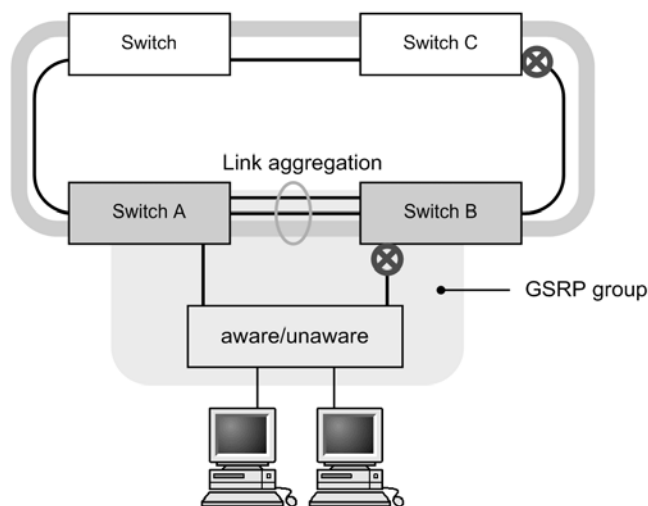
The Switch cannot use the Ring Protocol concurrently with GSRP. However, the Switch can be included in the ring configuration that is configured by switches that use GSRP with the Ring Protocol (for example, AX2400S/3600S/6700S series switches).

23.2.1 Operational overview

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 switchover 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.

The following figure shows an example of the Ring Protocol and GSRP being used together.

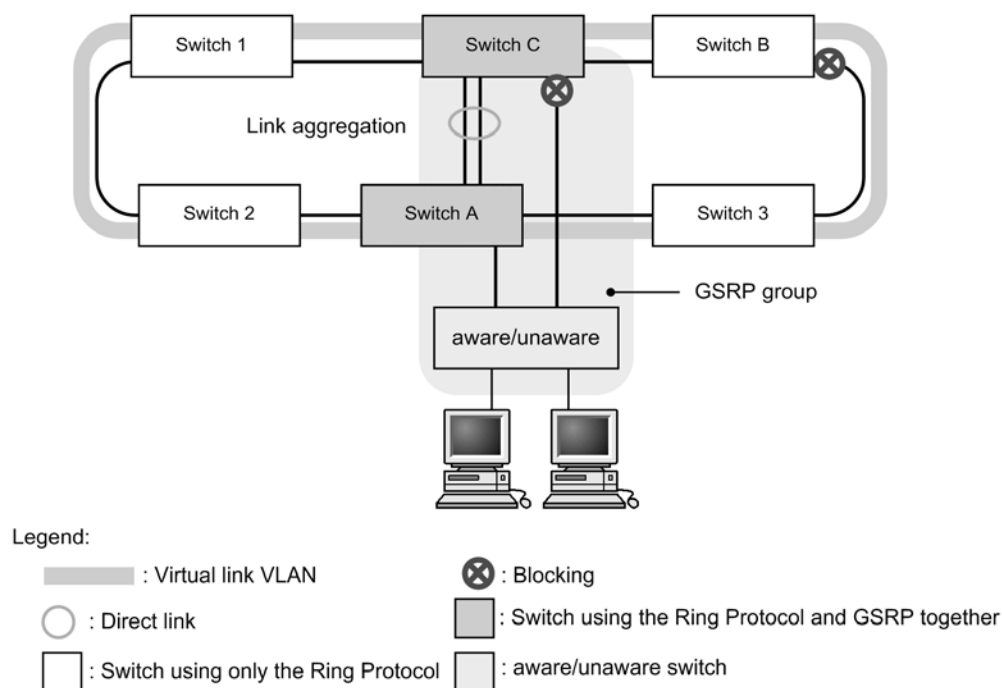
Figure 23-9 Example of positioning of Switches when the Ring Protocol and GSRP are used together (when direct links are used on a ring network)



Legend:

- | | |
|---------------------------------------|--|
| : Virtual link VLAN | : Blocking |
| : Direct link | : Switch using the Ring Protocol and GSRP together |
| : Switch using only the Ring Protocol | : aware/unaware switch |

Figure 23-10 Example of positioning of Switches when the Ring Protocol and GSRP are used together (when direct links are not used on a ring network)



The Switches only perform forwarding of virtual link control frames described below and clearing of the MAC address table. For details about operations when using the Ring Protocol together with GSRP and about virtual links, see the manuals for AX series switches (such as AX2400S, AX3600S, and AX6700S series switches).

(1) Forwarding of virtual link control frames of GSRP

As is the case when two switches that use both the Ring Protocol and Spanning Tree Protocols are connected (as shown above), a virtual link is established between two switches on a ring network that use both the Ring Protocol and GSRP. A virtual link VLAN that is set on the ring network is used to send and receive virtual link control frames. A VLAN belonging to the data transfer VLAN group on the ring ports is used as the virtual VLAN.

The virtual link control frame sent from the GSRP switch are forwarded by the switches (including the Switches) on the ring network.

(2) Clearing MAC address tables during GSRP network switching

In a network using both the Ring Protocol and GSRP, the MAC address tables of the switches configuring the ring network need to be cleared when path-switching occurs in the GSRP network. If these MAC address tables are not cleared, communication might not be immediately restored. When a Switch becomes the GSRP master, the Switch sends ring-network flush control frames on the virtual link VLAN configured on the ring network to clear the MAC address tables of the devices on the ring network.

The switches (including the Switch) on the ring network receive the flush control frames sent from the GSRP master, and then the switches clear their MAC address tables.

23.3 Virtual link configuration

Virtual links are set to use the Ring Protocol and Spanning Tree Protocols on the same switch.

Note that virtual link setting for using Ring Protocol and GSRP together is configured on the GSRP switches (AX2400S, AX3600S, and AX6700S series switches). Therefore, the setting is unnecessary for the Switch.

23.3.1 List of configuration commands

The following table describes the commands used to configure a virtual link.

Table 23-4 List of configuration commands

Command name	Description
<code>axrp virtual-link</code>	Sets a virtual link ID.

23.3.2 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. Make sure that you set the same virtual link ID and virtual link VLAN for partner switches 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.

23.3.3 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`
`(config-axrp)# exit`

Sets VLAN mapping IDs 1 and 2 for VLAN group 1.

23.3.4 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`
`(config-mst) # exit`
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.

23.4 Virtual link operation

23.4.1 List of operation commands

The following table describes the operation commands for virtual links.

Table 23-5 List of operation commands

Command name	Description
<code>show spanning-tree</code>	Shows the application status of virtual links in a Spanning Tree Protocol.

23.4.2 Checking the status of virtual links

Use the `show spanning-tree` operation command to check virtual link information. Check **Port Information** to confirm the existence of virtual link ports.

The following figure shows the results of executing the `show spanning-tree` operation command.

Figure 23-11 Results of executing show spanning-tree

```
> show spanning-tree

Date 2012/02/27 06:39:38 UTC
VLAN 100 PVST+ Spanning Tree: Enabled Mode: PVST+
  Bridge ID      Priority: 100      MAC Address: 0012.e2f0.0008
  Bridge Status: Designated
  Root Bridge ID Priority: 100      MAC Address: 0012.e2f0.0001
  Root Cost: 1
  Root Port: 0/1-2(VL: 250)          ... 1
Port Information
  VL: 250    Up    Status: Forwarding Role: Root    -    ... 1

>
1.    VL indicates a virtual link ID.
```

24. Description of IGMP Snooping and MLD Snooping

IGMP snooping and MLD snooping are functions that use Layer 2 switches to control multicast traffic within a VLAN. This chapter describes IGMP snooping and MLD snooping.

24.1 Overview of IGMP snooping and MLD snooping

24.2 Functionality supported for IGMP snooping and MLD snooping

24.3 IGMP snooping

24.4 MLD snooping

24.5 Notes on IGMP snooping and MLD snooping usage

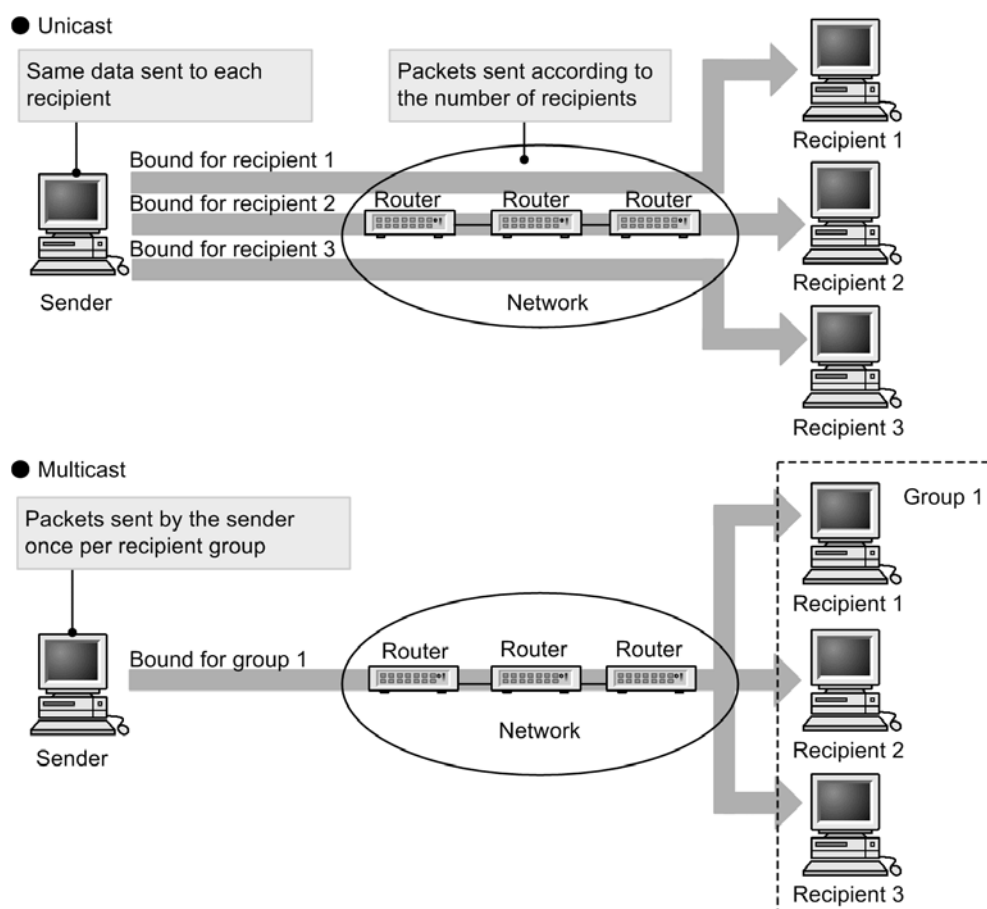
24.1 Overview of IGMP snooping and MLD snooping

This section describes an overview of multicast, IGMP snooping, and MLD snooping.

24.1.1 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 shows an overview of multicast.

Figure 24-1 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 24-1 Multicast group address

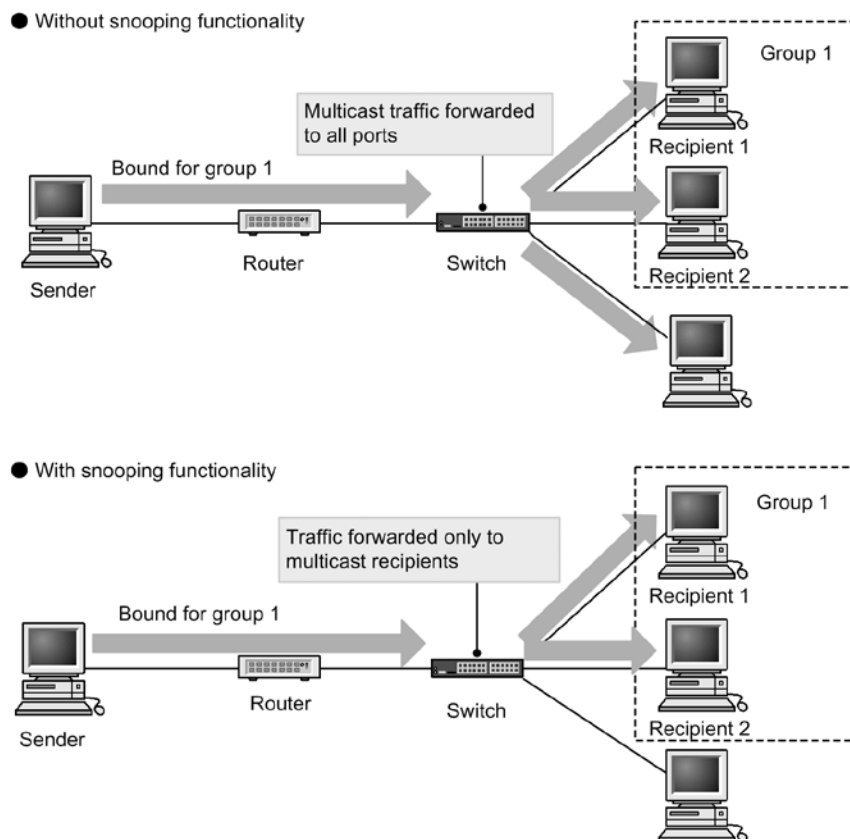
Protocol	Address range
IPv4	224.0.0.0 to 239.255.255.255
IPv6	IPv6 addresses whose highest 8 bits are ff (in hexadecimal)

24.1.2 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 shows an overview of IGMP snooping and MLD snooping.

Figure 24-2 Overview of IGMP snooping and MLD snooping



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 a router and a host by using IGMP on IPv4 networks and MLD on IPv6 networks. The Switch detects packets sent from the host, indicating group participation and leave, to learn the connected ports to which multicast traffic should be forwarded.

24.2 Functionality supported for IGMP snooping and MLD snooping

The following table describes the IGMP snooping and MLD snooping functionality supported by the Switch.

Table 24-2 Supported functionality

Item		Support	Remarks
Interface type		Full Ethernet support Only Ethernet V2 frame formats	--
Supported IGMP version Supported MLD version		IGMP: Versions 1, 2, and 3 MLD: Versions 1, and 2	--
Learning for this functionality	IPv4	0100.5e00.0000 to 0100.5e7f.ffff	For details, see RFC 1112.
MAC address range	IPv6	3333.0000.0000 to 3333.ffff.ffff	For details, see RFC 2464.
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 IGMP Leave messages, or IGMPv3 Report (leave request) messages for which the multicast address record type is CHANGE_TO_INCLUDE_MODE	--

Legend: --: Not applicable

24.3 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.

IGMP snooping uses the MAC address control method to control forwarding for multicast traffic.

24.3.1 MAC address control method

(1) MAC address learning

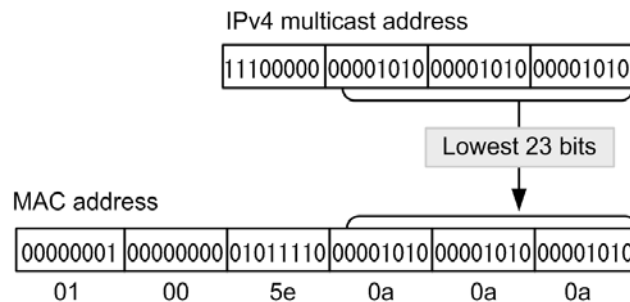
For VLANs for which IGMP snooping is set, multicast MAC addresses are dynamically learned when IGMP messages are received. The learned multicast MAC addresses are registered to the MAC address table.

(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. In Layer 2 forwarding, these addresses are treated as packets bound for the same MAC address. The following figure shows the correspondence between IPv4 multicast addresses and MAC addresses.

Figure 24-3 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 IGMP Leave message is received.

Group-Specific Query messages are sent from the Switch to the port that received IGMP Leave messages, twice every second (Group-Specific Query messages are sent only 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 the ports in the VLAN, the entry itself is deleted.

When IGMP instant leave is used and an IGMP 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 sent only 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.

Notes

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 packets

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 (1)(a) *Registering entries* 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.

24.3.2 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 routers and hosts, IGMP messages are accepted by routers and hosts. The Switch forwards IGMP messages

as shown in the following table.

Table 24-3 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 IGMP Leave message, the IGMP Leave message is not forwarded regardless of the querier settings.

Table 24-4 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.

24.3.3 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.

24 Description of IGMP Snooping and MLD Snooping

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.

24.3.4 IGMP instant leave

IGMP instant leave stops multicast communication to the corresponding ports as soon as an IGMP 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.

24.4 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.

MLD snooping uses the MAC address control method to control forwarding for multicast traffic.

24.4.1 MAC address control method

(1) MAC address learning

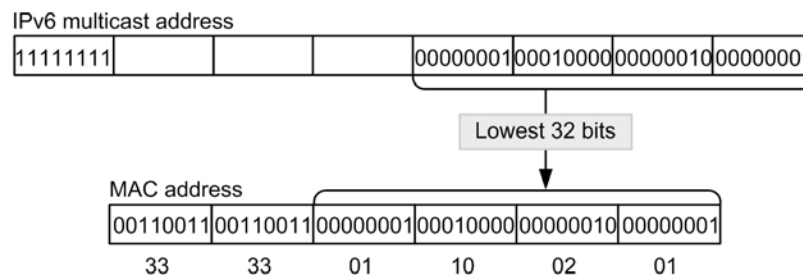
For VLANs for which MLD snooping is set, multicast MAC addresses are dynamically learned when MLD messages are received. The learned multicast MAC addresses are registered to the MAC address table.

(a) Registering entries

When an MLDv1 Report message or an 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 24-4 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 sent only 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 sent only 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 whose multicast address record type of **BLOCK_OLD_SOURCES** is received, Group-Specific Query messages are sent and entry deletion processing is performed only when a querier is 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.

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.

(2) Layer 2 forwarding for IPv6 multicast packets

Layer 2 forwarding within VLANs receiving IPv6 multicast packets is performed based on MAC addresses, just as with 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.

24.4.2 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 24-5 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 24-6 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.	
	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.

24.4.3 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 a Query message every 125 seconds.

In order to use the MLD querier functionality, the source IP address of an MLD Query message 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 MLD 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.

24.5 Notes on IGMP snooping and MLD snooping usage

(1) Notes on use with other functionality

For details, see *16.3 Compatibility between Layer 2 switch functionality and other functionality*.

(2) Flooding control packets

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 multicast MAC addresses.

Table 24-7 Control packet flooding

Protocol	Address range
IGMP snooping	224.0.0.0 to 224.0.0.255
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 24-8 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

Protocol	Multicast group address
	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
	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. In addition, in this type of configuration, the IGMP snooping or MLD snooping functionality must be enabled for each Layer 2 switch (a port is connected to switches that support the snooping functionality).

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

The following action needs to be performed when the Switch is connected to an IGMPv3 host:

- 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

To connect an MLDv2 host to a Switch, connect an MLDv2 router and set an IP address so that the target router becomes the representative querier. If the representative querier is an MLDv1 router, the network becomes an MLDv1 mode network.

Also, operation must be in an environment where MLDv2 messages from an MLDv2 host are not fragmented.

(6) IGMP instant leave

When IGMP instant leave is used and an IGMP 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.

25. 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 describes how to set and use IGMP snooping and MLD snooping.

25.1	Configuration of IGMP snooping
------	--------------------------------

25.2	IGMP snooping operation
------	-------------------------

25.3	Configuration of MLD snooping
------	-------------------------------

25.4	MLD snooping operation
------	------------------------

25.1 Configuration of IGMP snooping

25.1.1 List of configuration commands

The following table describes the configuration commands for IGMP snooping.

Table 25-1 List of configuration commands

Command name	Description
<code>ip igmp snooping</code> (global)	Suppresses IGMP snooping functionality for the Switch when <code>no ip igmp snooping</code> is set.
<code>ip igmp snooping</code> (interface)	Sets IGMP snooping functionality for the specified interface.
<code>ip igmp snooping fast-leave</code>	Sets IGMP instant leave.
<code>ip igmp snooping mrouter</code>	Sets IGMP multicast router ports.
<code>ip igmp snooping querier</code>	Sets IGMP querier functionality.

25.1.2 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`
`(config-if)# exit`

Switches to the VLAN interface configuration mode for VLAN 2, and enables IGMP snooping functionality.

25.1.3 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 in the VLAN interface configuration mode for the corresponding VLAN.

Command examples

1. `(config)# interface vlan 2`
`(config-if)# ip igmp snooping querier`
`(config-if)# exit`

Enables IGMP querier functionality.

Notes

This setting is enabled only if an IPv4 address is set for the target interface.

25.1.4 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 in the VLAN interface configuration mode for the corresponding VLAN. In the example below, a multicast router is connected to the Ethernet interface on port 0/1 in the target VLAN.

Command examples

1.

```
(config)# interface vlan 2
(config-if)# ip igmp snooping mrouter interface gigabitethernet 0/1
(config-if)# exit
```

Specifies the multicast router port for the corresponding interface.

Notes

If you specify a port number belonging to a port channel interface for a multicast router port, no operation is performed.

25.2 IGMP snooping operation

25.2.1 List of operation commands

The following table describes the operation commands for IGMP snooping.

Table 25-2 List of operation commands

Command name	Description
<code>show igmp-snooping</code>	Shows IGMP snooping information.
<code>clear igmp-snooping</code>	Clears all of the information regarding IGMP snooping.

25.2.2 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` operation command to check that the settings related to IGMP snooping are correct.

Figure 25-1 Displayed status for IGMP snooping settings

```
> show igmp-snooping

Date 2011/02/23 14:21:03 UTC
VLAN counts: 3
VLAN: 3253
  IP Address: 192.168.53.100      Querier: enable
  IGMP querying system: 192.168.53.100
  Querier version: V3
  Fast-leave: Off
  Port(4): 0/13-16
  Mrouter-port: 0/13-16
  Group counts: 3
VLAN: 3254
  IP Address: 192.168.54.100      Querier: disable
  IGMP querying system:
  Querier version: V2
  Fast-leave: Off
  Port(4): 0/17-20
  Mrouter-port: 0/17-20
  Group counts: 3
VLAN: 3255
  IP Address: 192.168.55.100      Querier: disable
  IGMP querying system:
  Querier version: V3
  Fast-leave: Off
  Port(4): 0/21-24
  Mrouter-port: 0/21-24
  Group counts: 3

>
```

(2) Check during operation

Execute the following command to check the status of IGMP snooping during operation.

- Use the `show igmp-snooping group` operation command to check learned MAC

addresses, IPv4 multicast addresses forwarded within a VLAN, and the status of the destination port list.

Figure 25-2 Results of executing show igmp-snooping group

```
> show igmp-snooping group
```

Date 2011/02/23 14:21:41 UTC

Total Groups: 9

VLAN counts: 3

VLAN 3253 Group counts: 3

Group Address	MAC Address	Version	Mode
230.0.0.11	0100.5e00.000b	V3	INCLUDE
Port-list: 0/13			
230.0.0.10	0100.5e00.000a	V2, V3	EXCLUDE
Port-list: 0/13			
230.0.0.12	0100.5e00.000c	V1, V2, V3	EXCLUDE
Port-list: 0/13			

VLAN 3254 Group counts: 3

Group Address	MAC Address	Version	Mode
230.0.0.34	0100.5e00.0022	V1	-
Port-list: 0/17			
230.0.0.33	0100.5e00.0021	V2	-
Port-list: 0/17			
230.0.0.32	0100.5e00.0020	V3	EXCLUDE
Port-list: 0/17			

VLAN 3255 Group counts: 3

Group Address	MAC Address	Version	Mode
230.0.0.24	0100.5e00.0018	V1, V2	-
Port-list: 0/21			
230.0.0.23	0100.5e00.0017	V1, V3	EXCLUDE
Port-list: 0/21			
230.0.0.22	0100.5e00.0016	V2, V3	EXCLUDE
Port-list: 0/21			

```
>
```

- Use the `show igmp-snooping port` operation command to check the participation group display example for each port.

Figure 25-3 Results of executing show igmp-snooping port

```
> show igmp-snooping port 0/13
```

Date 2011/02/23 14:23:02 UTC

Port 0/13 VLAN counts: 1

VLAN: 3253 Group counts: 3

Group Address	Last Reporter	Uptime	Expires
230.0.0.11	192.168.53.17	02:15	03:37
230.0.0.10	192.168.53.16	02:15	03:37
230.0.0.12	192.168.53.18	02:15	03:37

```
>
```

25.3 Configuration of MLD snooping

25.3.1 List of configuration commands

The following table describes the configuration commands for MLD snooping.

Table 25-3 List of configuration commands

Command name	Description
<code>ipv6 mld snooping</code> (global)	Suppresses MLD snooping functionality for a Switch when <code>no ipv6 mld snooping</code> is set.
<code>ipv6 mld snooping</code> (interface)	Sets MLD snooping functionality for the specified interface.
<code>ipv6 mld snooping mrouter</code>	Sets MLD multicast router ports.
<code>ipv6 mld snooping querier</code>	Sets MLD querier functionality.
<code>ipv6 mld snooping source</code>	Sets the source IP address of an MLD Query message sent from the Switches.

25.3.2 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`
`(config-if)# exit`

Switches to the VLAN interface configuration mode for VLAN 2, and enables MLD snooping functionality.

25.3.3 Configuring 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)# interface vlan 2`
`(config-if)# ipv6 mld snooping querier`
`(config-if)# exit`

Enables MLD querier functionality.

Notes

This setting is enabled only if the source IP address of an MLD Query message is set for the target interface.

25.3.4 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 Ethernet interface on port 0/1 within the target VLAN.

Command examples

1.

```
(config)# interface vlan 2
(config-if)# ipv6 mld snooping mrouter interface gigabitethernet 0/1
(config-if)# exit
```

Specifies the multicast router port for the corresponding interface.

Notes

If you specify a port number belonging to a port channel interface for a multicast router port, no operation is performed.

25.3.5 Configuring the source IP address for MLD Query messages

Points to note

In order to use the MLD querier functionality, the source IP address of an MLD Query message sent from a switch must be set. Specify the settings below in the VLAN interface configuration mode for the VLAN in which the MLD querier functionality is used.

Command examples

1.

```
(config)# interface vlan 2
(config-if)# ipv6 mld snooping source fe80::1
(config-if)# exit
```

Specifies **fe80::1** for the source IP address of an MLD Query message for the target interface.

Notes

1. The configured settings are applied only to the source IP address of an MLD Query message.
2. Specify an IPv6 link-local address for the source address.

25.4 MLD snooping operation

25.4.1 List of operation commands

The following table describes the operation commands for MLD snooping.

Table 25-4 List of operation commands

Command name	Description
<code>show ml d- snoopi ng</code>	Shows MLD snooping information.
<code>cl ear ml d- snoopi ng</code>	Clears all of the information regarding the MLD snooping.

25.4.2 Checking MLD snooping

The following describes the MLD snooping contents to be checked when MLD snooping functionality is used.

(1) Check after configuration

Execute the `show ml d- snoopi ng` operation command to check that the settings related to MLD snooping are correct.

Figure 25-4 Displayed status for MLD snooping settings

```
> show ml d- snoopi ng

Date 2012/12/06 02:01:53 UTC
VLAN counts: 3
VLAN: 100
  IP Address: fe80::1 Querier: enable
  MLD querying system: fe80::1
  Querier version: V1
  Port(1): 0/20
  Mrouter-port:
  Group counts: 2
VLAN: 200
  IP Address: fe80::2 Querier: enable
  MLD querying system: fe80::2
  Querier version: V1
  Port(1): 0/21
  Mrouter-port:
  Group counts: 3
VLAN: 300
  IP Address: fe80::3 Querier: disable
  MLD querying system: fe80::10
  Querier version: V2
  Port(2): 0/11, 0/22
  Mrouter-port: 0/11
  Group counts: 3

>
```

(2) Check during operation

Execute the following command to check the status of MLD snooping during operation.

- Use the `show ml d- snoopi ng group` operation command to check learned MAC addresses, IPv6 multicast addresses forwarded within a VLAN, and the status of the destination port list.

Figure 25-5 Results of executing show mld-snooping group

```
> show mld-snooping group
```

```
Date 2012/12/06 02:02:29 UTC
```

```
Total Groups: 8
```

```
VLAN counts: 3
```

```
VLAN 100 Group counts: 2
```

Group Address	MAC Address	Version	Mode
ff03::10	3333.0000.0010	V1	-
Port-list: 0/20			
ff03::11	3333.0000.0011	V1	-
Port-list: 0/20			

```
VLAN 200 Group counts: 3
```

Group Address	MAC Address	Version	Mode
ff03::22	3333.0000.0022	V1	-
Port-list: 0/21			
ff03::21	3333.0000.0021	V1	-
Port-list: 0/21			
ff03::20	3333.0000.0020	V1	-
Port-list: 0/21			

```
VLAN 300 Group counts: 3
```

Group Address	MAC Address	Version	Mode
ff03::3	3333.0000.0003	V2	INCLUDE
Port-list: 0/22			
ff03::2	3333.0000.0002	V2	INCLUDE
Port-list: 0/22			
ff03::1	3333.0000.0001	V2	INCLUDE
Port-list: 0/22			

```
>
```

- Use the `show mld-snooping port` operation command to check the participation group display example for each port.

Figure 25-6 Results of executing show mld-snooping port

```
> show mld-snooping port 0/22
```

```
Date 2012/12/06 02:06:58 UTC
```

```
Port 0/22 VLAN counts: 1
```

```
VLAN 300 Group counts: 3
```

Group Address	Last Reporter	Uptime	Expires
ff03::3	fe80::10	08:24	04:20
ff03::2	fe80::10	08:24	04:20
ff03::1	fe80::10	08:24	04:20

```
>
```


26. IPv4 Interfaces

This chapter describes the IPv4 interface and its use.

26.1	Description
26.2	Configuration
26.3	Operation

26.1 Description

A Switch can be used to set the IPv4 address for a VLAN, in order to perform SNMP, Telnet, or FTP communication used for management. For the VLAN, an IPv6 address can be set together. To communicate with other subnets, static routes need to be set.

A Switch detects duplicated IPv4 addresses set for VLAN interfaces. Duplication detection cannot be enabled by configuration settings. Instead, duplication detection runs automatically when an IPv4 address for a VLAN interface is set.

(1) Detecting duplicated IP addresses

The IP address set for a Switch VLAN interface is checked for duplication. A Switch sends gratuitous ARPs for each VLAN interface, and checks the source IP address of the received ARP packets for duplication.

(a) Gratuitous ARP sent from a Switch

The IP address set for the Switch VLAN interface is set in the target protocol address field, and the gratuitous ARP is sent. A gratuitous ARP packet is sent each time a VLAN interface goes up. Only one packet is sent.

(b) Check target for duplication detection

Duplication is detected not only for gratuitous ARP responses but also for all normally received ARP packets that meet the following conditions.

- The destination MAC address is a broadcast or a VLAN unicast of the Switch.
- Discarding has not occurred due a Spanning Tree Protocol, an access list, the dynamic ARP inspection functionality, or the authentication functionality on the Switch.
- An IP address has been set for a receiving VLAN interface.

(c) Detection conditions

When both of the following conditions are met, the IP address is considered to have been duplicated.

- The source MAC address during an ARP payload is a MAC address other than the unicast MAC address of the Switch (common to all VLANs).
- The source IP address is an IP address that has been set for the Switch.

(d) Detection operation

When a duplicated IP address is detected, the Switch outputs an operation log entry that includes the information in the following table.

Table 26-1 Operation log information output for a duplicated IP address

Log information	Description
VLAN ID	Interface number of the VLAN on which the duplicate IP address was detected
IP address	IP address whose duplication was detected
MAC address	MAC address of the remote device with the duplicate IP address (source MAC address during ARP payload)

Note that an operation log entry is not output if an entry has been output for the same IP address within the past 10 minutes.

26.2 Configuration

26.2.1 List of configuration commands

The following tables lists the commands used to configure IPv4 interfaces.

Table 26-2 List of configuration commands

Command name	Description
<code>arp</code>	Creates a static ARP table.
<code>ip address</code>	Specifies the IPv4 address of an interface.
<code>ip route</code>	Specifies a static route for IPv4.

26.2.2 Configuring an interface

Points to note

Set an IPv4 address for a VLAN. To specify an IPv4 address, you need to switch to interface configuration mode.

Command examples

1. `(config)# interface vlan 100`
Switches to the interface configuration mode for VLAN ID 100.
2. `(config-if)# ip address 192.168.1.1 255.255.255.0`
`(config-if)# exit`
Sets the IPv4 address 192.168.1.1 and the subnet mask 255.255.255.0 for VLAN ID 100.

26.2.3 Configuring multihoming

Points to note

Set multiple IPv4 addresses for a VLAN. For the second and subsequent IPv4 addresses, the `secondary` parameter needs to be specified.

Command examples

1. `(config)# interface vlan 100`
Switches to the interface configuration mode for VLAN ID 100.
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 ID 100.
3. `(config-if)# ip address 170.1.1.1 255.255.255.0 secondary`
`(config-if)# exit`
Sets the secondary IPv4 address 170.1.1.1 and the subnet mask 255.255.255.0 for VLAN ID 100.

26.2.4 Configuring static routes

Points to note

The Switches do not support routing protocol settings. Accordingly, communication with subnets outside the VLAN requires the setting of static routes.

Command examples

1. `(config)# ip route 192.168.2.0 255.255.255.0 192.168.1.254`
Specifies the forwarding route of the destination subnets 192.168.2.0/24 to 192.168.1.254.

26.2.5 Configuring static ARP

Points to note

Set static ARP on the Switch.

An interface needs to be specified.

Command examples

1. `(config)# arp 123.10.1.1 interface vlan 100 0012.e240.0a00`
Sets the next hop IPv4 address as 123.10.1.1 and sets destination MAC address 0012.e240.0a00 for VLAN ID 100 to configure static ARP.

26.3 Operation

26.3.1 List of operation commands

The following tables lists the operation commands for the IPv4 interface.

Table 26-3 List of operation commands

Command name	Description
<code>show ip-dual interface</code>	Shows the status of the interface for which both IPv4 and IPv6 are set.
<code>show ip interface</code>	Shows the status of the IPv4 interface.
<code>show ip arp</code>	Shows ARP entry information.
<code>clear arp-cache</code>	Deletes dynamic ARP entry information.
<code>show ip route</code>	Shows a route table.
<code>ping</code>	The <code>ping</code> command is used to determine whether communication is possible to the device with the specified IP address.
<code>tracert</code>	Shows the route (the route of gateways that have been passed through and the response time between the gateways) over which ICMP messages are sent to the destination host.

26.3.2 Checking the up/down status of the IPv4 interface

After specifying an IPv4 address on a Switch line or a port on an internal line to be connected to an IPv4 network, use the `show ip interface` operation command to check that the up/down status of the IPv4 interface is **Up**.

Figure 26-1 Example of displaying the IPv4 interface status

```
>show ip interface summary

Date 2012/03/03 13:49:51 UTC
VLAN0001: Up 192.168.0.100/24
           192.168.1.100/24
           192.168.2.100/24
VLAN0010: Down 192.168.10.100/24
VLAN3005: Up 192.168.5.10/24
           192.168.6.10/24
VLAN3253: Down 192.168.53.100/24
VLAN3254: Up 192.168.54.100/24
VLAN3255: Up 192.168.55.100/24
VLAN3256: Down 192.168.56.100/24
VLAN4094: Up 192.168.4.10/24

>
```

26.3.3 Checking the availability of communication with a destination address

Use the `ping` operation command to check whether the interface on a Switch connected to an IPv4 network can communicate with the remote device.

Figure 26-2 Results of executing ping when communication is available

```

> ping 192.168.100.2
PING 192.168.100.2 (192.168.100.2): 56 data bytes
64 bytes from 192.168.100.2: icmp_seq=0 ttl=128 time=17 ms
64 bytes from 192.168.100.2: icmp_seq=1 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=3 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=4 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=5 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=6 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=7 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=8 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=9 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=10 ttl=128 time=0 ms
^C
---- 192.168.100.2 PING Statistics ----
11 packets transmitted, 11 packets received, 0.0% packet loss
round-trip min/avg/max = 0/2/17 ms
>

```

Figure 26-3 Results of executing ping when communication is unavailable

```

> ping 192.168.254.254
PING 192.168.254.254 (192.168.254.254): 56 data bytes
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=0)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=1)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=2)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=3)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=4)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=5)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=6)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=7)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=8)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=9)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=10)
^C
---- 192.168.254.254 PING Statistics ----
14 packets transmitted, 0 packets received, 100.0% packet loss
>

```

26.3.4 Checking the route to a destination address

Use the **traceroute** operation command to check forwarding devices between the interface of a Switch connected to an IPv4 network and the remote device.

Figure 26-4 Results of executing traceroute

```

> traceroute 192.168.30.1 waittime 1 ttl 2
traceroute to 192.168.30.1 (192.168.30.1), 2 hops max, 8 byte packets
 1  192.168.30.1 (192.168.30.1)  0 ms  0 ms  0 ms
>

```

26.3.5 Checking ARP information

After specifying an IPv4 address on a Switch line or on a port on an internal line to be connected to an IPv4 network, use the **show ip arp** operation command to check whether addresses between the Switches and neighboring devices are resolved (whether ARP entry information exists).

Figure 26-5 Results of executing show ip arp

```

> show ip arp

Date 2012/03/03 12:16:02 UTC
Total: 9

```

IP Address	Linklayer Address	Interface	Expi re	Type
10. 0. 0. 6	00eb. f002. 0001	VLAN2000	19mi n	arpa
10. 10. 10. 3	incompl ete	VLAN3333	- -	arpa
192. 168. 254. 53	0090. cc42. 2dc4	VLAN4094	16mi n	arpa
192. 168. 254. 77	000f. fefa. f721	VLAN4094	6mi n	arpa
192. 168. 254. 98	001b. 7888. 1ffd	VLAN4094	19mi n	arpa
192. 168. 254. 99	1cc1. de64. f234	VLAN4094	15mi n	arpa
192. 168. 254. 102	00ce. a4bd. aad8	VLAN4094	Stati c	arpa
192. 168. 254. 250	0000. 8768. b663	VLAN4094	17mi n	arpa
192. 168. 254. 252	0012. e282. 680d	VLAN4094	2mi n	arpa

>

26.3.6 Checking the route table

The IPv4 route table is displayed. Use the **show ip route** operation command to check whether routing information between the Switches and devices on other subnets is set.

Figure 26-6 Results of executing show ip route

```
> show ip route
```

```
Date 2010/08/10 17:32:39 UTC
```

```
Total: 5
```

Destination	Nexthop	Interface	Protocol
192. 168. 0. 0/24	192. 168. 0. 100	VLAN0001	Connected
192. 168. 4. 0/24	192. 168. 4. 10	VLAN4094	Connected
192. 168. 5. 0/24	192. 168. 5. 10	VLAN3005	Connected
192. 168. 54. 0/24	192. 168. 54. 100	VLAN3254	Connected
192. 168. 55. 0/24	192. 168. 55. 100	VLAN3255	Connected

>

27. IPv6 Interfaces

This chapter describes the IPv6 interface and its use.

27.1	Description
27.2	Configuration
27.3	Operation

27.1 Description

A Switch can be used to set the IPv6 address for a VLAN, in order to perform SNMP, Telnet, or FTP communication used for management. For the VLAN, an IPv4 address can be set together. To communicate with other subnets, the default root (gateway) needs to be set.

(1) Automatic generation of IPv6 addresses when receiving router advertisements

Routers use router advertisements (RAs) to distribute to terminals the information that they need to generate IPv6 addresses as well as the default routes.

Routers regularly distribute only the prefix of their addresses in router advertisements. When a terminal receives a router advertisement, it generates its address by combining its own interface ID and the prefix in the router advertisement. In a sense, router advertisements provide terminals with a simple method of obtaining the prefixes of links without the need for servers.

The Switch can automatically generate IPv6 addresses by receiving router advertisements when the `ipv6 nd accept-ra` configuration command is set. When an interface receives a prefix from a router, an IPv6 global address is automatically generated by setting the MAC address of the Switch to the interface ID and then the IPv6 global address is assigned to the interface. At the same time, the router advertisement source address (interface link-local address of the router that sent the router advertisement) is set as the default gateway address. The default gateway is used prior to the default gateway set by using the `ipv6 default-gateway` configuration command.

If the information received by a router advertisement exceeds capacity limits, the previously received information takes priority.

27.2 Configuration

27.2.1 List of configuration commands

The following tables lists the commands used to configure IPv6 interfaces

Table 27-1 List of configuration commands

Command name	Description
<code>ipv6 address</code>	Sets the IPv6 address.
<code>ipv6 default-gateway</code>	Specifies the IPv6 default route.
<code>ipv6 enable</code>	Enables IPv6 on an interface. This command automatically generates a link-local address.
<code>ipv6 nd accept-ra</code>	Automatically creates IPv6 addresses and the default gateway when receiving router advertisements.
<code>ipv6 neighbor</code>	Creates a static NDP table.

27.2.2 Configuring an interface

Points to note

Set an IPv6 address for a VLAN. Up to seven addresses can be set per interface. First, use the `ipv6 enable` configuration command to enable the IPv6 functionality. If the `ipv6 enable` configuration command is not set, IPv6 setting cannot be applied.

Command examples

1. `(config)# interface vlan 100`
Switches to the interface configuration mode for VLAN ID 100.
2. `(config-if)# ipv6 enable`
Enables VLAN ID 100 to use an IPv6 address.
3. `(config-if)# ipv6 address 2001:100::1/64`
Sets the IPv6 address 2001:100::1 and a prefix length of 64 for VLAN ID 100.
4. `(config-if)# ipv6 address 2001:200::1/64`
`(config-if)# exit`
Sets the IPv6 address 2001:200::1 and a prefix length of 64 for VLAN ID 100.

27.2.3 Configuring the default route

Points to note

The Switches do not support routing protocol setting. To communicate with external subnets, the default route must be set.

Command examples

1. `(config)# ipv6 default-gateway interface vlan 100 fe80::100`

Specifies fe80::100 for the IPv6 default route (gateway).

27.2.4 Configuring a static NDP entry

Points to note

Register a static NDP entry.

Command examples

1. `(config)# ipv6 neighbor 2001:100::2 interface vlan 100 0012.e240.0a00`

Registers IPv6 address 2001:100::2 and MAC address 0012.e240.0a00 as the static NDP entry of the next hop node of VLAN ID 100.

27.2.5 Configuring settings for automatically generating an IPv6 address by receiving a router advertisement

Points to note

The example below shows how to configure settings so that an IPv6 address is automatically generated on a VLAN interface when receiving a router advertisement.

When an interface receives the prefix from a router, an IPv6 global address is automatically generated by setting the MAC address of the Switch for the interface ID and then the IPv6 global address is assigned to the interface.

At the same time, the router advertisement source address (link-local address of the router interface that sent the router advertisement) is set as the default gateway address.

Command examples

1. `(config)# interface vlan 200`

Switches to the interface configuration mode for VLAN ID 200.

2. `(config-if)# ipv6 nd accept-ra`

Configure settings so that IPv6 addresses are automatically generated when receiving router advertisements on VLAN ID 200.

3. `(config-if)# ipv6 enable`

`(config-if)# exit`

Permits IPv6 addresses on VLAN ID 200.

Notes

1. The default gateway set by receiving a route advertisement is used prior to the setting by the `ipv6 default-gateway` configuration command.
2. VLAN interfaces for which the `ip mtu` configuration command is not set support MTU settings from received router advertisements. The reception of router advertisements is specific to IPv6, but support for MTU settings from received router advertisements applies to IPv4 as well.
3. When using this command, make sure that the `ipv6 enable` configuration command is not set.

27.3 Operation

27.3.1 List of operation commands

The following tables lists the operation commands for the IPv6 interface.

Table 27-2 List of operation commands

Command name	Description
<code>show ip-dual interface</code>	Shows the status of the interface for which both IPv4 and IPv6 are set.
<code>show ipv6 interface</code>	Shows the status of the IPv6 interface.
<code>show ipv6 neighbors</code>	Shows NDP information.
<code>clear ipv6 neighbors</code>	Deletes dynamic NDP information.
<code>show ipv6 router-advertisement</code>	Shows RA information
<code>ping ipv6</code>	The <code>ping ipv6</code> command is used to determine whether communication is possible to the device with the specified IPv6 address.
<code>Traceroute ipv6</code>	Shows the route (the route of gateways that have been passed through and the response time between the gateways) over which ICMPv6 messages are sent to the destination host.

27.3.2 Checking the up/down status of the IPv6 interface

After specifying an IPv6 address on a Switch line or a port on an internal line to be connected to an IPv6 network, use the `show ipv6 interface` operation command to check that the up/down status of the IPv6 interface is **Up**.

Figure 27-1 Example of displaying the IPv6 interface status

```
> show ipv6 interface summary

Date 2012/03/03 14:33:50 UTC
VLAN0010: Up 2001::1:10/64
           fe80::2eb:f0ff:fe02:1%VLAN0010/64

>
```

27.3.3 Checking the availability of communication with a destination address

Use the `ping ipv6` operation command to check whether the interface on a Switch connected to an IPv6 network can communicate with the remote device.

Figure 27-2 Results of executing ping ipv6 when communication is available

```
> ping ipv6 3000::1
PING6(56=40+8+8 bytes) 3000::2 --> 3000::1
16 bytes from 3000::1, icmp_seq=0 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=1 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=2 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=3 hlim=64 time=0 ms
16 bytes from 3000::1, icmp_seq=4 hlim=64 time=17 ms
```

```

16 bytes from 3000::1, icmp_seq=5 hlim=64 time=0 ms
16 bytes from 3000::1, icmp_seq=6 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=7 hlim=64 time=0 ms
16 bytes from 3000::1, icmp_seq=8 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=9 hlim=64 time=0 ms
16 bytes from 3000::1, icmp_seq=10 hlim=64 time=0 ms
^C
--- 3000::1 ping6 statistics ---
11 packets transmitted, 11 packets received, 0.0% packet loss
round-trip min/avg/max = 0/9/17 ms
>

```

Figure 27-3 Results of executing ping ipv6 when communication is unavailable

```

> ping ipv6 3000::1
PING6(56=40+8+8 bytes) 3000::2 --> 3000::1
^C
--- 3000::1 ping6 statistics ---
11 packets transmitted, 0 packets received, 100.0% packet loss
>

```

27.3.4 Checking the route to a destination address

Use the **tracert ipv6** operation command to check forwarding devices between the interface of a Switch connected to an IPv6 network and the remote device.

Figure 27-4 Results of executing traceroute ipv6

```

> traceroute ipv6 100::2 numeric
traceroute6 to 100::2 (100::2) from 3000::2, 30 hops max, 8 byte packets
 1 3000::1 33 ms 0 ms 0 ms
 2 100::2 33 ms 33 ms 17 ms
>

```

27.3.5 Checking NDP information

After specifying an IPv6 address on a Switch line or on a port on an internal line to be connected to an IPv6 network, use the **show ipv6 neighbors** operation command to check whether addresses between the Switches and neighboring devices are resolved (whether NDP entry information exists).

Figure 27-5 Results of executing show ipv6 neighbor

```

> show ipv6 neighbors interface vlan 4094

Date 2012/03/07 11:05:51 UTC
Total: 7
Neighbor                               Linklayer Address Interface Expi re   S Flgs
2001:254::2                           782b.cb7f.7fa1  VLAN4094 1s        R
2001:254::99                           1cc1.de64.f234  VLAN4094 14s       R
2001:254::252                           0012.e282.680d  VLAN4094 permanent R S
2001:254::951:b8c:84bd:9cd3             1cc1.de64.f234  VLAN4094 6s        R
fe80::1bc:91af:3b96:2f72%VLAN4094       782b.cb7f.7fa1  VLAN4094 19m56s    S
fe80::212:e2ff:fe82:680d%VLAN4094       0012.e282.680d  VLAN4094 permanent R S
fe80::951:b8c:84bd:9cd3%VLAN4094        1cc1.de64.f234  VLAN4094 19m56s    S
>

```

28. DHCP Server Functionality

The DHCP server functionality is used to dynamically assign IP addresses or option information to DHCP clients. This chapter describes the DHCP server functionality and its configuration settings.

28.1	Description
28.2	Configuration
28.3	Operation

28.1 Description

The DHCP server functionality is used to dynamically assign IP addresses or option information to DHCP clients. This section describes the specifications and operation of the DHCP server functionality of the Switch.

28.1.1 Supported specifications

The following table describes the support specification of the DHCP server of the Switch. The DHCP server and the clients are direct-coupled on the same network.

Table 28-1 Support specification of the DHCP server

Item	Specifications
Connection configuration	Directly handles DHCP clients. DHCP clients cannot be handled via a DHCP relay agent.
BOOTP server functionality	Not supported
Dynamic DNS link	Not supported
Dynamic IP address distribution functionality	Supported
Fixed IP address distribution functionality	Supported

28.1.2 Information distributed to clients

The following table describes the information that the Switch can distribute to the clients. The information that can be distributed does not include the information handled as an option even if the option for distributing the information is specified on the Switch, unless the client side uses an option request list to request the Switch to distribute the information handled as option.

Table 28-2 List of information distributed to clients

Item	Specifications
IP address	Set an IP address that can be used by a client.
IP address lease time	Set the lease time of an IP address to be distributed. On the Switch, the value is determined by <code>default-lease-time</code> and <code>max-lease-time</code> parameters and a request from the client. (Option No. 51)
Subnet mask	The subnet mask length of network information specified by configuration is used. (Option No. 1)
Router option	Specify the IP address of the router on the subnet of the client. This IP address is used as the gateway address of the client. (Option No. 3)
DNS option	Specify the IP address of a domain name server available for the client. (Option No. 6)

28.1.3 Preventing duplicate distribution of IP addresses

When the Switch restarts during provision of service by the DHCP server of the Switch (that is, in the state in which addresses are assigned to DHCP clients), the entire pool for assigning IP addresses on the Switch becomes blank. However, when the Switch assigns an IP address thereafter, duplicate IP address assignment is prevented by sending ICMP Echo Request packets to the assigned IP addresses, and checking whether other clients are using the IP addresses. If the IP address is being used, there will be a response packet.

Also, when responses to ICMP Echo Request packets are returned (that is, another terminal on the network is using the IP address), information about the terminals receiving DECLINE messages is displayed as a detected address conflict in the information displayed by the `show ip dhcp conflict` operation command.

28.1.4 Notes on using the DHCP server functionality

This section provides notes on using the DHCP server functionality.

(1) IP address of the input interface for multihomed connection

For multihomed connection, the primary IP address is the IP address of the input interface. IP addresses are assigned to DHCP clients from the address pool set for the subnet.

28.2 Configuration

28.2.1 List of configuration commands

The following table describes the configuration commands for DHCP servers.

Table 28-3 List of configuration commands

Command name	Description
<code>default t-router</code>	Specifies a router option for distribution to a client. A router option is an IP address the client can use as a router IP address over the subnet (default router). Set the IP address of the router that a client uses as described in <i>28.2.2 Settings for distributing IP addresses to clients</i> .
<code>dns-server</code>	Sets the domain name server option that is distributed to clients.
<code>hardware-address</code>	Specifies the MAC address of the target device when the fixed IP address is distributed to client devices. This command is used together with a host command as a set. Set the MAC address of a client as described in <i>28.2.3 Settings for distributing static IPs to clients</i> .
<code>host</code>	Specifies an IP address to be assigned when the fixed IP address is distributed to client devices. This command is used together with a hardware address command as a set. Set an IP address that a client uses as described in <i>28.2.3 Settings for distributing static IPs to clients</i> .
<code>ip dhcp excluded-address</code>	Specifies the range of IP addresses to be excluded from distribution, from among the IP address pool specified by the <code>network</code> command. For the address range of the network, set IP addresses to be excluded from distribution to a client as described in <i>28.2.2 Settings for distributing IP addresses to clients</i> .
<code>ip dhcp pool</code>	Configures DHCP address pool information.
<code>lease</code>	Specifies the default lease time of an IP address to be distributed to a client. Set the lease time of the IP address that a client will use as described in <i>28.2.2 Settings for distributing IP addresses to clients</i> .
<code>max-lease</code>	Specifies the maximum allowable lease time when a client specifies a lease time and requests an IP address.
<code>network</code>	Specifies the subnet of the network that dynamically distributes IP addresses via DHCP. Only the subnets whose host bits in the IP address host part are not all 0 or 1 are actually registered in the DHCP address pool. Set the network in which IP addresses are distributed via DHCP as described in <i>28.2.2 Settings for distributing IP addresses to clients</i> .
<code>service dhcp</code>	Specifies the interface to enable a DHCP server. Only the interface specified using this command receives DHCP packets. Set a VLAN interface to which DHCP clients are connected as described in <i>28.2.2 Settings for distributing IP addresses to clients</i> .

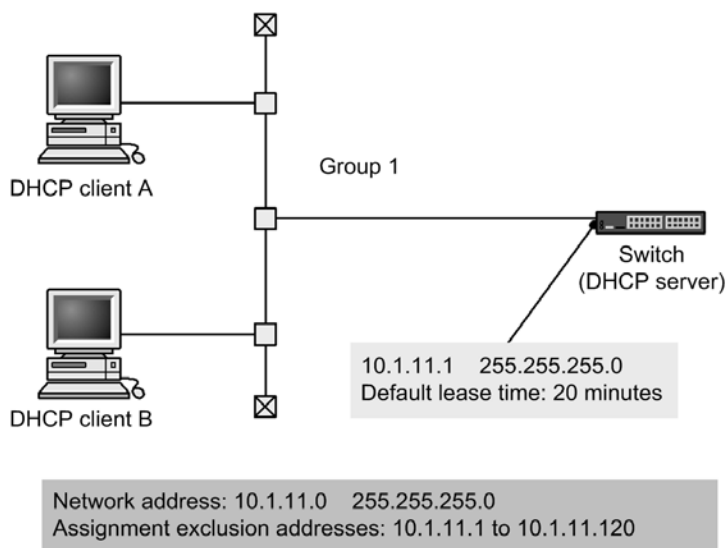
28.2.2 Settings for distributing IP addresses to clients

Points to note

Specify the IP addresses that you do not want to assign to DHCP clients as addresses to be excluded from distribution. Also, configure the DHCP address pool

to distribute IP addresses to DHCP clients dynamically.

Figure 28-1 Configuration of a client and server (for distribution of dynamic IP addresses)



Command examples

1. `(config)# interface vlan 10`
`(config-if)# ip address 10.1.11.1 255.255.255.0`
`(config-if)# exit`
 Sets a VLAN interface and IP address beforehand.
2. `(config)# service dhcp vlan 10`
 Sets a VLAN on which a DHCP server is enabled.
3. `(config)# ip dhcp excluded-address 10.1.11.1 10.1.11.120`
 Sets an IP address to be excluded from those assigned to a DHCP client by a DHCP server.
4. `(config)# ip dhcp pool Group1`
 Sets the DHCP address pool.
 Switches to DHCP configuration mode.
5. `(dhcp-config)# network 10.1.11.0 255.255.255.0`
 Sets the network address of the DHCP address pool.
6. `(dhcp-config)# lease 0 0 20`
 Sets 20 minutes as the default lease time of the DHCP address pool.
7. `(dhcp-config)# default-router 10.1.11.1`

```
(dhcp-config) # exit
```

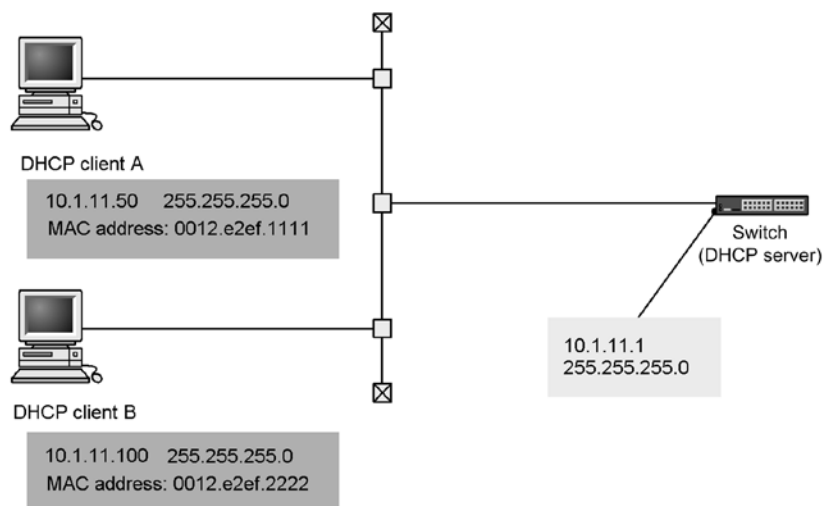
Specifies the IP address of a router on the subnet.

28.2.3 Settings for distributing static IPs to clients

Points to note

Set an IP address and MAC address for each client to distribute a fixed IP address for each DHCP client.

Figure 28-2 Configuration of a client and server (for distribution of fixed IP addresses)



Command examples

1.

```
(config) # interface vlan 10
```



```
(config-if) # ip address 10.1.11.1 255.255.255.0
```



```
(config-if) # exit
```

Sets a VLAN interface and IP address beforehand.
2.

```
(config) # service dhcp vlan 10
```

Sets a VLAN on which a DHCP server is enabled.
3.

```
(config) # ip dhcp pool Group1
```

Specifies the address pool name of DHCP client A.
Switches to DHCP configuration mode.
4.

```
(dhcp-config) # host 10.1.11.50 255.255.255.0
```

Sets a fixed IP address for the address pool of DHCP client A.
5.

```
(dhcp-config) # hardware-address 0012.e2ef.1111 ethernet
```

Sets a MAC address for the DHCP address pool of DHCP client A.
6.

```
(dhcp-config) # default-router 10.1.11.1
```

```
(dhcp-config)# exit
```

Specifies the IP address of a router on the subnet.

7.

```
(onfig)# ip dhcp pool Client2
```

```
(dhcp-config)# host 10.1.11.100 255.255.255.0
```

```
(dhcp-config)# hardware-address 0012.e2ef.2222 ethernet
```

```
(dhcp-config)# default-router 10.1.11.1
```

```
(dhcp-config)# exit
```

Sets the address pool name, fixed IP address, and MAC address for DHCP client B in the same way as item numbers 3 to 6.

28.3 Operation

28.3.1 List of operation commands

The following table describes the operation commands for the DHCP server.

Table 28-4 List of operation commands

Command name	Description
<code>show ip dhcp binding</code>	Shows the binding information on the DHCP server.
<code>clear ip dhcp binding</code>	Deletes the binding information from the DHCP server database.
<code>show ip dhcp conflict</code>	Shows IP address conflicts detected by the DHCP server. An IP address conflict refers to an IP address assigned to a terminal over the network though it is blank as a pool IP address on the DHCP server. An IP address conflict is detected by checking the existence of responses for ICMP packet sending, or receiving DECLINE messages before the DHCP server assigns an IP address to a DHCP client.
<code>clear ip dhcp conflict</code>	Clears an IP address conflict from the DHCP server.
<code>show ip dhcp server statistics</code>	Shows statistics about the DHCP server.
<code>clear ip dhcp server statistics</code>	Resets statistics on the DHCP server.

28.3.2 Checking the DHCP server

(1) Checking the number of assignable IP addresses

The number of IP addresses that can be assigned to clients is displayed by `address pools`, which is in the results of the `show ip dhcp server statistics` operation command. Make sure the number is greater than the number of IP addresses you want to assign to clients.

Figure 28-3 Results of executing `show ip dhcp server statistics`

```
> show ip dhcp server statistics

Date 2010/07/23 08:34:35 UTC
< DHCP Server use statistics >
  address pools      : 1010
  automatic bindings : 13
  manual bindings    : 1
  expired bindings   : 0
  over pools request : 0
  discard packets    : 0
< Receive Packets >
  DHCPDISCOVER       : 14
  DHCPREQUEST        : 14
  DHCPDECLINE        : 0
  DHCPRELEASE        : 0
  DHCPINFORM         : 1
< Send Packets >
  DHCPOFFER          : 14
  DHCPACK            : 15
  DHCPNAK            : 0
```

>

(2) Checking distributed IP address

Use the `show ip dhcp binding` operation command to check IP addresses assigned to DHCP clients. IP addresses whose lease time has not expired are displayed.

Figure 28-4 Results of executing show ip dhcp binding

> show ip dhcp binding

Date 2010/07/23 08:41:12 UTC

No	IP Address	MAC Address	Lease Expiration	Type
1	192.168.1.1	0012.e2c4.a8c7		Manual
2	192.168.1.0	0012.e26a.015c	2010/07/24 08:34:05	Automatic
3	192.168.1.2	0012.e26a.015f	2010/07/24 08:34:06	Automatic

>

Appendix

A Supported Standards

A. Supported Standards

A.1 TELNET/FTP/TFTP

Table A-1 Relevant standards and recommendations for TELNET/FTP/TFTP

Name (month and year issued)	Name of standard
RFC 854 (May 1983)	TELNET PROTOCOL SPECIFICATION
RFC 855 (May 1983)	TELNET OPTION SPECIFICATIONS
RFC 959 (October 1985)	FILE TRANSFER PROTOCOL (FTP)
RFC 1350 (July 1992)	THE TFTP PROTOCOL (REVISION 2)
RFC 2428 (September 1998)	FTP Extensions for IPv6 and NATs

A.2 RADIUS

Table A-2 Relevant standards and recommendations for RADIUS

Name (month and year issued)	Name of standard
RFC 2865 (June 2000)	Remote Authentication Dial In User Service (RADIUS)
RFC 3162 (August 2001)	RADIUS and IPv6

A.3 NTP

Table A-3 Relevant standard and recommendation for NTP

Name (month and year issued)	Name of standard
RFC 2030 (October 1996)	Simple Network Time Protocol (SNTP) Version4 for IPv4, IPv6 and OSI

A.4 DNS

Table A-4 Relevant standards and recommendations for DNS resolver

Name (month and year issued)	Name of standard
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 802.2 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 2008 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
10GBASE-R	IEEE 802.3ae Standard-2002	Media Access Control(MAC) Parameters, Physical Layer, and Management Parameters for 10Gb/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 VLANs

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 recommendations 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 standard and recommendation for IGMP snooping and MLD snooping

Name (month and year issued)	Name of standard
draft-ietf-magma-snoop-12.txt (August 2005)	IGMP and MLD snooping switches

A.10 IPv4 interfaces

Table A-10 Relevant standards and recommendations for IP version 4

Name (month and year issued)	Name of standard
RFC 791 (September 1981)	Internet Protocol
RFC 792 (September 1981)	Internet Control Message Protocol
RFC 826 (November 1982)	An Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware
RFC 922 (October 1984)	Broadcasting Internet datagrams in the presence of subnets
RFC 950 (August 1985)	Internet Standard Subnetting Procedure
RFC 1027 (October 1987)	Using ARP to implement transparent subnet gateways
RFC 1122 (October 1989)	Requirements for Internet hosts-communication layers

A.11 IPv6 interfaces

Table A-11 Relevant standards and recommendations for IP version 6

Name (month and year issued)	Name of standard
RFC 2373 (July 1998)	IP Version 6 Addressing Architecture
RFC 2460 (December 1998)	Internet Protocol, Version 6 (IPv6) Specification
RFC 2461 (December 1998)	Neighbor Discovery for IP Version 6 (IPv6)
RFC 2462 (December 1998)	IPv6 Stateless Address Autoconfiguration
RFC 2463 (December 1998)	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC 2710 (October 1999)	Multicast Listener Discovery for IPv6

A.12 DHCP server functionality

Table A-12 Relevant standards for DHCP server functionality

Name (month and year issued)	Name of standard
RFC 2131 (March 1997)	Dynamic Host Configuration Protocol
RFC 2132 (March 1997)	DHCP Options and BOOTP Vendor Extensions

Index

1

1000BASE-T, 175

- automatic recognition, 175
- auto-negotiation, 177
- configuring, 185
- connection interfaces, 175
- connection specifications, 175
- connection specifications for transmission speed and duplex mode (full or half), 176
- flow control, 177
- flow control for receiving on switch, 178
- flow control for sending on switch, 178
- jumbo frame support status, 182
- jumbo frames, 181

1000BASE-X, 191

- auto-negotiation, 192
- configuring, 197
- connection interfaces, 191
- connection specifications, 192
- connection specifications for transmission speed and duplex mode (full or half), 192
- flow control, 192
- flow control for receiving on switch, 193
- flow control for sending on switch, 193
- jumbo frame support status, 196
- jumbo frames, 196

100BASE-FX

- connection interfaces, 187
- connection specifications, 187
- connection specifications for transmission speed and duplex mode (full or half), 187
- flow control, 187
- flow control for receiving on switch, 188
- flow control for sending on switch, 188
- jumbo frame support status, 189
- jumbo frames, 188

100BASE-FX [24S4X] [24S4XD], 187

- configuring, 190

100BASE-TX, 175

- automatic recognition, 175
- auto-negotiation, 177
- configuring, 185
- connection interfaces, 175
- connection specifications, 175
- connection specifications for transmission speed and duplex mode (full or half), 176
- flow control, 177
- flow control for receiving on switch, 178
- flow control for sending on switch, 178
- jumbo frame support status, 182
- jumbo frames, 181

10BASE-T, 175

- automatic recognition, 175
- auto-negotiation, 177
- configuring, 185
- connection interfaces, 175
- connection specifications, 175

- connection specifications for transmission speed and duplex mode (full or half), 176
- flow control, 177
- flow control for receiving on switch, 178
- flow control for sending on switch, 178
- jumbo frame support status, 182
- jumbo frames, 181

10GBASE-R

- connection interfaces, 198
- connection specifications, 198
- flow control, 198
- flow control for receiving on switch, 199
- flow control for sending on switch, 199
- jumbo frame support status, 199
- jumbo frames, 199

10GBASE-R [10G model], 198

- configuring, 201

10GBASE-R connection

- notes on, 200

A

assigning IP address to Switch

- remote login, 83

authentication sequence

- with end-by-reject specified, 96
- without end-by-reject specified, 95

automatic generation of IPv6 addresses when

- receiving router advertisements, 470

automatic MDIX functionality, 181

automatic recognition

- 10BASE-T, 100BASE-TX, and 1000BASE-T, 175

auto-negotiation

- 1000BASE-X, 192
- 10BASE-T, 100BASE-TX, and 1000BASE-T, 177

auto-recovery

- disabling, 128

B

backing up

- switch information, 125

backup ring, 377

baking up switch information

- operation commands, 125

basic VLAN functionality

- configuration commands, 252

C

capacity limits, 19, 22

- DHCP snooping, 41

- filters, 31

- high reliability based on redundant configurations, 41

- high reliability function based on network failure detection, 42

Index

- IP interfaces, 28
- Layer 2 authentication functionality, 36
- Layer 2 switch functionality, 23
- lines, 20
- link aggregation, 22
- login security, 22
- modules, 20
- neighboring device information (LLDP), 44
- QoS, 31
- capacity limits
 - RADIUS, 22
- checking
 - communication between remote operation terminal and switch, 85
 - time, 108
- CLI
 - notes on, 61
 - operations, 56
- CLI environment information, 59
- CLI settings
 - customizing, 59
- commands
 - input modes, 54
 - operations, 53
- common Spanning Tree functionality, 340
 - configuration commands, 346
 - configuring, 346
 - operation commands, 350
 - operations, 350
- configuration commands
 - basic VLAN functionality, 252
 - common Spanning Tree functionality, 346
 - DHCP servers, 478
 - DNS, 117
 - editing procedures, 71
 - Ethernet, 170
 - host names, 117
 - IGMP snooping, 452
 - inter-port relay blocking functionality, 292
 - IPv4 interfaces, 463
 - IPv6 interfaces, 471
 - L2 protocol frame transparency functionality, 289
 - link aggregation basic functionality, 209
 - link aggregation extended functionality, 219
 - login security, 88
 - MAC address learning, 241
 - MAC VLANs, 270
 - managing devices, 120
 - MLD snooping, 456
 - mode transitions, 70
 - Multiple Spanning Tree, 332
 - NTP, 111
 - port VLANs, 257
 - power saving functionality, 153
 - protocol VLANs, 262
 - PVST+, 312
 - RADIUS, 99
 - remote login, 83
 - Ring Protocol, 400
- Single Spanning Tree, 320
- Spanning Tree operating mode, 306
- tag translation, 286
- time, 111
- virtual links, 433
- VLAN tunneling, 284
- configurations
 - operations, 77
- configuring
 - 1000BASE-T, 185
 - 1000BASE-X, 197
 - 100BASE-FX [24S4X] [24S4XD], 190
 - 100BASE-TX, 185
 - 10BASE-T, 185
 - 10GBASE-R [10G model], 201
 - basic VLAN functionality, 252
 - common Spanning Tree functionality, 346
 - DHCP servers, 478
 - editing procedures, 71
 - IGMP snooping, 452
 - inter-port relay blocking functionality, 292
 - IPv4 interfaces, 463
 - L2 protocol frame transparency functionality, 289
 - link aggregation basic functionality, 209
 - link aggregation extended functionality, 219
 - MAC address learning, 241
 - MAC VLANs, 270
 - MLD snooping, 456
 - Multiple Spanning Tree, 332
 - NTP, 111
 - port VLANs, 257
 - power saving functionality, 153
 - protocol VLANs, 262
 - PVST+, 312
 - RADIUS, 99
 - remote login, 83
 - Ring Protocol, 400
 - shared SFP/SFP+ ports [10G model], 203
 - Single Spanning Tree, 320
 - Spanning Tree operating mode, 306
 - switch, 9, 67, 68
 - time, 111
- connection interfaces
 - 1000BASE-X, 191
 - 100BASE-FX, 187
 - 10BASE-T, 100BASE-TX, and 1000BASE-T, 175
 - 10GBASE-R, 198
 - shared SFP/SFP+ ports, 202
- connection specifications
 - 1000BASE-X, 192
 - 100BASE-FX, 187
 - 10BASE-T, 100BASE-TX, and 1000BASE-T, 175
 - 10GBASE-R, 198
- connection specifications for transmission speed and duplex mode (full or half)
 - 1000BASE-X, 192
 - 100BASE-FX, 187

- 10-BASE-T, 100BASE-TX, and 1000BASE-T, 176
- console, 46
- creating
 - user accounts, 89
- customizing
 - CLI settings, 59
- D**
 - deleting
 - user accounts, 89
 - detecting
 - duplicated IP addresses, 462
 - devices
 - managing, 119
 - DHCP server functionality
 - supported standards, 489
 - DHCP servers, 476
 - configuration commands, 478
 - configuring, 478
 - functionality, 475
 - information distributed to clients, 476
 - notes on using the DHCP server
 - functionality, 477
 - operation commands, 482
 - operations, 482
 - preventing duplicate distribution of IP addresses, 477
 - supported specifications, 476
 - DHCP snooping
 - capacity limits, 41
 - direct attach cables, 202
 - disabling
 - auto-recovery, 128
 - discarding conditions
 - received frames, 168
 - DNS, 115
 - configuration commands, 117
 - DNS resolver
 - supported standards, 486
 - down-shift functionality, 182
 - duplicated IP addresses
 - detecting, 462
- E**
 - editing
 - running configuration, 69
 - editing procedures
 - configuration commands, 71
 - configuring, 71
 - operation commands, 71
 - Ethernet, 165
 - configurations common to all interfaces, 170
 - information common to all ports, 166
 - operation commands, 174
 - operations common to all interfaces, 174
 - supported standards, 487
 - Ethernet
 - configuration commands, 170

- F**
 - failures
 - restoring from, 128
 - filters
 - capacity limits, 31
 - flow control
 - 1000BASE-X, 192
 - 100BASE-FX, 187
 - 10BASE-T, 100BASE-TX, and 1000BASE-T, 177
 - 10GBASE-R, 198
 - flow control for receiving on switch
 - 1000BASE-X, 193
 - 100BASE-FX, 188
 - 10BASE-T, 100BASE-TX, and 1000BASE-T, 178
 - 10GBASE-R, 199
 - flow control for sending on switch
 - 1000BASE-X, 193
 - 100BASE-FX, 188
 - 10BASE-T, 100BASE-TX, and 1000BASE-T, 178
 - 10GBASE-R, 199
 - forced cancellation of sleep mode, 138
 - frame formats
 - controlling on MAC and LLC sublayers, 167
 - LLC sublayer, 167
 - MAC sublayer, 167
 - FTP
 - supported standards, 486
- H**
 - handling
 - padding, 168
 - TYPE/LENGTH field, 167
 - high reliability based on redundant configurations
 - capacity limits, 41
 - high reliability function based on network failure detection
 - capacity limits, 42
 - host names, 115
 - configuration commands, 117
- I**
 - IGMP instant leave, 444
 - IGMP querier functionality
 - IGMP snooping, 443
 - IGMP snooping, 437, 441
 - configuration commands, 452
 - configuring, 452
 - connecting with multicast routers, 442
 - IGMP querier functionality, 443
 - Layer 2 forwarding for IPv4 multicast packets, 442
 - list of supported functionality, 440
 - MAC address control method, 441
 - MAC address learning, 441
 - operation commands, 454

- operations, 451, 454
 - overview, 438
 - settings, 451
 - supported functionality, 440
 - supported standards, 488
 - usage notes, 448
- IGMP snooping and MLD snooping
 - overview, 439
- IGMPv1 message operation, 443
- IGMPv2 message operation, 443
- IGMPv3 message
 - operation, 443
- inter-port relay blocking functionality, 290
 - configuration commands, 292
 - configuring, 292
- IP interfaces
 - capacity limits, 28
- IPv4 interfaces, 461, 462
 - configuration commands, 463
 - configuring, 463
 - operation commands, 465
 - operations, 465
 - supported standards, 488
- IPv4 multicast addresses and MAC addresses
 - correspondence, 441
- IPv6 interfaces, 469
 - configuration commands, 471
 - operation commands, 473
 - operations, 473
 - supported standards, 488
- IPv6 multicast addresses and MAC addresses
 - correspondence, 445

J

- jumbo frame support status
 - 100BASE-X, 196
 - 100BASE-FX, 189
 - 10BASE-T, 100BASE-TX, and 1000BASE-T, 182
 - 10GBASE-R, 199
- jumbo frames
 - 100BASE-X, 196
 - 100BASE-FX, 188
 - 10BASE-T, 100BASE-TX, and, 1000BASE-T, 181
 - 10GBASE-R, 199

L

- L2 protocol frame transparency functionality, 288
 - configuration commands, 289
 - configuring, 289
- Layer 2 authentication functionality
 - capacity limits, 36
- Layer 2 forwarding for IPv4 multicast packets
 - IGMP snooping, 442
- Layer 2 forwarding for IPv6 multicast packets
 - MLD snooping, 446
- Layer 2 switch functionality

- capacity limits, 23
- Layer 2 switching
 - compatibility with other functionality, 228
 - overview, 225, 226
 - supported functionality, 227
- license
 - registering, 164
- lines
 - capacity limits, 20
- link aggregation, 205
 - basic functionality, 206
 - capacity limits, 22
 - configuring the basic functionality, 209
 - configuring the extended functionality, 219
 - extended functionality, 217
 - operation commands, 221
 - operations, 221
 - supported standards, 487
- link aggregation basic functionality
 - configuration commands, 209
- link aggregation extended functionality
 - configuration commands, 219
- LLC sublayer
 - frame formats, 167
- logging in, 52
 - procedures, 45
 - remotely, 81
 - security, 87
- logging out, 52
- login control
 - overview, 88
- login security
 - capacity limits, 22
 - configuration commands, 88
 - operation commands, 88
 - settings, 88

M

- MAC address control method
 - IGMP snooping, 441
 - MDL snooping, 445
- MAC address learning, 235, 236
 - configuration commands, 241
 - configuring, 241
 - IGMP snooping, 441
 - MLD snooping, 445
 - operation commands, 243
 - operations, 243
- MAC sublayer
 - frame formats, 167
- MAC VLANs, 266
 - configuration commands, 270
 - configuring, 270
- managing
 - devices, 119
 - operation terminal, 46
 - software, 161
- managing devices
 - configuration commands, 120
 - operation commands, 120

- maximum number of concurrent users
 - setting, 90
- MDI and MDI-X pin mappings, 181
- MDL snooping
 - MAC address control method, 445
- MLD querier functionality
 - MLD snooping, 447
- MLD snooping, 437, 445
 - configuration commands, 456
 - configuring, 456
 - connecting with multicast routers, 446
 - Layer 2 forwarding for IPv6 multicast packets, 446
 - list of supported functionality, 440
 - MAC address learning, 445
 - MLD querier functionality, 447
 - operation commands, 458
 - operations, 451, 458
 - overview, 438
 - settings, 451
 - supported functionality, 440
 - supported standards, 488
 - usage notes, 448
- MLDv1 message operation, 446
- MLDv2 message operation, 447
- modules
 - capacity limits, 20
- multicast group address, 438
- multi-fault monitoring frames, 378
- multi-fault monitoring functionality, 377
- multi-fault monitoring VLAN, 379
- Multiple Spanning Tree, 326
 - configuration commands, 332
 - configuring, 332
 - operation commands, 338
 - operations, 338
- multi-ring operation
 - overview, 368

N

- neighboring device information (LLDP)
 - capacity limits, 44
- normal time range, 142
- notes on 100BASE-FX connection, 189
- notes on a 1000BASE-X connection, 196
- notes on a 10BASE-T, 100BASE-TX, or 1000BASE-T connection, 183
- NTP, 107
 - configuration commands, 111
 - configuring, 111
 - operation commands, 113
 - operations, 113
 - supported standards, 486

O

- operation commands
 - backing up switch information, 125
 - common Spanning Tree functionality, 350
 - DHCP servers, 482

- editing procedures, 71
- Ethernet, 174
- IGMP snooping, 454
- input modes, 54
- IPv4 interfaces, 465
- IPv6 interfaces, 473
- link aggregation, 221
- login security, 88
- MAC address learning, 243
- managing devices, 120
- MLD snooping, 458
- Multiple Spanning Tree, 338
- NTP, 113
- power saving functionality, 158
- PVST+, 317
- RADIUS, 103
- remote login, 85
- restoring switch information, 125
- Single Spanning Tree, 325
- software management, 162
- time, 113
- virtual links, 435
- VLAN extended functionality, 295
- VLANs, 276
- operation terminal
 - connection features, 47
 - connection topology, 46
 - functional requirements, 46
 - managing, 46
- overview of IGMP snooping and MLD snooping, 439

P

- padding
 - handling, 168
- password for switching to administrator mode
 - setting, 89
- port blocking
 - power saving functionality, 138
- port VLANs, 256
 - configuration commands, 257
 - configuring, 257
- power saving functionality, 131, 132
 - configuration commands, 153
 - configuring, 153
 - link-down ports, 137
 - operation commands, 158
 - operations, 158
 - option that wakes switch when incoming WOL packet is detected, 139
 - option that wakes switch when link-up state is detected, 141
 - port blocking, 138
 - wake-up option, 139
- procedures
 - logging in, 45
- protocol VLANs, 260
 - configuration commands, 262
 - configuring, 262
- PVST+, 309

Index

- configuration commands, 312
- configuring, 312
- operation commands, 317
- operations, 317

Q

QoS

- capacity limits, 31

R

RADIUS, 87, 92

- capacity limits, 22
- configuration commands, 99
- configuring, 99
- operation commands, 103
- operations, 103
- overview, 92
- supported standards, 486

RADIUS implementation scope, 92

RADIUS server group information, 97

RADIUS support scope, 93

received frames

- discarding conditions, 168

registering

- license, 164

remote login, 81

- assigning IP address to Switch, 83
- configuration commands, 83
- configuring, 83
- description, 82
- operation commands, 85
- operations, 85

remote operation terminal, 47

restoring

- switch information, 125

restoring from

- failures, 128

restoring switch information

- operation commands, 125

Ring Protocol, 353

- basic principles, 358
- configuration commands, 400
- configuring, 400
- network design, 386
- operations, 399, 415
- overview, 354
- settings, 399
- usage notes, 395
- using with Spanning Tree Protocols, 420
- using with Spanning Tree Protocols/GSRP, 419

running configuration

- editing, 69

S

scheduled time range, 142

security

- logging in, 87

setting

- IP addresses of remote operation terminals permitted to log in, 90
- maximum number of concurrent users, 90
- password for switching to administrator mode, 89

- time, 108

shared SFP/SFP+ ports

- connection interfaces, 202

shared SFP/SFP+ ports [10G model], 202

- configuring, 203

single ring operation

- overview, 363

Single Spanning Tree, 318

- configuration commands, 320

- configuring, 320

- operation commands, 325

- operations, 325

sleep mode, 138

software

- managing, 161

- updating, 163

software management

- operation commands, 162

Spanning Tree operating mode

- configuration commands, 306

- configuring, 306

Spanning Tree Protocols, 297

- overview, 298

- supported standards, 487

starting up

- switch, 50

status display

- settings, 120

support specification of the DHCP server, 476

supported standards, 486

- DHMP server functionality, 489

- Ethernet, 487

- FTP, 486

- IGMP snooping, 488

- IPv4 interfaces, 488

- IPv6 interfaces, 488

- link aggregation, 487

- MLD snooping, 488

- NTP, 486

- RADIUS, 486

- Spanning Tree Protocols, 487

- TELNET, 486

- TFTP, 486

- VLANs, 487

supported standards:, 486

switch

- components, 13

- configuring, 9, 67, 68

- features, 3

- model range, 10

- overview, 1, 2

- starting up, 50

switch information

- backing up, 125

- restoring, 125

system operation
 settings, 120

T

tag translation
 configuration commands, 286

TELNET
 supported standards, 486

TFTP
 supported standards, 486

time
 checking, 108
 configuration commands, 111
 configuring, 111
 operation commands, 113
 operations, 113
 setting, 108
 settings, 107
TYPE/LENGTH field
 handling, 167

U

updating
 software, 163

user accounts
 creating and deleting, 89

V

virtual links, 421
 configuration commands, 433
 operation commands, 435
VLAN extended functionality, 281
 operation commands, 295
 operations, 295
VLAN mapping, 386
VLAN tunneling
 configuration commands, 284
VLANs, 245
 basic functionality, 246
 configuring basic functionality, 252
 operation commands, 276
 operations, 276
 supported standards, 487

W

wake-up option
 power saving functionality, 139