

AX2200S/AX1250S/AX1240S Software Manual

Configuration Guide Vol. 1

For Version 2.4

AX1240S-S001X-60

Alaxala

■ Relevant products

This manual applies to the AX2200S, AX1250S, and AX1240S models of switches. The manual describes the functionality in version 2.4 of the software for the AX2200S, AX1250S, and AX1240S series switches that are supported by the software OS-LT4, OS-LT3 and OS-LT2, and by optional licenses.

■ Export restrictions

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

■ Trademarks

- 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 SecurID are trademarks or registered trademarks of RSA Security Inc. in the United States and other countries.
- Wake on LAN is a registered trademark of IBM Corp.
- 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

July 2012 (Edition 7) AX1240S-S001X-60

■ Copyright

All Rights Reserved, Copyright(C),2008, 2012, ALAXALA Networks, Corp.

■ History of Amendments

For version 2.4 (Edition 7)

Summary of amendments

Location and title	Changes
Addition of series	● A description of AX2200S series switches was added.
2 Switch Configuration	● A description of AX2200S series switches was added.
3 Capacity Limit	● A description of AX2200S series switches was added.
10 Device Management	● A description of AX2200S series switches was added.
PowerSaving Functionality	● A description of AX2200S series switches was added.
13. Ethernet	● A description of AX2200S series switches was added.

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

For version 2.3 (Edition 6)

Summary of amendments

Location and title	Changes
Capacity Limit	● In (6) <i>Ring Protocol</i> , the capacity limits for (c) <i>Multi-fault monitoring functionality</i> was added.
Command Operations	● In Notes on CLI operation, descriptions in Restrictions on the display of command line completion and Help were changed.
MAC Address Learning	● The following conditions were added as triggers that clear the MAC address table. ■ A flush control frame is received in a configuration using a Spanning Tree Protocol and Ring Protocol. ■ A flush control frame is received in a configuration using GSRP and Ring Protocol. ■ A flush control frame is received when the multi-fault monitoring functionality is enabled.
Description of the Ring Protocol	● A description of the multi-fault monitoring functionality was added.
Settings and Operation for Ring Protocol	● A description of the multi-fault monitoring functionality was added.
Using the Ring Protocol with Spanning Tree Protocols/GSRP	● Descriptions were changed as the Switch supports ring configurations in which a device uses both Ring Protocol and a Spanning Tree Protocol. ● Descriptions were changed as the Switch supports ring configurations in which a device uses both Ring Protocol and a Spanning Tree Protocol.

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

For version 2.3 (Edition 5)
Summary of amendments

Location and title	Changes
Capacity Limit	● In (13) <i>Layer 2 authentication functionality</i>, other capacity limits for common authentication methods were changed. ● (15) Capacity limits for uplink redundancy were added.
Command Operations	● In Notes on CLI operation, descriptions in Restrictions on the display of command line completion and Help were changed.
Login Security and RADIUS	● Descriptions for authentication using RADIUS were changed with the support of RADIUS server group. ● Setting examples for login authentication methods were changed with the support of RADIUS server group. ● Descriptions for authentication using RADIUS were changed with the support of end-by-reject. ● Setting examples for login authentication methods were changed with the support of end-by-reject.
Time Settings and NTP	● A description for checking the time was added.
Device Management	● A description of checking the switch environment and the temperature log was added.
Power Saving Functionality	● A description about start conditions was added to the cooling fan control subsection. ● Descriptions about port power saving were added. ● Descriptions about start mode for the scheduling functionality were changed with the support of automatic cancel of Schedule-disabled mode.
Ethernet	● Notes on connected devices by PoE were added.

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

For version 2.2 (Edition 4)
Summary of amendments

Location and title	Changes
Addition of series	● A description of AX1250S was added.
Switch Configuration	● A description of AX1250S was added. ● Descriptions were added with the support of the 100BASE-FX (SFP).
Capacity Limit	● A description of AX1250S was added. ● Descriptions were added with the support of the 100BASE-FX (SFP).
Time Settings and NTP	● A description of AX1250S was added. ● Descriptions about error locations and recovery processing were added.
Ethernet	● Descriptions were added with the support of the 100BASE-FX (SFP).

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

For version 2.2 (Edition 3)

Summary of amendments

Location and title	Changes
Capacity Limit	● Capacity limits for login security and RADIUS were added. ● Capacity limits for the Ring Protocol were added. ● Capacity limits for authentication method groups were added to IEEE 802.1X, Web authentication, and MAC authentication. ● Capacity limits for custom file sets were added to Web authentication. ● Capacity limits for CFM were added.
Login Security and RADIUS	● A description of the RADIUS server group has been added.
Device Management	● Operation command names for which the input format was changed were added to <i>Compatibility between AX1200S series switches</i>.
Layer 2 Switching Overview	● <i>Restrictions on the Ring Protocol</i> was added to <i>Interoperability of Layer 2 switching and other functionality</i>.
MAC Address Learning	● A description about clearing the MAC address table was added.
Extended VLAN Functionality	● Notes on CFM usage were added to <i>Notes on using the inter-port relay blocking functionality</i>.
Description of the Ring Protocol	● This chapter was added.
Settings and Operation for Ring Protocol	● This chapter was added.
Using the Ring Protocol with Spanning Tree Protocols/GSRP	● This chapter was added.
IPv4 interface	● A description about duplicate IP detection was added.

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

For version 2.1 (Edition 2)

Summary of amendments

Location and title	Changes
Capacity Limit	● Capacity limits for authentication-only RADIUS servers were added to IEEE 802.1X, Web authentication, and MAC authentication.
Login Procedures	● A diagram showing the workflow from starting up to stopping the Switch was changed.
Remote Login	● ftp was added to the list of operation commands.

Location and title	Changes
Login Security and RADIUS	Due to the addition of authentication RADIUS server information, descriptions about selecting RADIUS servers and restoring RADIUS servers were moved to Chapter 5. <i>Overview of Layer 2 Authentication</i> in the <i>Configuration Guide Vol. 2</i>.
Device Management	show cpu and show memory summary were added to the list of operation commands (resource information check).
Power Saving Functionality	- A description of automatic LED operation was added. - A description about port power saving was added. - A description of Switch sleep was added. - A description of cooling fan control was added. - Scheduling of power saving functionality was added.
Layer 2 Switching Overview	A description about link aggregation was deleted from <i>Restrictions on IGMP and MLD snooping in Interoperability of Layer 2 switching and other functionality</i>.
MAC Address Learning	Notes on the aging time when using Layer 2 authentication functionality were added.
VLAN	A description about automatic VLAN allocation to MAC ports during linkage with Layer 2 authentication was added to the notes in <i>Descriptions of MAC VLANs</i>.
Extended VLAN Functionality	Notes on the usage of DHCP snooping and IGMP/MLD snooping were added to <i>Notes on using the inter-port relay blocking functionality</i>.

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

Preface

Applicable products and software versions

This manual applies to the AX2200S, AX1250S, and AX1240S models of switches. The manual describes the functionality in version 2.4 of the software for the AX2200S, AX1250S, and AX1240S series switches that are supported by the software OS-LT4, OS-LT3 and OS-LT2, and by optional licenses.

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

Unless otherwise noted, this manual describes the functions applicable to the AX2200S, AX1250S, and AX1240S. Model-specific functions are indicated as follows:

[AX2200S]:

The information following this label applies only to the AX2200S series.

[AX1250S]:

The description applies to AX1250S series switches.

[AX1240S]:

The description applies to AX1240S series switches.

Unless otherwise noted, this manual describes the functions of the OS-LT4, OS-LT3 and OS-LT2 software. The functions of software supported by optional licenses are indicated as follows:

[OP-WOL]:

The description applies to the OP-WOL optional license.

[OP-OTP]:

The description applies to the OP-OTP optional license.

Corrections to the manual

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

Intended readers

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

Readers must have an understanding of the following:

- The basics of network system management

Manual URL

You can view this manual on our website at:

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

Reading sequence of the manuals

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

- Details on basic settings at initial installation, hardware requirements, and instructions for handling the switch

AX2200S/AX1250S/AX1240S
Hardware Instruction Manual
(AX1240S-H001X)

- Software functionality, configuration, and operation commands

Configuration Guide Vol. 1
(AX1240S-S001X)
Vol. 2
(AX1240S-S002X)

- Proper syntax for configuration commands and details on parameters

Configuration Command
Reference
(AX1240S-S003X)

- Proper syntax for operation commands and details on parameters

Operation Command Reference
(AX1240S-S004X)

- Details on messages and logs

Message Log Reference
(AX1240S-S005X)

- Details on MIBs

MIB Reference
(AX1240S-S006X)

- Handling problems

Troubleshooting Guide
(AX1240S-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
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control

Preface

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
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
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: KB, MB, GB, and TB

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

Conventions: The terms "Switch" and "switch"

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

- AX2200S series switch
- AX1250S series switch
- AX1240S 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.

Contents

Preface	I
Part 1: Overview and Capacity Limits of the Switch	1
1. Overview of the Switch	1
1.1 Overview of the Switch.....	2
1.2 Features of the Switch	3
2. Switch Configuration	7
2.1 Range of Switch models	8
2.1.1 External view.....	9
2.2 Switch components	12
2.2.1 Hardware.....	12
2.2.2 Software	17
3. Capacity Limit	19
3.1 Line and module capacities.....	20
3.1.1 Maximum number of lines.....	20
3.1.2 Installed memory.....	21
3.2 Capacity limits	22
Part 2: Operation Management	39
4. Login Procedures	39
4.1 Terminal-based management.....	40
4.1.1 Operation terminals.....	40
4.1.2 Connection characteristics.....	41
4.1.3 Overview of operation management functionality.....	42
4.2 Starting the switch	43
4.2.1 Workflow from starting to stopping the Switch	43
4.2.2 Starting a switch	44
4.2.3 Stop procedure.....	44
4.3 Login and logout.....	45
5. Command Operations	47
5.1 Command input mode	48
5.1.1 List of operation commands.....	48
5.1.2 Command input mode.....	48
5.2 CLI operations	50
5.2.1 Entry completion	50
5.2.2 Help.....	50
5.2.3 Entry-error detection functionality	51
5.2.4 Abbreviated-command execution	51
5.2.5 History functionality	52
5.2.6 Paging	53
5.2.7 Keyboard command functionality.....	53
5.3 Notes on CLI operation	55
6. Configuration	61
6.1 Configuration	62
6.1.1 Configuration at startup.....	62
6.1.2 Configuration during operation	62
6.2 Overview of editing a running configuration	63
6.3 Mode transitions when entering configuration commands.....	64
6.4 Configuration editing procedures	66
6.4.1 Lists of configuration commands and operation commands	66
6.4.2 Starting configuration editing (configure command and configure terminal command)	67
6.4.3 Displaying and checking configuration entries (show command).....	67

6.4.4 Adding, changing, and deleting configuration entries	69
6.4.5 Saving to the configuration file	70
6.4.6 Ending configuration editing (exit command).....	71
6.4.7 Notes on configuration editing	71
6.5 Configuration operations	72
6.5.1 Transferring files using FTP	72
6.5.2 Transferring files using a memory card.....	73
6.5.3 Notes on applying a backup configuration file	74
7. Remote Login	75
7.1 Description	76
7.2 Configuration	77
7.2.1 List of configuration commands	77
7.2.2 Assigning an IP address to the Switch.....	77
7.2.3 Permitting login by using the Telnet protocol	78
7.2.4 Permitting login by using FTP	78
7.3 Operation.....	79
7.3.1 List of operation commands.....	79
7.3.2 Verifying communication between a remote terminal and the Switch	79
8. Login Security and RADIUS.....	81
8.1 Setting login security	82
8.1.1 Lists of configuration commands and operation commands	82
8.1.2 Overview of login control.....	82
8.1.3 Changing the login user.....	83
8.1.4 Setting the password for switching to administrator mode	83
8.1.5 Permitting login from a remote operation terminal.....	83
8.1.6 Setting the maximum number of concurrent users	84
8.1.7 Restricting login from remote operation terminals	84
8.2 Description of RADIUS.....	86
8.2.1 Overview of RADIUS	86
8.2.2 Application functionality and scope of RADIUS authentication.....	86
8.2.3 Authentication using RADIUS	88
8.2.4 Connecting to RADIUS servers	91
8.3 Configuring RADIUS	93
8.3.1 List of configuration commands	93
8.3.2 Setting authentication methods	93
8.3.3 Configuring a RADIUS server group.....	95
8.4 RADIUS operations	97
8.4.1 List of operation commands.....	97
8.4.2 Displaying the effective RADIUS server information	97
9. Time Settings and NTP.....	99
9.1 Setting and checking the time	100
9.1.1 Supported specifications.....	100
9.1.2 Notes on changing the time	102
9.2 Configuration	103
9.2.1 List of configuration commands	103
9.2.2 Setting the system clock	103
9.2.3 Regularly obtaining time information from the NTP server	104
9.3 Operation.....	105
9.3.1 List of operation commands.....	105
9.3.2 Checking the time	105
9.3.3 Displaying the NTP client information	105
10. Device Management.....	107
10.1 Settings related to status display and system operation.....	108
10.1.1 Lists of configuration commands and operation commands	108
10.1.2 Checking the software version.....	109

10.1.3	Checking the switch status	110
10.1.4	Displaying and stopping display of the operation log on the monitor	112
10.1.5	Viewing logged data.....	112
10.1.6	Functions that use system function resources [AX1250S] [AX1240S].....	112
10.2	Backing up and restoring device information	113
10.2.1	List of operation commands.....	113
10.2.2	Target information to be backed up and restored	113
10.3	Compatibility between AX2200S and AX1200S series switches	115
10.3.1	Compatibility between AX2200S and AX1200S series switches	115
10.3.2	Compatibility of input commands between AX1250S/AX1240S series switches and AX1230S series switches	115
10.3.3	Compatibility of device information between AX1250S series switches and AX1240S series switches	117
10.3.4	Compatibility of device information between AX1250S/AX1240S series switches and AX1230S series switches	118
10.4	Failure recovery.....	121
10.4.1	Error locations and recovery processing	121
11.	Power Saving Functionality	123
11.1	Description of the power saving functionality	124
11.1.1	Supported functionality.....	124
11.1.2	LED behavior.....	125
11.1.3	Port power saving	132
11.1.4	Sleep mode [AX1250S] [AX1240S]	133
11.1.5	Cooling fan control (Semi-fanless operation) [AX1240S]	134
11.1.6	Power saving scheduling	134
11.1.7	Notes when the power saving functionality is used	141
11.2	Power control configuration.....	143
11.2.1	List of configuration commands	143
11.2.2	LED behavior setting	144
11.2.3	Setting power saving for ports in link-down status.....	144
11.2.4	Setting cooling fan control (Semi-fanless operation) [AX1240S]	144
11.2.5	Setting power saving based on scheduling.....	145
11.3	Power control operation.....	147
11.3.1	List of operation commands	147
11.3.2	Displaying the LED behavior.....	147
11.3.3	Displaying the status of port power saving control.....	147
11.3.4	Displaying the status of cooling fan control [AX1240S]	147
11.3.5	Displaying the operating status of the schedule	148
12.	Software Management	149
12.1	List of operation commands	150
12.2	Software update	151
12.2.1	Notes on updating the software	151
Part 3:	Network Interfaces	153
13.	Ethernet	153
13.1	Information common to all Ethernet interfaces	154
13.1.1	Network configuration example	154
13.1.2	Physical interfaces.....	154
13.1.3	Control on the MAC and LLC sublayers	155
13.1.4	MAC address of the Switch.....	156
13.1.5	Order of Ethernet frames	157
13.2	Configuration common to all Ethernet interfaces	159
13.2.1	List of configuration commands	159
13.2.2	Setting Ethernet interface ports [AX2200S]	160
13.2.3	Setting Ethernet interface ports [AX1250S] [AX1240S].....	160
13.2.4	Configuring multiple ports at one time	160

13.2.5 Shutting down a port	161
13.2.6 Setting the link-down detection timer	161
13.2.7 Flow control settings	162
13.2.8 Automatic MDIX functionality settings	162
13.2.9 Using jumbo frames	163
13.3 Operations common to all Ethernet interfaces	165
13.3.1 List of operation commands	165
13.3.2 Checking the Ethernet operating status	165
13.4 Description of Fastethernet [AX1250S] [AX1240S]	166
13.4.1 Functionality	166
13.5 Configuration of Fastethernet [AX1250S] [AX1240S]	172
13.5.1 Configuring ports	172
13.5.2 Flow control settings	173
13.5.3 Automatic MDIX functionality settings	173
13.5.4 Using jumbo frames	173
13.6 Description of Gigabitethernet (RJ45)	174
13.6.1 Functionality	174
13.6.2 Automatic SFP recognition (selection of media type) [AX1250S] [AX1240S] ...	182
13.7 Configuration of Gigabitethernet (RJ45)	183
13.7.1 Configuring ports	183
13.7.2 Flow control settings	184
13.7.3 Automatic MDIX functionality settings	184
13.7.4 Using jumbo frames	184
13.7.5 Setting the media type [AX1250S] [AX1240S]	184
13.8 Description of Gigabitethernet (SFP)	186
13.8.1 Functionality	186
13.8.2 Notes on using SFP	193
13.9 Configuration of Gigabitethernet (SFP)	195
13.9.1 Setting 100BASE-FX ports [AX1250S]	195
13.9.2 Setting a 1000BASE-X port	195
13.9.3 Flow control settings	196
13.9.4 Using jumbo frames	196
13.9.5 Setting the media type [AX1250S] [AX1240S]	196
13.10 Description of PoE [AX2200S] [AX1240S]	197
13.10.1 Overview of PoE	197
13.10.2 Allocating the power supplied by PoE [AX2200S]	197
13.10.3 Allocating power supplied by PoE [AX1240S]	200
13.10.4 Setting behavior of when the maximum power supply is exceeded	201
13.10.5 Resuming and stopping power supply, and the port status	204
13.10.6 Notes on PoE usage	207
13.11 Configuration of PoE [AX2200S] [AX1240S]	209
13.11.1 List of configuration commands	209
13.11.2 Setting the maximum amount of power that can be supplied for system 1 [AX2200S]	209
13.11.3 Setting port priority	210
13.11.4 Setting so that priority is given to powered ports	210
13.11.5 Allocating power that can be supplied to each port	211
13.12 Operation of PoE [AX2200S] [AX1240S]	212
13.12.1 Checking the PoE power supply status	212
14. Link Aggregation	215
14.1 Description of the basic link aggregation functionality	216
14.1.1 Overview	216
14.1.2 Link aggregation configuration	216
14.1.3 Supported specifications	216
14.1.4 MAC address of the channel group	217
14.1.5 Port allocation for sending frames	217
14.1.6 Notes on using link aggregation	217

14.2 Configuration of the basic link aggregation functionality.....	219
14.2.1 List of configuration commands	219
14.2.2 Configuring static link aggregation	219
14.2.3 Configuration of LACP link aggregation.....	220
14.2.4 Configuration of a port channel interface.....	221
14.2.5 Deleting a channel group	224
14.3 Description of the link aggregation extended functionality.....	226
14.3.1 Standby link functionality.....	226
14.4 Configuration of the link aggregation extended functionality	228
14.4.1 List of configuration commands	228
14.4.2 Configuration of the standby link functionality	228
14.5 Operation for link aggregation.....	230
14.5.1 List of operation commands.....	230
14.5.2 Displaying link aggregation information	230
Part 4: Layer 2 Switching.....	233
15. Layer 2 Switching Overview.....	233
15.1 Overview	234
15.1.1 MAC address learning	234
15.1.2 VLAN.....	234
15.2 Supported functions	235
15.3 Compatibility between Layer 2 switch functionality and other functionality	236
16. MAC Address Learning.....	241
16.1 Description of MAC address learning.....	242
16.1.1 Source MAC address learning	242
16.1.2 Aging and MAC address learning	242
16.1.3 Layer 2 switching by MAC address	242
16.1.4 Registering static entries.....	242
16.1.5 Clearing the MAC address table	243
16.1.6 Notes.....	244
16.2 MAC address learning configuration	246
16.2.1 List of configuration commands	246
16.2.2 Setting the aging time	246
16.2.3 Configuring static entries	246
16.3 MAC address learning operation.....	248
16.3.1 List of operation commands.....	248
16.3.2 Checking the status of MAC address learning.....	248
16.3.3 Checking the MAC address learning count	248
17. VLANs.....	251
17.1 Description of the basic VLAN functionality	252
17.1.1 VLAN type	252
17.1.2 Port type.....	252
17.1.3 Default VLAN	253
17.1.4 VLAN priority.....	253
17.1.5 VLAN tags.....	255
17.1.6 Notes on VLAN usage	257
17.2 Configuration of the basic VLAN functionality.....	258
17.2.1 List of configuration commands	258
17.2.2 Configuring VLANs	258
17.2.3 Configuring ports.....	259
17.2.4 Setting trunk ports.....	259
17.3 Description of port VLANs.....	261
17.3.1 Access ports and trunk ports.....	261
17.3.2 Native VLANs.....	261
17.3.3 Notes on regarding port VLAN usage	261
17.4 Configuring port VLANs	262

17.4.1 List of configuration commands	262
17.4.2 Configuring a port VLAN	262
17.4.3 Configuring native VLANs for trunk ports	263
17.5 Description of protocol VLANs	265
17.5.1 Overview	265
17.5.2 Distinguishing protocols	265
17.5.3 Protocol ports and trunk ports	266
17.5.4 Native VLANs for protocol ports	266
17.6 Configuration of protocol VLANs	267
17.6.1 List of configuration commands	267
17.6.2 Creating protocol VLANs	267
17.6.3 Configuring native VLAN for protocol ports	269
17.7 Description of MAC VLANs	271
17.7.1 Overview	271
17.7.2 Connections between switches and MAC address settings	271
17.7.3 Linkage with the Layer 2 authentication functionality	272
17.7.4 Optional functionality of MAC ports	273
17.8 Configuration of MAC VLANs	275
17.8.1 List of configuration commands	275
17.8.2 Configuring MAC VLANs	275
17.8.3 Configuring native VLANs for MAC ports	278
17.8.4 Setting forwarding of tagged frames on a MAC port	278
17.9 VLAN operation	281
17.9.1 List of operation commands	281
17.9.2 Checking VLAN status	281
18. Extended VLAN Functionality	285
18.1 Description of L2 protocol frame transparency functionality	286
18.1.1 Overview	286
18.2 Configuring the L2 protocol frame transparency functionality	287
18.2.1 List of configuration commands	287
18.2.2 Configuring the L2 protocol frame transparency functionality	287
18.3 Description of the inter-port relay blocking functionality	288
18.3.1 Overview	288
18.3.2 Notes on using the inter-port relay blocking functionality	288
18.4 Configuration of the inter-port relay blocking functionality	290
18.4.1 List of configuration commands	290
18.4.2 Configuring the inter-port relay blocking functionality	290
18.4.3 Changing blocked ports	291
18.5 Operation for the VLAN extended functionality	292
18.5.1 List of operation commands	292
18.5.2 Checking VLAN extended functionality	292
19. Spanning Tree Protocol	295
19.1 Overview of Spanning Tree Protocols	296
19.1.1 Overview	296
19.1.2 Types of Spanning Tree Protocols	296
19.1.3 Spanning Tree Protocols and rapid Spanning Tree Protocols	297
19.1.4 Configuration components for Spanning Tree topologies	299
19.1.5 Designing Spanning Tree topologies	300
19.1.6 STP compatibility mode	301
19.1.7 Notes common to Spanning Tree Protocols	303
19.2 Configuration of the Spanning Tree operating mode	304
19.2.1 List of configuration commands	304
19.2.2 Configuring the operating mode	304
19.3 Description of PVST+	307
19.3.1 Using PVST+ to balance load	307
19.3.2 PVST+ for access ports	307

19.3.3 Notes on PVST+ usage	309
19.4 PVST+ configuration	310
19.4.1 List of configuration commands	310
19.4.2 Configuring PVST+	310
19.4.3 Configuring PVST+ topologies.....	311
19.4.4 Configuring PVST+ parameters.....	312
19.5 PVST+ operation	315
19.5.1 List of operation commands.....	315
19.5.2 Checking PVST+ statuses	315
19.6 Description of Single Spanning Tree	316
19.6.1 Overview	316
19.6.2 Usage with PVST+	316
19.6.3 Notes on Single Spanning Tree usage	317
19.7 Configuration of Single Spanning Tree.....	318
19.7.1 List of configuration commands	318
19.7.2 Configuring Single Spanning Tree	318
19.7.3 Configuring topologies for Single Spanning Tree.....	319
19.7.4 Configuring Single Spanning Tree parameters.....	320
19.8 Operation for Single Spanning Tree	323
19.8.1 List of operation commands.....	323
19.8.2 Checking the Single Spanning Tree status	323
19.9 Description of Multiple Spanning Tree.....	325
19.9.1 Overview	325
19.9.2 Designing networks for Multiple Spanning Tree.....	327
19.9.3 Compatibility with other Spanning Tree Protocols	329
19.9.4 Notes on Multiple Spanning Tree usage	330
19.10 Configuration of Multiple Spanning Tree	331
19.10.1 List of configuration commands	331
19.10.2 Configuring Multiple Spanning Tree	331
19.10.3 Configuring topologies for Multiple Spanning Tree	332
19.10.4 Configuring Multiple Spanning Tree parameters.....	334
19.11 Operation for Multiple Spanning Tree.....	337
19.11.1 List of operation commands	337
19.11.2 Checking the Multiple Spanning Tree status	337
19.12 Description of common Spanning Tree functionality	339
19.12.1 PortFast.....	339
19.12.2 BPDU filter	340
19.12.3 Loop guard	340
19.12.4 Root guard	343
19.13 Configuration of the common Spanning Tree functionality	345
19.13.1 List of configuration commands	345
19.13.2 Setting PortFast	345
19.13.3 Setting BPDU filters	346
19.13.4 Configuring loop guards.....	347
19.13.5 Setting root guards.....	347
19.13.6 Configuring link types.....	348
19.14 Operation for common Spanning Tree functionality	349
19.14.1 List of operation commands.....	349
19.14.2 Checking the status of common Spanning Tree functionality	349
20. Description of the Ring Protocol	351
20.1 Overview of the Ring Protocol.....	352
20.1.1 Overview	352
20.1.2 Features	353
20.1.3 Supported specifications.....	355
20.2 Basic Ring Protocol principles.....	356
20.2.1 Network configuration	356
20.2.2 Control VLAN	357

20.2.3	Fault monitoring methods	358
20.2.4	Switching communication paths.....	358
20.3	Overview of single ring operation.....	359
20.3.1	Normal ring operation	359
20.3.2	Operation when a fault is detected	359
20.3.3	Operation when recovery is detected	361
20.4	Overview of multi-ring operation	363
20.4.1	Normal ring operation	363
20.4.2	Operation for shared link faults and restoration.....	365
20.4.3	Operation for faults and restoration other than for shared links in a shared link non-monitoring ring.....	367
20.4.4	Faults and restoration other than for shared links in a shared link monitoring ring	369
20.5	Multi-fault monitoring functionality for the Ring Protocol.....	372
20.5.1	Overview	372
20.5.2	Basic configuration for the multi-fault monitoring functionality.....	373
20.5.3	Overview of operation for multi-fault monitoring	373
20.5.4	Operation when multi-faults occur	374
20.5.5	Operation during multi-fault recovery.....	377
20.6	Ring Protocol network design	380
20.6.1	Using VLAN mappings.....	380
20.6.2	Using forwarding-delay-time for control VLANs.....	380
20.6.3	Prohibited Ring Protocol configurations.....	381
20.6.4	Prohibited configurations for the multi-fault monitoring functionality	381
20.7	Notes on Ring Protocol usage	382
21.	Settings and Operation for the Ring Protocol	385
21.1	Configuration	386
21.1.1	List of configuration commands	386
21.1.2	Flow of Ring Protocol settings	386
21.1.3	Configuring ring IDs	387
21.1.4	Setting control VLANs.....	387
21.1.5	Setting VLAN mappings.....	388
21.1.6	Configuring a VLAN group	389
21.1.7	Settings for modes and ring ports (for single rings and multi-ring configurations without shared links).....	389
21.1.8	Configuring modes and ring ports (for multi-ring configurations with shared links)	390
21.1.9	Setting various parameters	393
21.1.10	Setting the multi-fault monitoring functionality	393
21.2	Operation.....	395
21.2.1	List of operation commands.....	395
21.2.2	Checking Ring Protocol statuses	395
22.	Using the Ring Protocol with Spanning Tree Protocols/GSRP	397
22.1	Using the Ring Protocol with Spanning Tree Protocols.....	398
22.1.1	Overview	398
22.2	Using the Ring Protocol with GSRP.....	400
22.2.1	Operational overview	400
23.	DHCP Snooping	403
23.1	Description of the DHCP snooping functionality	404
23.1.1	Monitoring DHCP packets.....	406
23.1.2	Terminal filtering	409
23.1.3	Forwarding DHCP packets with Option 82	411
23.1.4	Limiting the rate of DHCP packet reception.....	411
23.1.5	Dynamic ARP inspection functionality	412
23.1.6	Saving a binding database.....	415
23.1.7	Notes on using DHCP snooping	417

23.2 Configuration of DHCP snooping	419
23.2.1 List of configuration commands	419
23.2.2 Configuration procedure for DHCP snooping	419
23.2.3 Basic configuration (when DHCP snooping is performed via a Layer 3 switch)	420
23.2.4 When connecting a DHCP relay agent to the Switch	423
23.2.5 Setting the rate of DHCP packet reception	425
23.2.6 Setting the dynamic ARP inspection functionality	425
23.2.7 Setting how to save the binding database	427
23.3 DHCP snooping operation	429
23.3.1 List of operation commands	429
23.3.2 Checking DHCP snooping	429
23.3.3 Checking dynamic ARP inspection	430
24. Description of IGMP Snooping and MLD Snooping	433
24.1 Overview of IGMP snooping and MLD snooping	434
24.1.1 Overview of multicast	434
24.1.2 Overview of IGMP snooping and MLD snooping	434
24.2 Functionality supported for IGMP snooping and MLD snooping	436
24.3 IGMP Snooping	437
24.3.1 MAC address control method	437
24.3.2 Connections with multicast routers	438
24.3.3 IGMP querier functionality	438
24.4 MLD Snooping	440
24.4.1 MAC address control method	440
24.4.2 Connections with multicast routers	441
24.4.3 MLD querier functionality	442
24.5 Notes on IGMP snooping and MLD snooping usage	443
25. Settings and Operation for IGMP Snooping and MLD Snooping	447
25.1 Configuration of IGMP snooping	448
25.1.1 List of configuration commands	448
25.1.2 Configuring IGMP snooping	448
25.1.3 Configuring the IGMP querier functionality	448
25.1.4 Configuring multicast router ports	448
25.2 IGMP snooping operation	450
25.2.1 List of operation commands	450
25.2.2 Checking IGMP snooping	450
25.3 Configuration of MLD snooping	452
25.3.1 List of configuration commands	452
25.3.2 Configuring MLD snooping	452
25.3.3 Configuring the MLD querier functionality	452
25.3.4 Configuring multicast router ports	453
25.3.5 Setting the source IP address of an MLD Query message	453
25.4 MLD snooping operation	454
25.4.1 List of operation commands	454
25.4.2 Checking MLD snooping	454
Part 5: IP Interfaces	457
26. IPv4 Interfaces	457
26.1 Description	458
26.2 Configuration	459
26.2.1 List of configuration commands	459
26.2.2 Configures an interface	459
26.2.3 Setting static routes	459
26.3 Operation	460
26.3.1 List of operation commands	460
26.3.2 Checking the up/down state of an IPv4 interface	460
26.3.3 Checking the reachability to the destination	460

Contents

26.3.4 Checking the route to the destination	461
26.3.5 Checking ARP information	461
26.3.6 Checking the routing table	461
Appendix	463
A. Relevant standards.....	464
A.1 TELNET/FTP	464
A.2 RADIUS	464
A.3 NTP	464
A.4 Ethernet	464
A.5 Link aggregation	465
A.6 VLAN.....	465
A.7 Spanning Tree Protocol	465
A.8 IGMP snooping and MLD snooping.....	466
A.9 IPv4 interface	466
Index	467

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 Features of the Switch

1.1 Overview of the Switch

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

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

Due to their applicability for mission-critical operations, these Switches provide flexible options for building a highly reliable, available, and scalable information network infrastructure.

Product concept

The AX2200S series, AX1250S series, and AX1240S series switches are compact LAN switches that have various forms of functionality including rich authentication functionality. They are very suitable for establishing a floor or workgroup LAN.

The AX2200S series switches are Layer 2 switches supporting Gigabit Ethernet.

The AX1250S series and AX1240S series switches are Layer 2 switches supporting Fast Ethernet.

The Switch delivers the following functionality:

- Support various types of network redundancy for highly reliable and highly available networking.
- Feature link aggregation which provides 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 mission-critical 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 packet forwarding at the full wire rate.
- Support IEEE 802.3af- and IEEE 802.3at-compliant Power-over-Ethernet (PoE), allowing the switch to be positioned freely, regardless of where the power outlet is located. [AX2200S] [AX1240S]
- Support Open Autonomic Networking (OAN) to reduce the total cost of designing, configuring, and operating a network.

1.2 Features of the Switch

(1) Unified lineup

- Providing low-end switches
 - The Switches cover network edges as low-end Ethernet Layer 2 switches and provide consistent connectivity, operability, and interoperability throughout the AX series.
- Gigabit Ethernet Layer 2 switch [AX2200S]
Fast Ethernet Layer 2 switch [AX1250S] [AX1240S]

(2) Support for a wide range of high-speed VLAN functionality

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

(3) Robust security

- Authentication and quarantine solutions
 - Layer 2 authentication methods (IEEE 802.1X, Web authentication, and MAC-based authentication) enable individual PCs to be authenticated and placed into a VLAN, while maintaining the freedom of the physical configuration at the network edges.
 - IEEE 802.1X port-based authentication (static) restricts and releases communicable packets by using status monitoring, which gives permission for full access communication only to terminals that conform to a security policy.
 - Secure Wake-on-LAN allows access to your PC from outside the company, whether you are at home or on a business trip. You can use a Web browser to access a Switch and, via the in-house network, turn on or off the power to a desktop PC within the company^{#1}.
 - One-time password authentication linked with the RSA SecurID system is used for Web authentication, so that network access security can be increased. New PIN mode and Next token mode are also supported^{#1}.
 - Multistep authentication, which aims at granting access only to registered users using legitimate terminals, is supported^{#2}.

#1

To use this feature, a software option license must be purchased separately.

#2

Authentication is conducted in two steps; first the terminal authentication (MAC-based or IEEE 802.1X authentication) is conducted, and then the user authentication (IEEE 802.1X or Web authentication) is conducted.

- Unauthorized DHCP servers and terminals with fixed IP addresses are excluded from networks.
 - Strong security measures are provided via features such as DHCP snooping, which eliminates unauthorized DHCP servers and terminals with fixed IP

addresses.

- Advanced and fine-grained packet filtering
 - Hardware-based high-performance filtering processes
 - Partial specification of L2, L3, or L4 headers
- RADIUS-based switch login and password authentication can be set.

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

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

(5) High reliability for configuring mission-critical networks

- High product quality
 - High reliability assured through exacting component selection and strict design and testing standards
- Variety of redundant network configurations
 - High-speed path switching

Standard functionality, such as link aggregation (IEEE 802.3ad) and high-speed Spanning Tree Protocol (IEEE 802.1w and IEEE 802.1s), and proprietary functionality, such as GSRP-aware and Autonomous Extensible Ring Protocol[#] (abbreviated hereafter to Ring Protocol), allow a redundant high-reliability network to be built. Uplink redundancy, which can build redundant configurations without using a Spanning Tree, is supported.

#

This Switch supports transit nodes only. For details about the Ring Protocol, see *20 Description of the Ring Protocol*.

- Layer 2 loop avoidance
 - UDLD prevents Spanning Tree loops and link aggregation frame loss.
 - The Layer 2 loop detection functionality helps prevent loops by detecting improperly connected devices on the network.

(6) 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 linktraces.
- In addition to the basic MIB-II, supports a wide range of MIBs including RMON.
- Supports port mirroring to monitor and analyze traffic.
- Support for SD memory cards[#]

- Users can easily back up the configuration and save error information.
- Simplified maintenance

#

In the manuals for this series of switches, MC refers to an SD memory card, which appears in the description of operations and display items for an SD memory card.

- The Ethernet ports, console port, and the memory card slot are all on the front panel.
- Device cooling methods appropriate for stable operation
 - The air intake on the front and the air exhaust on the rear (AX2200S), or the air intake on the side and the air exhaust on the rear (AX1240S) reduce the effects of heat vented from other devices, and enable stable operation.

(7) Fanless design (AX2230S-24T, AX1250S-24T2C, and AX1240S-24T2C)

- Problems due to dust sucked into devices decrease, and a quiet office environment (without noise) is achieved.

(8) PoE support

- PoE devices such as IP telephone and wireless LAN AP can be handled (AX2230S-24P and AX1240S-24P2C).
 - Because the work of installing power cables is not required, the inconvenience of increasing cables is removed, the costs for installing power cables are reduced, and the network construction period is shortened.
 - Maximum power supply is 370.0 W.
 - IEEE 802.3af full power supply (Class 3: 15.4 W) allows 24 ports to be powered at the same time.
 - IEEE 802.3at (Class 4: 30.0 W) is supported, allowing any mixture of class 1 to class 3.
 - Ports 0/1 to 0/4 support 60 W power supply. [AX2200S]

(9) Compact design and low environmental impact

- Compact chassis
 - Compact 1U chassis
 - High port density, accommodating a maximum of 48 10BASE-T and 100BASE-TX ports
- RoHS compliant with reduced environmental impact.

(10) Power saving

- Schedule functionality
 - The switches can switch automatically to a sleep state and be woken up from the sleep state, in accordance with the schedule settings for long holidays, Saturdays, Sundays, public holidays, and evenings. [AX1250S] [AX1240S]
 - The LED operation and port power saving described below can be set up by schedule settings.
- LED operation control
 - LED operation is controlled in two steps: normal brightness and off. [AX2200S]
 - LED operation is controlled in three steps: normal brightness, power saving brightness (operation with lower brightness than normal), and off. [AX1250S] [AX1240S]

1 Overview of the Switch

- LEDs can be set to blink or turn on in normal brightness when consoles are connected to the switches, 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 operations are completed.
- Port power saving
 - To save power, the power to a port is shut off when a link-down is detected at the port or the port is blocked (the shutdown setting is configured by using configuration commands).[#]

#

An SFP port supports only port power saving by blocking the port.

(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 *AX-Config-Master part* in the *OAN User's Guide*.

2. Switch Configuration

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

2.1 Range of Switch models

2.2 Switch components

2.1 Range of Switch models

These Switches are 1U size box-type Ethernet switches. AX2200S series switches are equipped with a maximum of 24 10BASE-T, 100BASE-TX, and 1000BASE-T ports. AX1250S series switches are equipped with a maximum of 24 10BASE-T and 100BASE-TX ports. AX1240S series switches are equipped with a maximum of 48 10BASE-T and 100BASE-TX ports.

AX1250S series switches inherit the functionality of AX1240S series switches, and their concept is high reliability and improved environmental resistance (operation environment up to 50 degrees Celsius).

AX2200S series, AX1250S series, and AX1240S series switches are equipped with link aggregation, VLAN, the Spanning Tree Protocol, DHCP snooping, IGMP/MLD snooping, and Layer 2 authentication. They provide advanced filtering and QoS functionality, and support wire-rate and non-blocking switching.

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

Table 2-1 Switch models by maximum number of ports

Categorized by maximum number of ports [#]		Model
10BASE-T/100BASE-TX/1000BASE-T 1000BASE-X	24 ports 4 ports	AX2230S-24T
10BASE-T/100BASE-TX/1000BASE-T (PoE/PoE Plus) 10BASE-T/100BASE-TX/1000BASE-T (PoE/PoE Plus/60 W power supply) 1000BASE-X	24 ports 4 ports 4 ports	AX2230S-24P
10BASE-T/100BASE-TX 10BASE-T/100BASE-TX/1000BASE-T or 1000BASE-X	24 ports 2 ports	AX1250S-24T2C AX1240S-24T2C
10BASE-T/100BASE-TX 10BASE-T/100BASE-TX/1000BASE-T or 1000BASE-X	48 ports 2 ports	AX1240S-48T2C
10BASE-T/100BASE-TX (PoE/PoE Plus) 10BASE-T/100BASE-TX/1000BASE-T or 1000BASE-X	24 ports 2 ports	AX1240S-24P2C

#

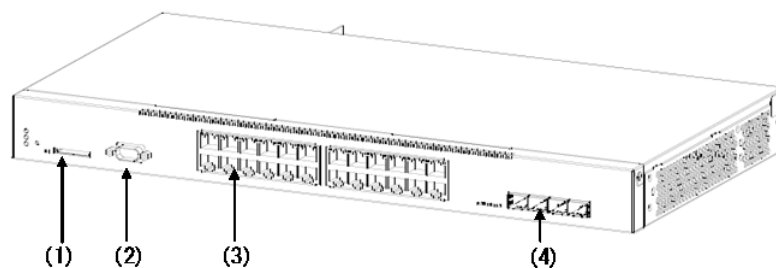
For details on the maximum number of ports that can be used concurrently, see [3.1 Line and module capacities](#).

2.1.1 External view

External views of the models are shown below.

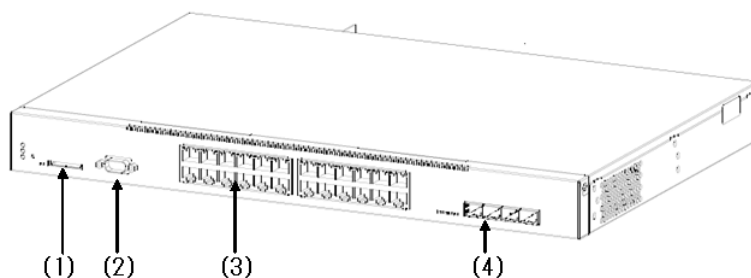
(1) AX2200S series

Figure 2-1 AX2230S-24T model



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

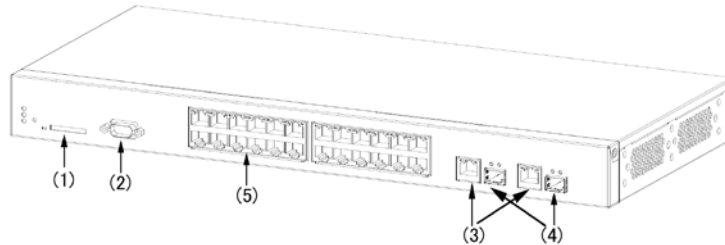
Figure 2-2 AX2230S-24P model



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

(2) AX1250S Series

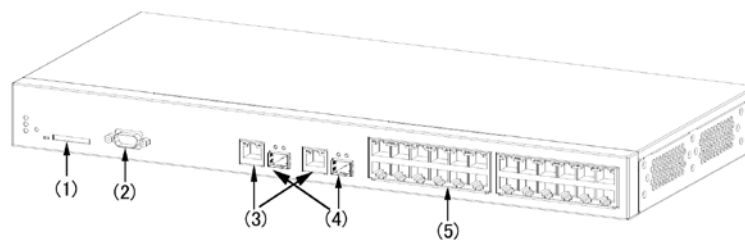
Figure 2-3 AX1250S-24T2C model



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

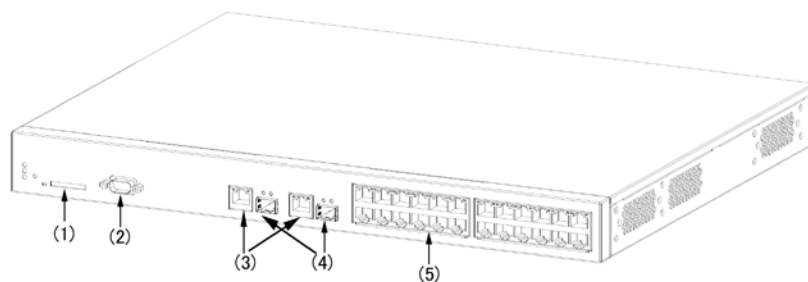
(3) AX1240S Series

Figure 2-4 AX1240S-24T2C model



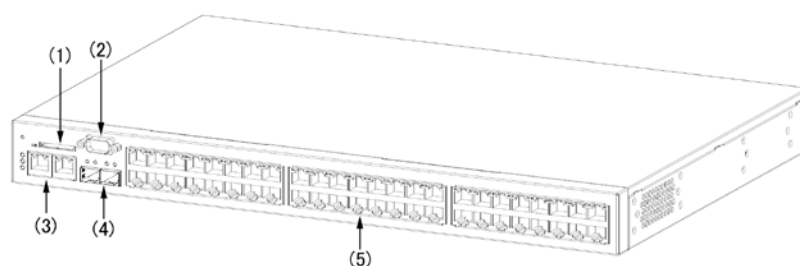
- (1) Memory card slot
- (2) CONSOLE port
- (3) 10BASE-T/100BASE-TX/1000BASE-T Ethernet ports
- (4) SFP slot
- (5) 10BASE-T/100BASE-TX Ethernet ports

Figure 2-5 AX1240S-24P2C model



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

Figure 2-6 AX1240S-48T2C model



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

2.2 Switch components

2.2.1 Hardware

The models of this Switch are designed under a uniform architecture.

The following figures show the hardware configuration.

(1) AX2200S series

Figure 2-7 Hardware configuration (AX2230S-24T model)

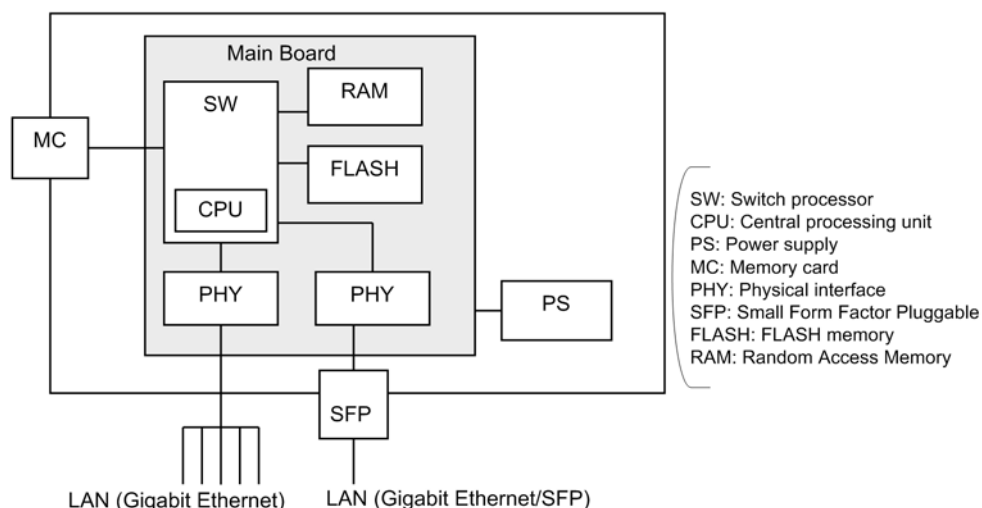
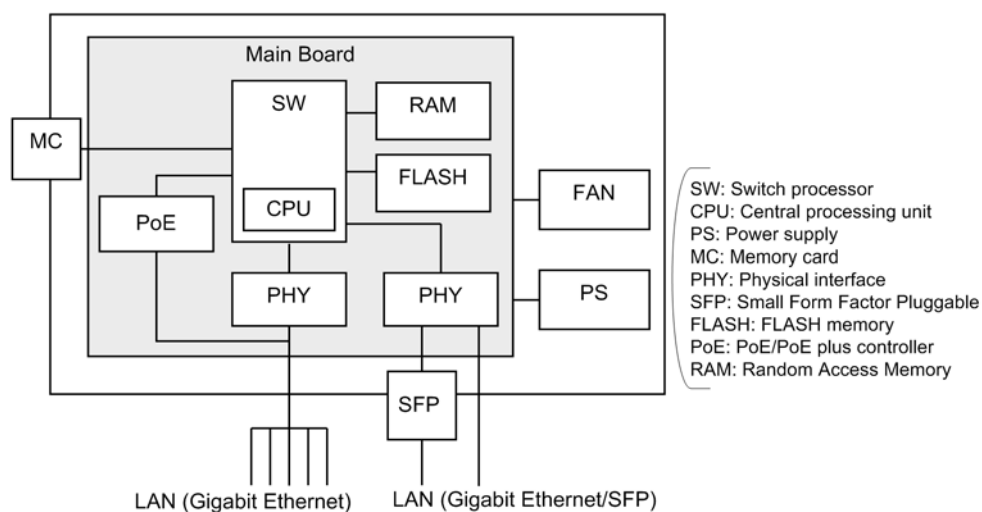


Figure 2-8 Hardware configuration (AX2230S-24P model)



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

(a) Main board

The main board consists of the CPU subunit, SW subunit, memory card (MC), flash subunit, PHY subunit, and PoE subunit.

- CPU (central processing unit) subunit
Switch-wide management, PHY subunit control, and protocol processing are performed by software.
The software is stored in internal flash memory installed on the flash subunit.
- SW (switch processor)
This subunit performs L2 frame switching. The SW subunit performs hardware-based processing including MAC address learning and aging, link aggregation, filter or QoS table lookups, and DMA transfers of incoming and outgoing frames. Such processing makes high-speed frame switching possible.
- MC (memory card)
MC slot.
An SD card is used as a memory card for storing configuration files and failure information.
- Flash subunit (flash memory)
This subunit stores software, configuration files, and log data.
- PHY (physical interface) subunit
This interface subunit supports various kinds of media.
- PoE/PoE Plus/PoE (60 W power supply) subunit (AX2230S-24P model)
A Gigabit Ethernet port supplies a maximum of 60 W power (port 0/1 to 0/4) or a maximum of 30 W power (port 0/5 to 0/24) to power-receiving devices.

(b) PS (power supply)

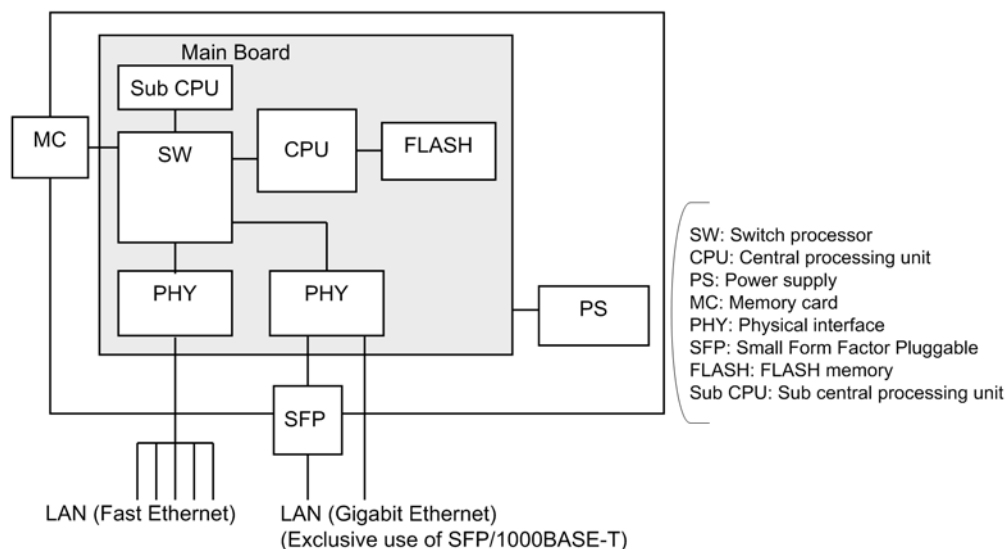
The power supply converts power from an external source to DC power that can be used inside the Switch. To replace the PS unit, you must stop and replace the whole Switch.

(c) FAN (AX2230S-24P model)

The Switch is equipped with fans that cool the inside of the Switch.

(2) AX1250S Series

Figure 2-9 Hardware configuration (AX1250S-24T2C model)



The Switch chassis includes the main board and a power supply (PS) unit.

(a) Main board

The main board consists of the CPU subunit, SW subunit, memory card (MC), flash subunit, PHY subunit, and Sub-CPU subunit.

- CPU (central processing unit) subunit
 Switch-wide management, PHY subunit control, and protocol processing are performed by software.
 The software is stored in internal flash memory installed on the flash subunit.
- SW (switch processor)
 This subunit performs L2 frame switching. The SW subunit performs hardware-based processing including MAC address learning and aging, link aggregation, filter or QoS table lookups, and DMA transfers of incoming and outgoing frames. Such processing makes high-speed frame switching possible.
- MC (memory card)
 MC slot.
 An SD card is used as a memory card for storing configuration files and failure information.
- Flash subunit (flash memory)
 This subunit stores software, configuration files, and log data.
- PHY (physical interface) subunit
 This interface subunit supports various kinds of media.
- Sub-CPU (sub-central processing unit) subunit
 This subunit monitors the temperature sensor.

(b) PS (power supply)

The power supply converts power from an external source to DC power that can be used inside the Switch. To replace the PS unit, you must stop and replace the whole Switch.

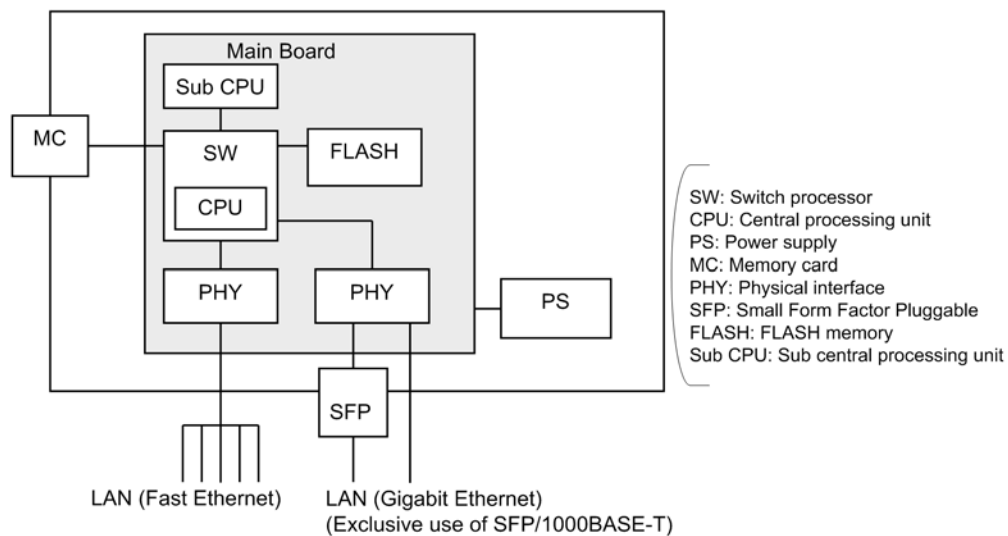
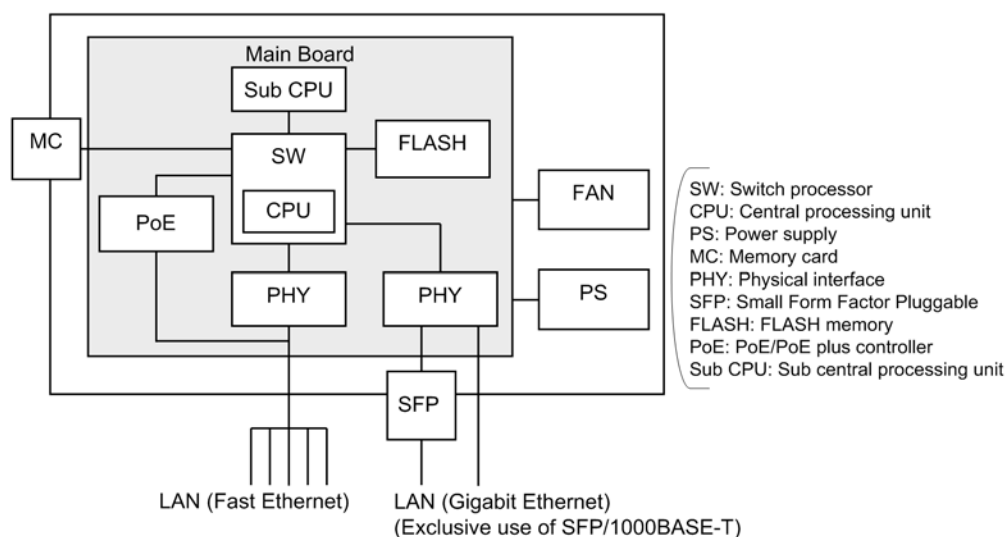
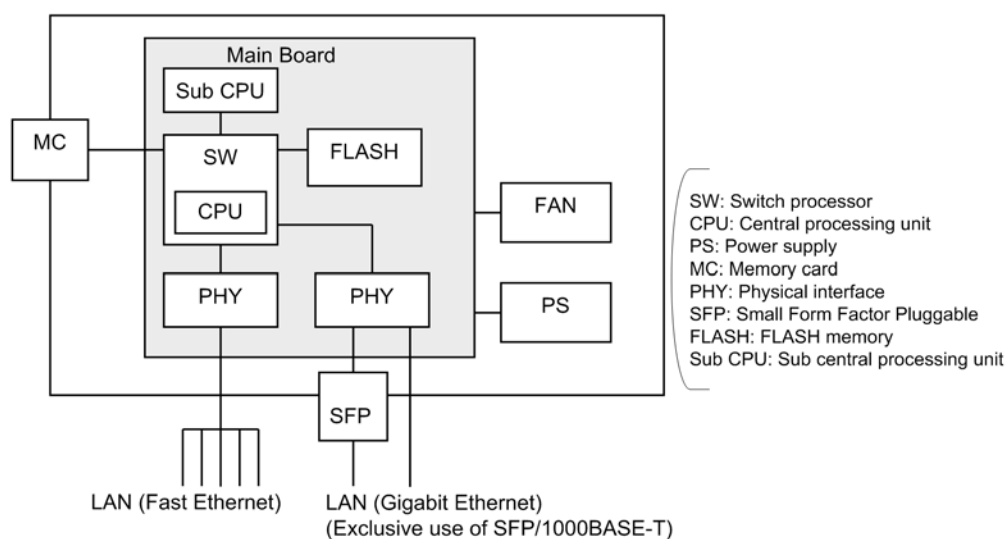
(3) AX1240S Series**Figure 2-10** Hardware configuration (AX1240S-24T2C model)**Figure 2-11** Hardware configuration (AX1240S-24P2C model)

Figure 2-12 Hardware configuration (AX1240S-48T2C model)



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

(a) Main board

The main board consists of the SW subunit, memory card (MC), flash subunit, PHY subunit, Sub-CPU subunit, and PoE subunit.

- CPU (central processing unit) subunit
Switch-wide management, PHY subunit control, and protocol processing are performed by software.
The software is stored in internal flash memory installed on the flash subunit.
- SW (switch processor)
This subunit performs L2 frame switching. The SW subunit performs hardware-based processing including MAC address learning and aging, link aggregation, filter or QoS table lookups, and DMA transfers of incoming and outgoing frames. Such processing actualizes 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 subunit (flash memory)
This subunit stores software, configuration files, and log data.
- PHY (physical interface) subunit
This interface subunit supports various kinds of media.
- Sub-CPU (sub-central processing unit) subunit
This subunit monitors the temperature sensor.
- PoE or PoE Plus subunit (AX1240S-24P2C model)
This subunit supplies a maximum of 30 W power per port to Fast Ethernet ports and power-receiving devices.

(b) PS (power supply)

The power supply converts power from an external source to DC power that can be used inside the Switch. To replace the PS unit, you must stop and replace the whole Switch.

(c) FAN (AX1240S-24P2C and AX1240S-48T2C models)

The Switch is equipped with fans that cool the inside of the Switch.

2.2.2 Software

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

Table 2-2 Which model supports which software

Model	Software abbreviation	Description
AX2200S	OS-LT4	Software for AX2200S Such as L2 switch forwarding, VLAN, the Spanning Tree Protocol, SNMP, and LLDP
AX1250S	OS-LT3	Software for AX1250S Such as L2 switch forwarding, VLAN, the Spanning Tree Protocol, SNMP, and LLDP
AX1240S	OS-LT2	Software for AX1240S Such as L2 switch forwarding, VLAN, the Spanning Tree Protocol, SNMP, and LLDP

The following table describes the optional licenses of the Switch. Optional licenses are used in common by AX2200S, AX1250S and AX1240S series switches.

Table 2-3 Optional licenses used in the Switch

Optional license abbreviation	Description
OP-WOL	Secure Wake-on-LAN
OP-OTP	One-time password authentication

3. Capacity Limit

This chapter describes the capacity limits for the Switch.

3.1 Line and module capacities

3.2 Capacity limits

3.1 Line and module capacities

3.1.1 Maximum number of lines

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

Table 3-1 Maximum number of lines

Model	Ethernet						
	10/100BASE-TX	10/100BASE-TX	10/100/1000BASE-T			100BASE-FX 1000BASE-X	1000BASE-X
	RJ45	PoE/ PoE Plus	RJ45	PoE/ PoE Plus	PoE/PoE Plus/60W power supply	SFP	SFP
AX2230S-24T	n/a	n/a	24	n/a	n/a	n/a	4
AX2230S-24P	n/a	n/a	n/a	20	4	n/a	4
AX1250S-24T 2C	24	n/a	2 [#]	n/a	n/a	2 [#]	n/a
AX1240S-24T 2C	24	n/a	2 [#]	n/a	n/a	n/a	2 [#]
AX1240S-24P 2C	n/a	24	2 [#]	n/a	n/a	n/a	2 [#]
AX1240S-48T 2C	48	n/a	2 [#]	n/a	n/a	n/a	2 [#]

Legend n/a: Not applicable.

#

These ports are mutually exclusive and cannot be used concurrently.

If you use 10BASE-T, 100BASE-TX, or 1000BASE-T, subtract the number of such lines from the maximum number of lines for SFP.

3.1.2 Installed memory

The table below describes the amount of memory installed on the main board and available memory card capacity. Memory cannot be expanded for the Switch.

Table 3-2 Amount of memory installed on the main board, and capacity of the internal flash memory and memory card

Item	AX2200S series	AX1250S Series	AX1240S Series
Capacity of the memory installed on the main board (including the RAMDISK)	128 MB (12MB for the RAMDISK)	128 MB (12MB for the RAMDISK)	128 MB (12MB for the RAMDISK)
Capacity of the internal flash memory	16 MB	16 MB	16 MB

(1) RAMDISK

The RAMDISK is used as a temporary storage area when a file is copied from the Switch to a memory card, or from a memory card to the Switch.

For example, prior to the operations below, the target file is temporarily copied to the RAMDISK.

- Example 1: Copy the configuration file from the Switch to a memory card.
- Example 2: Register the Web authentication window replacement file created on the PC in the Switch.

After the file is copied to a memory card or registered in the Switch, the file on the RAMDISK is no longer required. Use an operation command to delete the file on the RAMDISK.

Restarting the Switch deletes the file on the RAMDISK.

3.2 Capacity limits

(1) Login Security and RADIUS

The following tables describe the maximum number of remote operation terminal logins allowed to the Switch, and the maximum number of RADIUS server information registrations.

Table 3-3 Maximum number of remote operation terminal logins allowed to the Switch

Model	telnet	ftp
All models	2	1

Table 3-4 Number of RADIUS server information registrations

Model	RADIUS server information Type	Number of information entries that can be registered	Quotable/not quotable to the RADIUS server group information	Number of groups that can be registered	Number of servers that can be registered in the RADIUS server group
All models	General-use RADIUS server information	20	Quotable	4/device	4/group
	IEEE 802.1X authentication RADIUS server information	4	Not quotable	--	--
	RADIUS server information for Web authentication	4	Not quotable	--	--
	RADIUS server information for MAC-based authentication	4	Not quotable	--	--

Legend --: Not supported

(2) Link aggregation

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

Table 3-5 Link aggregation capacities

Model	Maximum number of ports per channel group	Maximum number of channel groups per device
All models	8	8

(3) MAC Address Table

The Layer 2 switch functionality allows the MAC addresses of any connected hosts to be dynamically learned and entered in the MAC address table. Static entry of MAC addresses is also supported.

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

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

Model	Per device	
	Maximum number of entries	Number of static entries
All models	16,384 [#]	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 a configuration command for the Switch.

(4) 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 number of VLANs across all ports on the switch
AX2230S-24T AX2230S-24P	256	256	7,168
AX1250S-24T2C AX1240S-24T2C AX1240S-24P2C	256	256	6,656
AX1240S-48T2C	256	256	12,800

Note:

ALAXALA Networks Corporation recommends that you configure no more than 256 VLANs.

The 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.

A maximum of 256 VLANs can be set for this Switch. Of that number, the maximum number of VLANs (VLAN interfaces) to which IP addresses can be assigned is 128.

(a) Protocol VLAN

A protocol-based VLAN identifies protocols based on the values of the Ethernet-Type, LLC SAP, and SNAP type fields in an Ethernet frame. The following table describes the number of discrete protocols that can be configured on a switch.

Table 3-8 Maximum number of discrete protocols in a protocol-based VLAN

Model	Per port	Per device
All models	16	16

Table 3-9 Maximum number of protocol-based VLANs

Model	Per port	Per device
All models	48 [#]	48

#

The maximum protocol-based VLANs supported by a trunk port. A protocol port can support a maximum of 16 protocol-based VLANs.

(b) MAC VLAN

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

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

Model	Maximum number of MAC addresses registered by a configuration command	Maximum number of MAC addresses registered by Layer 2 authentication	Maximum number of MAC addresses that can be registered concurrently
All models	64	256 [#]	320

#

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

(5) Spanning Tree Protocol

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

Table 3-11 PVST+ capacity limitats

Model	Number of applicable VLANs	VLAN ports ^{#1}
All models	250	256 ^{#2}

#1

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

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

#2

Excludes ports that have PortFast enabled.

Table 3-12 Capacity limits for a Single-instance Spanning Tree

Model	Number of applicable VLANs	VLAN ports ^{#1}	VLAN ports ^{#1} (when PVST+ also used ^{#2})
All models	256 ^{#3}	1,024	256

#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 will be $100 \times 2 = 200$.

#2

The value of 256 includes the number of ports subject to PVST+.

#3

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

Table 3-13 Capacity limits for a Multiple Spanning Tree

Model	Number of applicable VLANs	VLAN ports ^{#1}	Number of MST instances	Number of VLANs in each MST instance ^{#2}
All models	256	1,024	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.

(6) Ring Protocol

(a) Ring Protocol

The following table describes the capacity limits for Ring Protocol.

Table 3-14 Capacity limits of the Ring Protocol

Item	Per ring	Per device
Number of rings	n/a	4
Number of VLAN mappings	n/a	128
Number of VLAN groups	2	8
Number of VLANs in a VLAN group	255 ^{#1, #3}	255 ^{#1, #3}
Number of ring ports ^{#2}	2	8

3 Capacity Limit

Legend n/a: Not applicable

#1

The maximum recommended number of VLANs for a switch.

A maximum of 256 VLANs are available for this Switch. However, a maximum of 255 VLANs are available for VLAN groups because the control VLAN needed for each ring accounts for one VLAN. As the number of rings increases, the number available for VLAN groups decreases.

#2

Each channel group is counted as one port.

#3

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

(b) Virtual links

This Switch does not support setting of virtual links. (The Switch only supports forwarding of virtual link control frames and receipt of flash control frames.)

(c) Multi-fault monitoring functionality

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

Table 3-15 Capacity limits for the multi-fault monitoring functionality

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

(7) DHCP snooping

The following table describes the Switch's capacity limits for DHCP snooping.

Table 3-16 Capacity limits of DHCP snooping

Item	Maximum number
Number of configurable VLANs	32
Total number of binding database entries	246
Number of binding database static entries [#]	64

#

The total number of binding database entries includes static entries.

(8) IGMP snooping and MLD snooping

The following table shows the capacity limits for IGMP/MLD snooping. Multicast MAC addresses learned in IGMP/MLD snooping are registered in the MAC address table. The following table shows the number of multicast MAC addresses that can be registered.

Table 3-17 Capacity limits of IGMP/MLD snooping

Item	Maximum number
Number of configured VLANs ^{#1, #3}	32
Registered entries ^{#2, #3}	500

#1

The sum of the ports on which IGMP/MLD snooping operates (sum of ports included in the VLANs configured for IGMP/MLD snooping) cannot be larger than 512 for all devices. For example, if IGMP/MLD snooping is enabled in 16 VLANs, each of which has 10 ports, there will be 160 IGMP/MLD snooping-enabled ports.

#2

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

#3

The number of entries means the total number of entries used in IGMP/MLD snooping. If both IGMP snooping and MLD snooping are set for the same VLAN, the number of VLANs is 2.

(9) Number of interfaces

In the Switch, you can assign IP addresses to VLANs. This subsection describes the maximum number of VLAN interfaces to which IP addresses can be assigned. It also explains the maximum number of assignable IP addresses.

(a) Maximum number of interfaces

The table below describes the maximum number of interfaces supported by the Switch.

Table 3-18 Maximum number of interfaces

Model	Maximum number of interfaces (per device)
All models	128

(b) Maximum number of multi-homed subnets

The Switch does not support multihoming.

(c) Maximum number of IP addresses

(i) IPv4 addresses

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

Table 3-19 Maximum number of IPv4 addresses that can be set for a switch by a configuration command

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

(10) Maximum number of partner devices

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

(a) Number of ARP entries

For IPv4, the hardware address corresponding to the destination address of the frame to be sent is determined by ARP in the LAN. Therefore, the maximum number of partner devices for this media depends on the number of ARP entries. The following table describes the maximum number of ARP entries supported by the Switch.

Table 3-20 Maximum number of ARP entries

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

(11) Maximum number of dynamic entries and static entries

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

This Switch supports static routing only, and does not support any routing protocols, such as RIP, RIPv2, OSPF, or OSPFv3.

Table 3-21 Maximum number of dynamic and static entries

Category	Item	Maximum number of device entries	Maximum number of dynamic entries	Maximum number of static entries
IPv4	Unicast route entries	128 [#]	--	128 [#]

Legend --: Not supported

[#]: Does not include the number of direct routes.

(12) Filtering 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 filter and QoS control. Select a flow detection mode to determine resource allocation based on the filter and QoS detection conditions. The conditions for determining the maximum allowable flow entries differ according to the mode you select. Settings for filter and QoS can be specified on the receiving-side only. Set the flow entries within the range of per-interface entry limits for the particular interface and device model you are using.

(a) Number of filter entries on the receiving side

The table below describes the maximum number of filter entries that can be set when you select the layer2-1 or layer2-2 flow detection mode for the receiving side. The flow detection condition depends on the selected mode. If the layer2-1 mode is selected, the MAC condition can be used. If the layer2-2 mode is used, the IPv4 condition can be used.

Table 3-22 Maximum number of filter entries on the receiving side in modes layer2-1 and layer 2-2

Model	Maximum number of filter entries on the receiving side [#]		
	Interface type	Per interface	Per switch
All models	Ethernet	128	128
	VLAN	128	128

#

When a filter entry is added, a discard entry, which is enabled when flow is undetected, is automatically added to the Ethernet interface or VLAN interface. Therefore, not all of the filter entries can be used. 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: 126.

Example 2:

Entry condition: Two entries are assigned to Ethernet interface 0/1 and three entries are assigned to 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: 121.

(b) Number of QoS entries on the receiving side

The table below describes the maximum number of QoS entries that can be set when you select the layer2-1 or layer2-2 flow detection mode for the receiving side. The flow detection condition depends on the selected mode. If the layer2-1 mode is selected, the MAC condition can be used. If the layer2-2 mode is used, the IPv4 condition can be used.

Table 3-23 Maximum number of QoS entries on the receiving side in layer2-1 and layer2-2 modes

Model	Maximum number of receiving-side QoS entries		
	Interface type	Per interface	Per switch
All models	Ethernet	64	64
	VLAN	64	64

(13) Layer 2 authentication functionality

The following table describes the number of terminals to be authenticated for the entire Switch.

Table 3-24 Number of terminals to be authenticated for the entire Switch[#]

Authentication mode	Authentication type	Number of terminals per authentication type	Entire system
Fixed VLAN mode	IEEE802.1X	256	
	Web Authentication	1024	
	MAC-based Authentication	1024	
	Maximum total number of authentication terminals in fixed VLAN mode		1024
Dynamic VLAN mode Legacy mode	IEEE802.1X	256	
	Web Authentication	256	
	MAC-based Authentication	256	
	Maximum total number of authentication terminals in dynamic VLAN mode and legacy mode		256
Maximum total number of terminals for all authentication types and modes within the entire system			1280

#

If DHCP snooping is also used, the maximum number of terminals is limited to 246.

Table 3-25 Other capacity limits for common Layer 2 authentication methods

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 device including the login security function.

#2

If the specified number of filter entries exceeds the capacity limit, only the entries 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.

(a) IEEE802.1X

The following table describes the capacity limits for IEEE 802.1X.

Table 3-26 Maximum number of terminals that can be authenticated for IEEE 802.1X^{#1}

Authentication mode		Port-based		Per-VLAN		Entire system	
		Maximum number of terminals	Limit on the number of terminals that can be authenticated ^{#2}	Maximum number of terminals	Limit on the number of terminals that can be authenticated ^{#2}	Maximum number of terminals	Limit on the number of terminals that can be authenticated ^{#2}
Port-based authentication	(static)	64	No			256	No
	(dynamic)	64	No			256	No
VLAN-based authentication	(dynamic)			256	No	256	No
Maximum number of terminals allowed in all IEEE 802.1X authentication modes (total number of terminals per port and per VLAN)						256	No

#1

If DHCP snooping is also used, the maximum number of terminals is limited to 246.

#2

In IEEE 802.1X, a limit on the number of terminals that can be authenticated cannot be set.

Table 3-27 Capacity limits for IEEE 802.1X

Item		Maximum number
Number of registered authentication method groups	Switch default	1
	Authentication method list	4
Number of registered IEEE 802.1X authentication RADIUS servers ^{#1}		4
Maximum physical ports for IEEE 802.1X	All models	Maximum physical ports for the device
Maximum number of excluded terminals for the authentication exclusion option	MAC address table static registration	256/device ^{#2}
	MAC address static registration in MAC VLAN	64/device ^{#3}

3 Capacity Limit

#1

The number of registered servers with the RADIUS account functionality is determined by the authentication RADIUS server setting (IEEE 802.1X authentication RADIUS server or general-use RADIUS server setting).

#2

Number of static entries in the MAC address table

#3

Maximum number of MAC addresses that can be registered due to the configuration's MAC VLAN capacity limits

(b) Web Authentication

The following table describes the capacity limits for Web authentication.

Table 3-28 Maximum number of Web authenticated users^{#1}

Authentication mode	Port-based		Per-VLAN		Entire system	
	Maximum number of users	Limit on the number of terminals that can be authenticated	Maximum number of users	Limit on the number of terminals that can be authenticated	Maximum number of users	Limit on the number of terminals that can be authenticated
Fixed VLAN mode	1,024	Yes			1,024	Yes
Dynamic VLAN mode	256	Yes			256	Yes
Legacy mode			256	No	256	Yes
Maximum number of users in all Web authentication modes (Total for fixed VLAN mode, dynamic VLAN mode, and legacy mode)					1280	No ^{#2}

#1

If DHCP snooping is also used, the maximum number of terminals is limited to 246.

#2

A limit cannot be set on the number of authenticated users in all Web authentication modes.

Table 3-29 Capacity limits for Web authentication

Item		Maximum number
Number of registered authentication method groups	Switch default	1
	Authentication method list	4
Number of registered Web authentication RADIUS servers ^{#1}		4
Registered users in the internal Web authentication DB		300 ^{#2}
Total size of files that can be specified in Web authentication page switching		256 KB/device ^{#3}
	Number of registered Web authentication page custom file sets ^{#4}	5/device File sets: Basic Web authentication pages: 1 Individual Web authentication pages: 4
	Number of files per file set	64
DHCP Server Functionality	Number of address pools (network)	32
	Number of address pools (host/mac)	N (Not supported)
	Number of IP addresses that can be distributed	512
	Number of addresses that are excluded from assignment	64

#1

The number of registered servers with the RADIUS account functionality is determined by the authentication RADIUS server setting (Web authentication RADIUS server or general-use RADIUS server).

#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 is the total of all the basic Web authentication pages and individual Web authentication pages. Because the file area includes a management area, the value is actually reduced to 240 KB. The area might also become smaller depending on the sizes of files.

#4

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

(c) MAC-based Authentication

The following table describes the capacity limits for MAC-based authentication.000

Table 3-30 Maximum number of MAC-based authentication terminals^{#1}

Authentication mode	Port-based		Per-VLAN		Entire system	
	Maximum number of terminals	Limit on the number of terminals that can be authenticated	Maximum number of terminals	Limit on the number of terminals that can be authenticated	Maximum number of terminals	Limit on the number of terminals that can be authenticated
Fixed VLAN mode	1,024	Yes			1,024	Yes
Dynamic VLAN mode	256	Yes			256	Yes
Legacy mode			256	No	256	Yes
Maximum number of terminals in all MAC-based authentication modes (Total for fixed VLAN mode, dynamic VLAN mode, and legacy mode)					1,280	No ^{#2}

#1

If DHCP snooping is also used, the maximum number of terminals is limited to 246.

#2

A limit cannot be set on the number of authenticated users across MAC-based authentication modes.

Table 3-31 Capacity limits of MAC-based authentication

Item		Maximum number
Number of registered authentication method groups	Switch default	1
	Authentication method list	4
Number of registered MAC-based authentication RADIUS servers [#]		4
Number of MAC addresses to be registered in the internal MAC-based authentication DB		1,024

#

The number of registered servers with the RADIUS account functionality is determined by the authentication RADIUS server setting (MAC-based authentication RADIUS server or general-use RADIUS server).

(14) Secure Wake-on-LAN [OP-WOL]

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

Table 3-32 Capacity limits for the Secure Wake-on-LAN functionality

Item	Maximum number
Maximum number of users who can use the secure Wake-on-LAN function concurrently	32 ^{#1}
Maximum number of terminals that can be registered in the internal DB used to register the terminal that sends the startup command	300
Maximum 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

Secure Wake-on-LAN functionality manages a single user from user authentication to the completion of the terminal startup confirmation.

Therefore, if a long timeout value is used when confirming a startup with the internal DB (used to register the terminals that send the startup command), the number of managed entries for concurrent users might become saturated, causing the Secure Wake-on-LAN functionality to become unavailable.

#2

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

(15) Uplink redundancy

The following figure shows the capacity limits for uplink redundancy.

Table 3-33 Capacity limits for uplink redundancy

Model	Number of uplink ports	Number of attached interfaces per uplink port
AX2230S-24T AX2230S-24P	14	2
AX1250S-24T2C AX1240S-24T2C AX1240S-24P2C	13	2
AX1240S-48T2C	25	2

Table 3-34 Capacity limits for the MAC address update functionality

Model	Maximum number of outgoing MAC address entries
All models	1024

(16) IEEE 802.3ah/UDLD

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

Table 3-35 Capacity limits for IEEE 802.3ah/UDLD

Model	Maximum number of link monitoring information items
All models	Maximum physical ports for the device

(17) L2 Loop Detection

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

Table 3-36 Transmission rate for L2 loop detection frames

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

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

$$\text{Number of ports and VLANs subject to L2 loop detection}^{\#2} / \text{frame transmission rate (pps)} \leq \text{transmission interval (sec.)}$$

#1

Frames that exceed 20 (packets/s) will not be sent. Loop failures cannot be detected on target ports or VLANs from which frames have not been sent.

#2

$$\text{Number of ports subject to L2 loop detection} \times \text{number of VLANs subject to L2 loop detection}$$

(18) CFM

The following table describes the capacity limits for CFM.

Table 3-37 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/device	32/device	32/device	32/device	256/device	2016/device

#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

Each channel group is counted as one port. You can check the total number of CFM ports using the `show cfm summary` 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 transmission interval. The capacity

limits of the total number of CFM ports and total number of remote MEPs change if you change the CCM transmission interval. The following table describes the capacity limits for total CFM ports and total remote MEPs according to the set CCM transmission interval.

Table 3-38 Capacity limits based on CCM transmission interval

Model	Interval for sending CCMs	Total number of CFM ports	Total number of remote MEPs
All models	1 minute or longer	256/device	2016/device
	10 seconds	100/device	640/device
	1 seconds	50/device	64/device

#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 3-39 Capacity limits for CFM physical ports and channel groups

Model	Total number of physical ports and channel groups to which MEP or MIP can be assigned [#]
All models	8/device

#

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

Table 3-40 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/device	1024/device 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).

(19) Neighboring device information (LLDP)

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

Table 3-41 Capacity limits for storing adjacent device information (LLDP)

Model	Item	Maximum capacity
AX2230S-24T AX2230S-24P	LLDP neighboring device information	28
AX1250S-24T2C AX1240S-24T2C AX1240S-24P2C AX1240S-48T2C	LLDP neighboring device information	50

4. Login Procedures

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

4.1 Terminal-based management

4.2 Starting the switch

4.3 Login and logout

4.1 Terminal-based management

4.1.1 Operation terminals

A console or remote operation terminal is required to operate the Switch. A console is a terminal connected via RS232C, and a remote operation terminal is a terminal connected via an IP network. The Switch also supports network management by an SNMP manager over an IP network. Figure 4-1 illustrates the terminal connections, and Table 4-1 describes their functional requirements.

Figure 4-1 Terminal connections

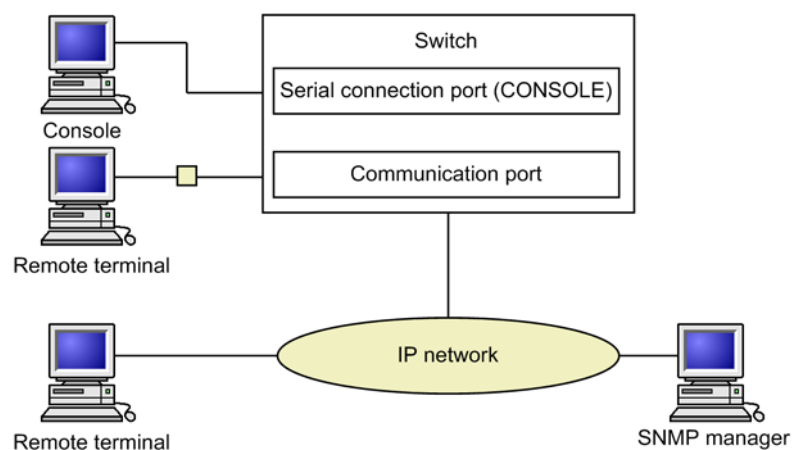


Table 4-1 Functional requirements of operation terminals

Terminal type	Connection method	Required specifications
Console	Serial connection (RS232C)	RS232C (transmission speed of 19200, 9600, 4800, 2400, or 1200)
Remote operation terminal	Communication port	TCP/IP telnet ftp

Note This Switch recognizes CR as the line feed code. Some terminals send CR and LF as the line feed code. If you connect to a Switch from this type of terminal, problems will occur; for example, blank lines might appear. If this is the case, check the terminal settings.

(1) Console

The console connects via RS232C and runs general communications software. To enable communication between the console and the Switch, make sure that the following standard VT100 settings (Switch defaults) are defined in the communication software:

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

If you want to use a console with a communication speed other than 9600 bps (1200, 2400, 4800, or 19200 bps), change the communication speed on the Switch side using the [line console speed](#) operation command. Then change the speed of the terminal software so that it is the same as the Switch speed.

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

```
> line console speed 19200 save
Do you wish to continue? (y/n): y
```

Note When you log in from a console, the Switch automatically acquires and sets the screen size using VT100 control characters. If the console does not support VT100 emulation, the screen size cannot be obtained or set. Invalid character strings might appear or the first CLI prompt might be displayed incorrectly. Use a console with the terminal operation mode set to VT100.

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 VT100 control characters. If this happens, log in again.

(2) Remote operation terminal

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

Note If the Telnet connection is dropped for some reason, such as a setting change or loss of the link to the connection port, the remote operation terminal might not be able to reconnect to the Switch for about 10 minutes.

4.1.2 Connection characteristics

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

Table 4-2 Connection features of operation terminals

Functionality	Serial connection	Communication port
Connected operation terminal	Console	Remote operation terminal
Remote login	No	Yes
Login from the Switch to a terminal	No	Yes
Access control	None	Yes
Command input	Yes	Yes
File transfer protocol	None	ftp
IP communication	No	IPv4
SNMP manager connection	No	Yes
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 a connected operation terminal you can execute operation commands and configuration commands to check the device status or to change the configuration as the connected network changes. The following table describes the Switch management operations you can perform.

Table 4-3 Operation management functionality

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

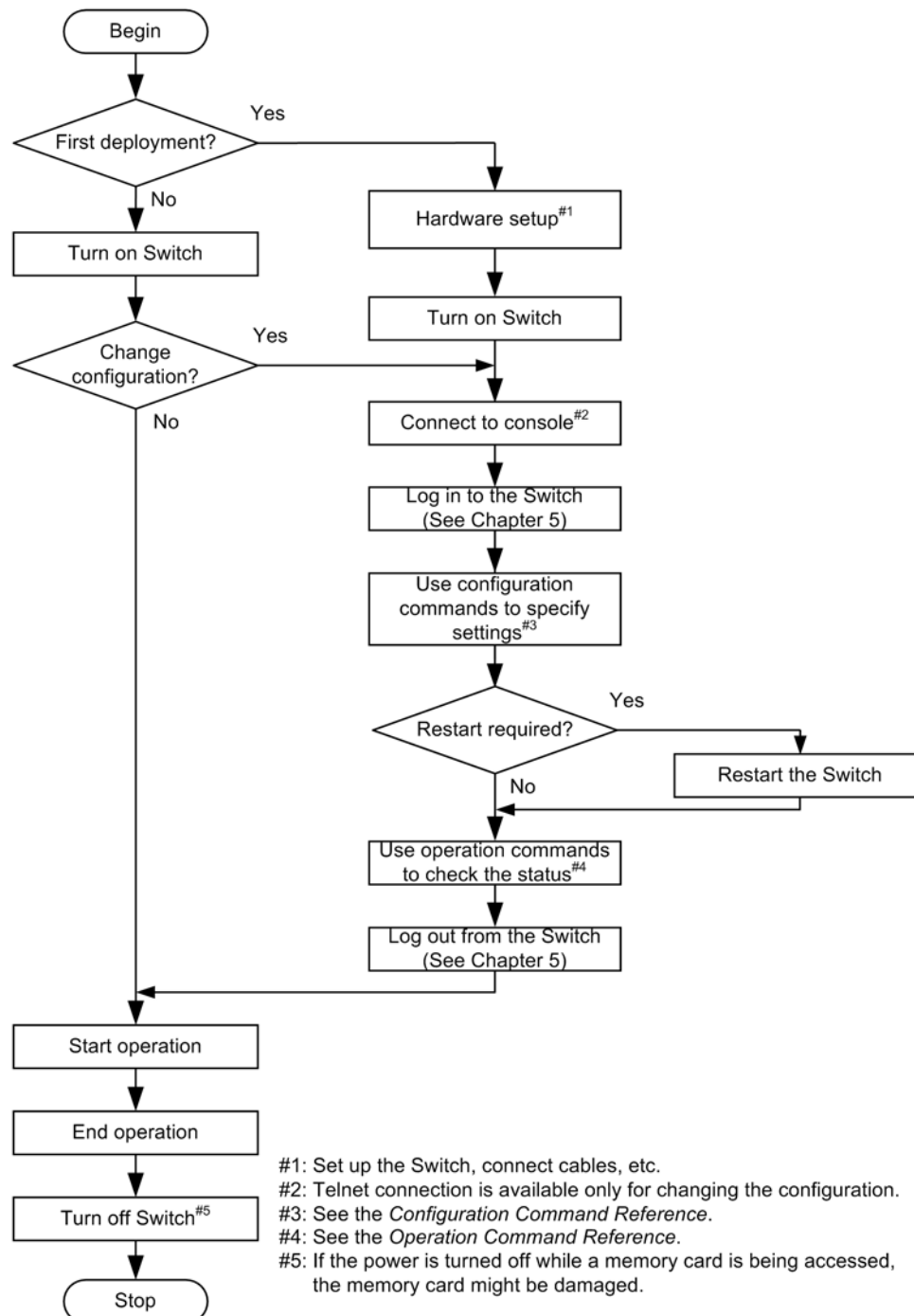
4.2 Starting the switch

This section describes how to start and stop a Switch.

4.2.1 Workflow from starting to stopping the 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 Switch



4.2.2 Starting a switch

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.

If the ST1 LED turns red when you start or restart the Switch, see the *Troubleshooting Guide*. For details about the LED indications, see the *Hardware Instruction Manual*.

The Switch boots from the memory card if you start or restart the Switch from an inserted memory card that contains the software image file [k.img](#).

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 window 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 window.

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

Figure 4-4 Login window

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

Copyright (c) 2006-2012 ALAXALA Networks Corporation. All rights reserved.

>                                           ...2
```

1. `Password:` is displayed only when a password has been set.
If a password has been set and you enter the password, the character string of the entered password is 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 window.

Figure 4-5 Logout window

```
> logout

login:
```

(3) Auto-logout

You are automatically logged out if there is no key input for a set duration (default: 30 minutes). You can change the auto-logout time 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 operation

5.1 Command input mode

5.1.1 List of operation commands

The following table lists and describes the operation commands related to command input mode transitions.

Table 5-1 List of operation commands

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

5.1.2 Command input mode

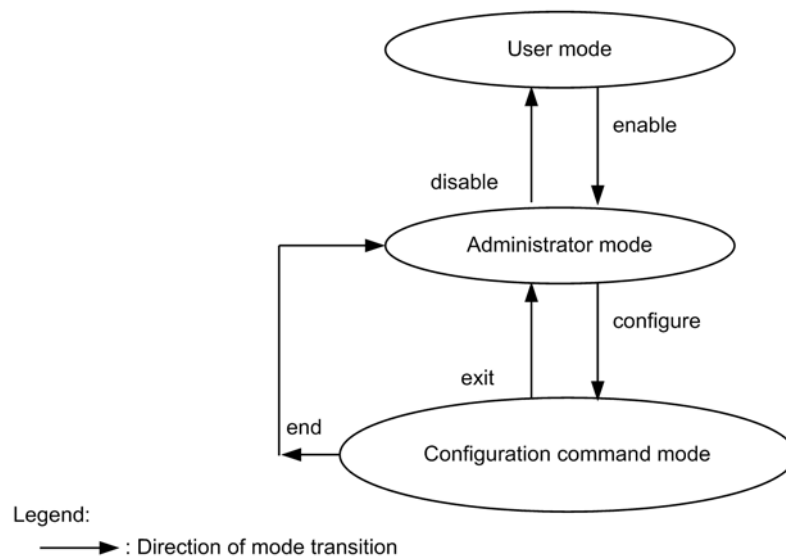
To change the configuration or check the status of the Switch, you must move to the appropriate command input mode, and then enter a configuration command or operation command. From the CLI prompt, you can tell which command input mode you are in.

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 be executed in administrator mode only.)	>
Administrator mode		#
Configuration command mode	Configuration commands	(config)#

The following figure provides an overview of mode transitions.

Figure 5-1 Overview of mode transitions

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

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

The following figure shows an example of these two situations.

Figure 5-2 Prompt display examples

```

> 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#
  
```

If you need to restart the Switch after you edit and save the configuration, an at mark (@) appears in front of the prompt. In this case, enter the `reload` operation command to restart the Switch.

Figure 5-3 Prompt display example (when @ appears)

```

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 Entry 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 entry completion

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

Pressing the Tab key displays the list of available commands or parameters.

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

Notes

You cannot always input the displayed options. For details, see the input format and valid range for each command in the *Configuration Command Reference* and *Operation Command Reference* manuals.

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. Parameter names that are not enclosed with < > might be displayed.
2. You cannot always input the displayed options. For details, see the input format and valid range for each command in the *Configuration Command Reference* and *Operation Command Reference* manuals.

If you type a question mark in a parameter without entering a preceding space, the entry completion functionality will activate.

5.2.3 Entry-error detection functionality

If you enter a command or parameter incorrectly, an error message appears on the next line. For details on error messages, see 36. *Error Messages on Configuration Editing* in the *Configuration Command Reference* manual. Input errors when you press the Tab key or type a question mark are indicated in the same manner.

Check and re-enter the command or parameter, referring to the error message. *Figure 5-6 Example of entry-error display (spelling mistake for fastethernet)* and *Figure 5-7 Example of display when a parameter is being entered (no parameter is specified for duplex)* show display examples of entry-error detection.

Figure 5-6 Example of entry-error display (spelling mistake for fastethernet)

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

Figure 5-7 Example of display when a parameter is being entered (no parameter is specified for duplex)

```
(config)# interface fastethernet 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 2008/11/14 20:04:23 UTC Total: 2
IP Address      Linklayer Address  Interface  Expire   Type
10.0.0.55       0013.20ad.0155     VLAN2048   20min    arpa
10.0.0.56       0013.20ad.0156     VLAN2048   20min    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 -n 1 192.168.0.1 ...1
Pinging 192.168.0.1 with 46 bytes of data:
Reply from 192.168.0.1: count=1. bytes=46

---- 192.168.0.1 Ping Statistics ----
Packet: sent 1, received 1, lost 0 (0% loss)
> ...2
> ping -n 1 192.168.0.1 ...3
Pinging 192.168.0.1 with 46 bytes of data:
Reply from 192.168.0.1: count=1. bytes=46

---- 192.168.0.1 Ping Statistics ----
Packet: sent 1, received 1, lost 0 (0% loss)
> ...4
> ping -n 1 192.168.0.2 ...5
Pinging 192.168.0.2 with 46 bytes of data:
Reply from 192.168.0.2: count=1. bytes=46

---- 192.168.0.2 Ping Statistics ----
Packet: sent 1, received 1, lost 0 (0% loss)
>
```

1. Execute the `ping` operation command on 192.168.0.1.
2. Press the up arrow key (↑) to call the preceding command.
In this example, pressing the up arrow key (↑) once displays the line `ping -n 1 192.168.0.1`. Simply press the Enter key to re-execute this command.
3. Execute the `ping` operation command on 192.168.0.1.
4. Press the up arrow key (↑) to call the preceding command, and then use the left arrow key (←) and the Backspace key to edit the command string.
In this example, pressing the up arrow key (↑) once displays the line `ping -n 1 192.168.0.1`. Change `1` in the IP address to `2`, and then press the Enter key.
5. Execute the `ping` operation command on 192.168.0.2.

Note

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

Available keys depend on the terminal application and terminal settings. ALAXALA Networks Corporation recommends that you use the key combinations listed in the following table (in which keys whose specification is clearly defined in VT100 are used) for operation.

Table 5-3 Recommended keyboard commands

Keyboard	Action of the Switch
Backspace	Deletes the character immediately before the cursor. (You can delete characters until the beginning of the line.)
Ctrl + A	Moves to the beginning of the command line.
Ctrl+ B	Moves one character backward. (You can move until the beginning of the line.)
Ctrl + C	Stops execution of the command.
Ctrl + D	Deletes one character.
Ctrl + E	Moves to the end of the command line.
Ctrl + F	Moves one character forward. (You can move until the end of the line.)
Ctrl + L	Refreshes the console screen, and clears everything in the display other than the command input line.
Ctrl + N	Displays the next command in the command history until the current command appears.
Ctrl + P	Displays the previous command in the command history.
Ctrl + U	Deletes the text on the cursor line.
Ctrl + W	Deletes from the beginning of the word to the cursor position. Example: <pre>!> show sysversion ~</pre> In the above input state, move the cursor immediately before the character v, and press Ctrl + W. The characters sys of the word sysversion are deleted as follows: <pre>!> show version</pre>
Ctrl + Z	Ends configuration command mode and returns you to administrator mode.
Ctrl + K	Deletes the text after the cursor.
Ctrl + T	Exchanges the current character and the previous character.

5 Command Operations

Keyboard	Action of the Switch
ESC + B	Moves one word backward.
ESC + F	Moves one word forward.
ESC + D	Deletes from the cursor position to the end of the word.

5.3 Notes on CLI operation

(1) Restrictions after login

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

(2) Restrictions on the display of command line completion and Help

Some commands have restrictions on command line completion and Help display.

Re-enter the relevant command. Refer to the *Configuration Command Reference* and *Operation Command Reference* manuals.

This subsection uses the following terms to describe parameters:

- Variable value parameter: A parameter for which an arbitrary numeric value or a character string is input.
- Fixed character string keyword: A parameter for which a fixed character string is input.

(a) When a fixed character string keyword follows a variable value parameter

Input format: *command* *<variable value>* *fixed character string keyword*

After *<variable value>* is entered, it might be possible to enter fixed character string keywords that are not allowed (command line completion is also available). However, such keywords are invalid, so an error occurs when you press the Enter key.

Figure 5-10 Example of displaying fixed character string keywords that cannot be input after a variable value parameter is entered

```
(config)# spanning-tree mst 5 [?]
configuration      - Configure the common information used by each MST ins
                    tance of multiple spanning tree, and enter MST config
                    uration 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 protoco
                    l 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 trans
                    mitted for one second
```

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

After you enter *spanning-tree mst 5* and then a question mark (?), the fixed character string keywords and parameters that can be input are displayed. However, at the same time, fixed character string keywords that cannot be input are displayed as shown in the above figure (marked with bold underline). In this case, if you enter *spanning-tree mst 5 configuration* and press the Enter key, an error occurs because the keyword *configuration* is an invalid input format.

(b) When more than one parameter with no fixed character string keywords is entered

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

If more than one parameter (enclosed with []) with no fixed character string keywords is entered, parameters that cannot be input might be displayed in Help display or in the list displayed when you press the Tab key.

Figure 5-11 Example of when more than one parameter (enclosed with []) with no fixed character string keyword is entered

```
(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>
```

In the above example, after you enter `lease 360` (when specifying until `days`) and then a question mark (`?`), parameters that can be input are displayed. However, at the same time, parameters that cannot be input are displayed as shown in the above figure (marked with bold underline).

(c) When a variable value parameter and a fixed character string keyword are in the same input order

When a variable value parameter and a fixed character string are in the same input order, the fixed character string keyword is given priority. Therefore, if the character string of a variable value parameter perfectly matches the beginning part of a fixed character string keyword, the character string is recognized as the fixed character string keyword (command line completion is enabled).

The following is an example of when an entered character string is recognized as a fixed character string keyword, and an example of when an entered character string is recognized as a variable value parameter.

Figure 5-12 Example of when a variable value parameter is recognized as a fixed character string keyword

```
(config)# aaa authentication mac-authentication
<List name>          - Specify the RADIUS server list name 1 to 32 characters
default              - Specify default mac authentication mechanism
(config)# aaa authentication mac-authentication de⇒ Recognized as a fixed character
string keyword
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 variable value parameter `<List name>`. However, because the entered character string `de` perfectly matches the beginning part of the fixed character string keyword `default`, which is in the same input order as `<List name>`, the entered character string is recognized as `default`, and the Help for the keywords that can be input after `default` is displayed.

Figure 5-13 Example of when an entered character string is recognized as a variable value parameter

```
(config)# aaa authentication mac-authentication device⇒ Recognized as a variable value
parameter.
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 variable value parameter `<List name>`. In this case, because the entered character string `device` does not perfectly match the beginning part of the fixed character string keyword `default`, which is in the same input order as `<List name>`, the entered character string is recognized as `device`, and the Help for the character string that can be input after `<List name>` is displayed.

(d) Restrictions on the number of characters for a command or parameter displayed in Help

If a command or parameter has 24 or more characters, only the beginning 24 characters are displayed in Help.

Figure 5-14 Example of when the number of characters displayed in Help is restricted

```
(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-selection`, which is more than 24 characters, is supposed to be displayed as Help for the `switchport-backup` command, but only `startup-active-port-sel` is displayed and the subsequent characters are omitted.

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

The Help display and command line completion of the configuration commands `deny`, `permit` (except for `ip access-list standard`), and `qos` are restricted as follows:

- When the input format of a command is shown in the Help display
If the parameter `<Src IPv4>` or `<Src MAC>` is specified, the Help display for the subsequent parameters always shows the input format of the relevant command as shown in the following figure.

Figure 5-15 Example of when the input format is shown in the Help display (example for `ip access-list extended`)

```
(config-ext-nacl)# permit
<protocol>          - 0-255, ah, esp, gre, icmp, igmp, ip, ipinip, ospf, pcp, pim, sct
                    p, tcp, tunnel, udp, vrrp
(config-ext-nacl)# permit ip
<PARAMS:input format> - [<Seq>] permit <Protocol> {<Src IPv4> <Src IPv4 wildc
ard> | host <Src IPv4> | any} [*1] {<Dst IPv4> <Dst I
Pv4 wildcard> | host <Dst IPv4> | any} [*2] [*3] {[to
s <TOS>] [precedence <Precedence>] | dscp <DSCP>] [vl
an <VLAN ID>] [user-priority <Priority>]          NOTE:
*1:for TCP/UDP - eq <Src port> *2:for TCP/UDP - eq
<Dst port> *3:for TCP - [ack] [fin] [psh] [rst] [sv
n] [urg]
```

- When `<cr>` is shown in the Help display
The Help display normally shows `<cr>` when the input is complete. However, for the configuration commands `deny`, `permit`, or `qos`, `<cr>` might be shown even when the input is incomplete. If you press the Enter key according to the `<cr>` display when the input is incomplete, an error occurs. Re-enter the relevant command. Refer to the *Configuration Command Reference* and *Operation Command Reference* manuals.

Figure 5-16 Example of <cr> shown when a command input is incomplete (example for ip access-list extended)

```
(config-ext-nacl)# permit ip any host
<PARAMs:input format> - [<Seq>] permit <Protocol> {<Src IPv4> <Src IPv4 wildc
ard> | host <Src IPv4> | any} [*1] {<Dst IPv4> <Dst I
Pv4 wildcard> | host <Dst IPv4> | any} [*2] [*3] {[to
s <TOS>] [precedence <Precedence>] | dscp <DSCP>} [vl
an <VLAN ID>] [user-priority <Priority>] NOTE:
*1:for TCP/UDP - eq <Src port> *2:for TCP/UDP - eq
<Dst port> *3:for TCP - [ack] [fin] [psh] [rst] [sy
n] [urg]

<cr>
```

- Restrictions on command line completion

Characters following the parameter <Src IPv4> or <Src MAC> cannot be completed.

Figure 5-17 Example of when command line completion is not available (example for ip access-list extended)

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

(config-ext-nacl)# permit ip a⇒ "any" cannot be completed.
```

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

Input format: *command* <parameter> [omissible parameter]

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 input are shown in the Help display or in the command list displayed when you press the Tab key

Figure 5-18 Example of displaying parameters that cannot be input

```
(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.

(g) Command line completion and Help for no

`no`, which you enter to delete a setting, is not displayed in the Help display when you enter a question mark (?) or in the command list displayed when you press the Tab key. Also, `no` is not completed when you press the Tab key.

(3) Input in the configuration mode

In level-2 configuration mode, you cannot enter any commands of the level-1 global configuration mode. To enter such commands, execute the `exit` command to return to the global configuration mode.

(4) Setting of the console (RS232C)

Use the console with the terminal operation mode set to VT100 and with the terminal size set to 80 characters/line × 24 lines.

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

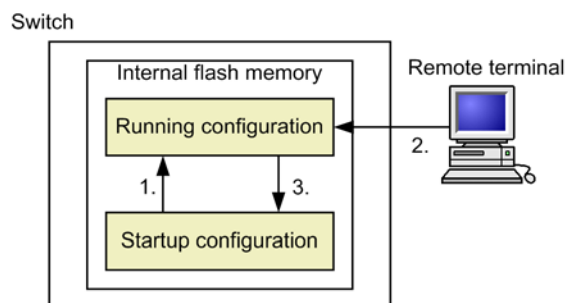
Both at deployment and during operation, the administrator will need to perform configuration settings relating to the connected network and the operating conditions of the Switch. The switch configuration is not predefined at initial deployment.

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. The file 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 provides an overview of the configuration at startup and during operation.

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



1. At startup 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 applied to the running configuration.
3. The new running configuration is saved in the startup configuration file.

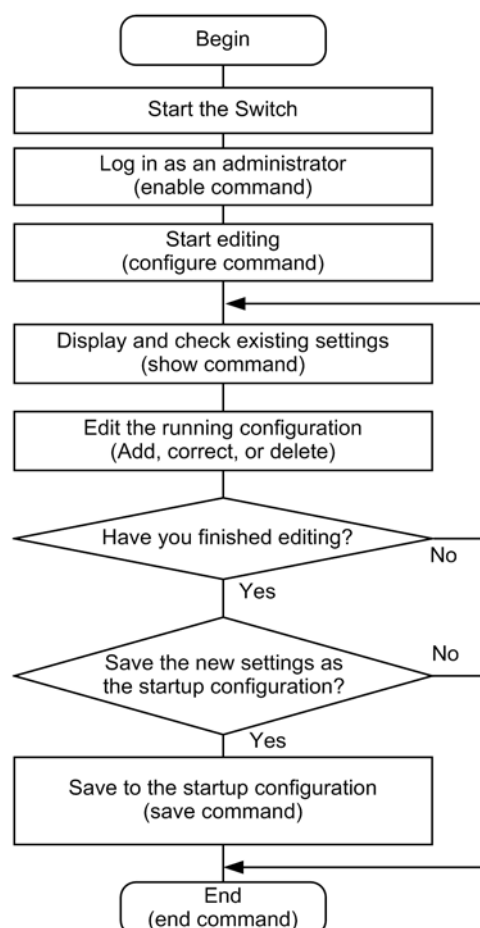
6.1.2 Configuration during operation

When you edit a configuration during operation, the edited contents are immediately applied as the running configuration. You can use the **save (write)** configuration command or the **copy** operation command to save the running configuration to the startup configuration file in internal flash memory. Note that the edited contents will be lost if you restart a switch without first saving the running configuration.

6.2 Overview of editing a running configuration

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

Figure 6-2 Workflow when editing a running configuration



6.3 Mode transitions when entering configuration commands

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

Figure 6-3 Overview of configuration mode transition

Global config mode (First hierarchy)	Mode switching command	Config mode (Second hierarchy)
config	interface fastethernet	config-if
	interface gigabitethernet	config-if
	interface range fastethernet	config-if-range
	interface range gigabitethernet	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
	mac access-list extended	config-ext-macl
	ip qos-flow-list	config-ip-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 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
end	Ends configuration command mode and returns you to administrator mode.
exit	Returns to the previous mode. If you are editing a configuration in global configuration mode, the command ends configuration command mode and returns you to administrator mode.
save (write)	Saves the edited configuration as the startup configuration file.
show	Displays the configuration being edited.
top	After a switch to configuration command mode, enter this command restores level-1 global configuration mode.

The following table lists and describes the operation commands for displaying configurations and operating files.

Table 6-2 List of operation commands

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

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

Figure 6-5 Example of displaying a running configuration

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

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

Figure 6-6 Displaying all configuration entries

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

1. When you omit all parameters, the entire running configuration is displayed.

Figure 6-7 Displaying information about the fastethernet interface

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

1. Display information about all fastethernet interfaces in the running configuration.

Figure 6-8 Displaying information for a specified interface

```
(config)# show interface fastethernet 0/1      ...1
interface fastethernet 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 fastethernet 0/1 ...1
(config-if)# show
interface fastethernet 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 disabling and reinstating functionality* shows an example of disabling and later reinstating functionality.

Figure 6-10 Example of editing a configuration

```
(config)# vlan 100 ...1
!(config-vlan)# state active ...2
!(config-vlan)# exit
!(config)# interface fastethernet 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 fastethernet 0/1 ...8
!(config-if)# no switchport access vlan ...9
!(config-if)# exit
!(config)#
```

1. Configure VLAN 100 as a port-based 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 disabling and reinstating functionality

```
(config)# interface fastethernet 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** (full-duplex mode) for **duplex**.
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 fastethernet 0/1
!(config-if)# description TokyoOsaka
!(config-if)#
```

Figure 6-13 Error message output for an incorrect configuration

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

6.4.5 Saving to the configuration file

You can save the edited running configuration to the startup configuration file using the **save** (**write**) configuration command or the **copy** operation command. The following figure shows an example of saving a configuration.

Figure 6-14 Example of saving 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 the 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. Execute 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 switch capacity, the message `Maximum number of entries are already defined` appears. If such a message appears, check whether any unnecessary entries exist.

(2) Copying and pasting configuration entries

When you copy and paste configuration entries, use no more than 1000 characters at one time, including spaces and line breaks.

If the configuration entries exceed 1000 characters, copy and paste them in multiple operations, each with no more than 1000 characters.

6.5 Configuration operations

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

6.5.1 Transferring files using FTP

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

(1) Transferring a backup configuration file to the Switch

Transfer the backup configuration file saved on the PC to the Switch by using the FTP protocol, and copy it to the startup configuration file by using the `copy` operation command.

On your PC, open the command prompt window. (On a standard Windows XP PC, click the Start menu, choose All Programs and then Accessories, and then click Command Prompt.)

Move to the directory in which the backup configuration file is stored, and log in to the Switch using the FTP protocol. Transfer the backup configuration data to the RAMDISK on the Switch in ASCII mode.

Set a VLAN and an IP address for the port used for the FTP connection.

The following figures (6-16 and 6-17) show an example of operations using the `backup.cnf` file that was saved in `C:\TEMP`.

Figure 6-16 Operations in the command prompt window: example of transferring a backup configuration file to the Switch

```
C:\TEMP>ftp 192.168.0.1
Connected to 192.168.0.1
220 AX1200 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>
```

Next, log in to the console, and use the `copy` operation command to copy the backup file from the RAMDISK to the startup configuration file.

Figure 6-17 Operations on the console screen: Applying the transferred file to 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 copy the startup configuration file to the RAMDISK by using the `copy` operation command.

Figure 6-18 Operations on the console screen: 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.

Move to the directory in which the backup configuration file is to be stored, and log in to the Switch by using the FTP protocol. Transfer the backup configuration file from the RAMDISK on the Switch to the PC in ASCII mode.

Figure 6-19 Operations in the command prompt window: example of transferring a backup configuration file to the Switch

```
C:\TEMP>ftp 192.168.0.1
Connected to 192.168.0.1
220 AX1200 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 the memory card containing the backup configuration file into the slot. Copy the backup configuration file on the memory card to the RAMDISK on the Switch by using the `copy` operation command. Copy the backup configuration file on the RAMDISK to the startup configuration file by using the `copy` operation command. An example is shown in the following figure.

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 on 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

Copy the backup configuration file to a memory card by using the `copy` operation command.

Copy the startup configuration file to the RAMDISK by using the `copy` operation command. Copy the backup configuration file on the RAMDISK to a memory card by using the `copy` operation command. An example is shown in the following figure.

Figure 6-21 Copying a backup configuration file on 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 a memory card.

6.5.3 Notes on applying a backup configuration file

When you copy the backup configuration file to the startup configuration file by using the `copy` operation command, the configuration cannot be directly applied to the running configuration. Restarting the device by turning it off and then on again, or by executing the `reload` operation command is necessary. Be careful if you are logged in from a remote terminal.

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

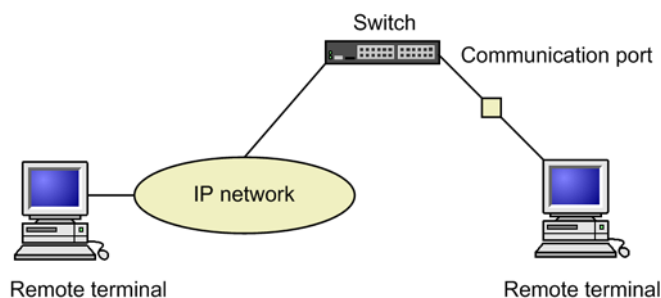
This chapter describes remote access to the Switch from a remote operation terminal.

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 connection.

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



7.2 Configuration

7.2.1 List of configuration commands

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

Table 7-1 List of configuration commands

Command name	Description
ftp-server	Permits access from remote operation terminals using FTP.
line vty	Permits Telnet remote access to a switch.
transport input	Regulates access from a remote operation terminal using the various protocols.

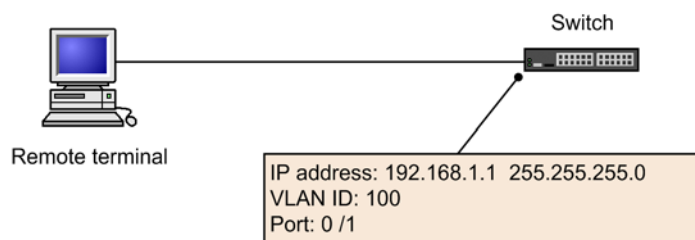
For details on configuration commands related to setting up VLANs and IPv4 interfaces, see *17 VLANs* and *26 IPv4 Interfaces*.

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 to which the terminal is to connect.

Figure 7-2 Example of connecting with a remote terminal



Command examples

1.

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

Configures VLAN ID 100 as a port-based VLAN.

2.

```
(config)# interface fastethernet 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.

3.

```
(config)# interface vlan 100
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# exit
```

```
(config)#
```

Switches to interface configuration mode for VLAN ID 100. Sets IPv4 address 192.168.1.1 and subnet mask 255.255.255.0 for VLAN ID 100.

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.

Configure the Switch so that remote login is allowed via Telnet.

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

Command examples

1.

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

Permits remote access to the Switch from a remote operation terminal by using the Telnet protocol. Limits the number of concurrent remote logins to a maximum of two 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.

Configure the Switch so that remote access is allowed 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 operation commands related to terminal connections and remote operations.

Table 7-2 List of operation commands

Command name	Description
set exec-timeout	Specifies the length of time until the user is automatically logged out.
set terminal pager	Enables or disables paging.
telnet	Connects via Telnet to a remote host that has a specified IP address.
ftp	Transfers files between the Switch and a remote operation terminal connected via TCP/IP.
line console speed	Changes the communication speed of the console (RS232C).
trace-monitor	Sets whether to display the operation log on the monitor.

7.3.2 Verifying communication between a remote terminal and the Switch

You can verify that the Switch and remote operation terminal are communicating by using the [ping](#) operation command. For details, see *26 IPv4 Interfaces*.

8. Login Security and RADIUS

This chapter describes login control, login security, and RADIUS for the Switch.

8.1	Setting login security
8.2	Description of RADIUS
8.3	Configuring RADIUS
8.4	RADIUS operations

8.1 Setting login security

8.1.1 Lists of configuration commands and operation commands

The following table describes the configuration commands related to login security.

Table 8-1 List of configuration commands

Command name	Description
aaa authentication login	Specifies the authentication method to be used at remote login.
aaa authentication login end-by-reject	Terminates authentication if login authentication is denied. If authentication fails due to an inability to communicate, such as a lack of response from the RADIUS server, the next authentication method specified in the aaa authentication login configuration command is used to perform authentication.
ip access-group	Sets an access list that specifies the IPv4 addresses of remote operation terminals for which remote login to the Switch is permitted or denied.

The following table describes the operation commands related to login security.

Table 8-2 List of operation commands

Command name	Description
password	Specifies the user login password.
clear password	Clears the user login password.
rename user	Changes the initial user ID operator to another name.
show sessions(who)	Display 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 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 check is performed at login.
2. Users can log in to a Switch concurrently from local and remote operation terminals.
3. The maximum number of users who can log in concurrently is 2. You can reduce this limit by using the [line vty](#) configuration command.
4. IPv4 addresses that are allowed to access the Switch can be restricted by using the [ip access-list standard](#) and [ip access-group](#) 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.
7. You are automatically logged out if there is no key input for a set duration (default: 30

minutes). You can change the auto-logout time by using the `set exec-timeout` operation command.

8. Login from a remote operation terminal (via Telnet) also supports one-time password authentication using the SecurID mechanism engineered by RSA Security. For details on the one-time password authentication, see *14 One-time Password Authentication [OP-OTP]* in the *Configuration Guide Vol. 2*.

8.1.3 Changing the login user

You can change the ID of the user who can log in to the Switch by using the `rename user` operation command. The following figure shows an example of changing the login user.

Figure 8-1 Changing the user operator

```
> enable
# rename user
Changing username.
Old username:operator          ... 1
New username:ax12-01          ... 2
# exit
>
```

1. Enter the current user ID.
2. Enter a new user ID using no more than eight characters.

If you do not intend to use the pre-defined `operator` account, to prevent security risks, we recommend that you change it to a new user account.

Do not forget the new 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 password authentication. You should therefore set an administrator password at deployment, as in the following example.

Figure 8-2 Setting the password for 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 operation 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 must 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 who can log in concurrently. Regardless of this setting, login from the console is always possible. The following setting example allows no more than two users to be logged in concurrently.

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

```
(config)# line vty 0 1
(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 Restricting login from remote operation terminals

The settings below enable you to restrict the remote operation terminals that can log in to the Switch. After performing this setup, make sure that other remote operation terminals are denied access.

(1) Setting the IP addresses of remote operation terminals permitted to log in

Points to note

If you want to allow only specific remote operation terminals to access the Switch, you must register the IP addresses of the terminals in advance using the `ip access-list standard` and `ip access-group` configuration commands. You can register IPv4 addresses and subnet masks for which access is permitted by using a maximum of 16 `ip access-group` entries. If you omit this setup, all remote operation terminals will be able to access the Switch.

Command examples

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 network 192.168.0.0/24 but denies login from IP address 192.168.0.254.

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 network IP address 192.168.0.0/24.

Notes

- An access list for use by the Switch does not depend on the settings of the flow detection mode.
- IP addresses that meet the permit conditions are permitted remote login.
IP addresses that meet the deny conditions are not permitted remote login.
- Implicit deny conditions for all IP addresses are set in the final list of the IP access group. If an IP address does not match any of the registered groups, it is assumed to meet an implicit deny condition, and the remote login is rejected.
- If no access list is registered in the IP access group, remote login is handled as if the permit conditions are met.

(2) Authenticating remote operation terminals by using RADIUS

RADIUS authentication can be used when a remote operation terminal tries to log in to the Switch.

8.2 Description of RADIUS

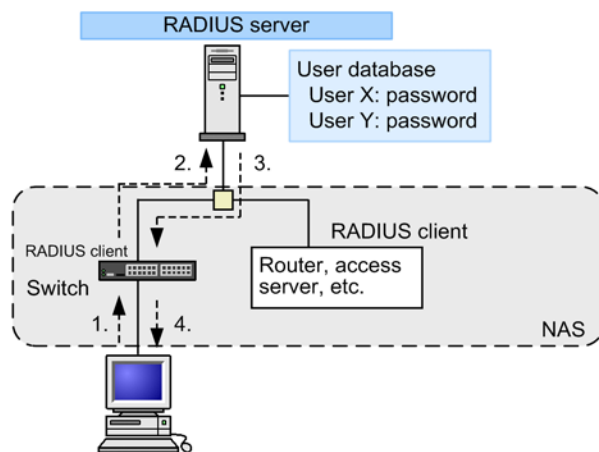
8.2.1 Overview of RADIUS

RADIUS (Remote Authentication Dial In User Service) 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 operates as a client of a RADIUS server. A NAS device requests services such as user authentication and accounting from the configured RADIUS server. The RADIUS 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



1. Using the Telnet protocol, user X connects to the Switch from the remote terminal.
2. The Switch requests authentication via the RADIUS server specified in the configuration.
3. The RADIUS server authenticates user X by using the user database, and then notifies the Switch that the user has been authenticated.
4. Based on the RADIUS authentication, the Switch permits Telnet access for user X from the remote terminal.

8.2.2 Application functionality and scope of RADIUS authentication

RADIUS authentication is applied to the following functionality of the Switch:

- User authentication for login from a remote operation terminal (hereafter referred to as login authentication)

RADIUS authentication

- Layer 2 authentication (IEEE 802.1X, Web authentication, and MAC-based authentication)

RADIUS authentication and RADIUS accounting

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

This subsection describes the scope of support of RADIUS authentication for login authentication.

(1) Scope of RADIUS authentication

RADIUS authentication can be used for the following operations:

- Telnet access from a remote terminal (IPv4)
- FTP access from a remote terminal (IPv4)

RADIUS authentication cannot be used for the following operation:

- Login from a console (RS232C)

(2) Scope of support of RADIUS server

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

Table 8-3 Scope of RADIUS implementation

Category	Description
Documentation	Supported RADIUS functions described herein are limited to NAS-related functions only.
Packet types	Supports the following packet types used for login authentication: ● Access-Request (send) ● Access-Accept (receive) ● Access-Reject (receive) ● Access-Challenge (receive)
Attribute	Supports the following attributes used for login authentication: ● User-Name ● User-Password ● Service-Type ● NAS-IP-Address ● Reply-Message ● State ● NAS-Identifier

(a) Description of supported RADIUS attributes

The table below describes the RADIUS attributes.

- Access-Request packet

No attributes other than those listed above are attached to Access-Request packets sent by the Switch.

- Access-Accept, Access-Reject, or Access-Challenge packet

Attributes other than those listed above are ignored by the Switch if attached to the packet.

Table 8-4 Description of supported RADIUS attributes

Attribute name	Attribute value	Packet types	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), Ignored when attached to Access-Accept or Access-Reject.
NAS-IP-Address	4	Access-Request	The IP address of the Switch. From among the VLAN interfaces that have an IP address registered, the IP address of the smallest VLAN ID is used.
Reply-Message	18	Access-Challenge Access-Accept ^{#1} Access-Reject ^{#1}	Text character string. This attribute value is displayed as a message in the telnet page displayed during one-time password authentication ^{#2} .
State	24	Access-Challenge Access-Request	Text character string. The Switch retains the State information passed by Access-Challenge used in one-time password authentication ^{#2} . When performing Access-Request for Access-Challenge, the State information retained 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.

#1

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

#2

For details on one-time password authentication, see *14 One-time Password Authentication [OP-OTP]* in the *Configuration Guide Vol. 2*.

8.2.3 Authentication using RADIUS

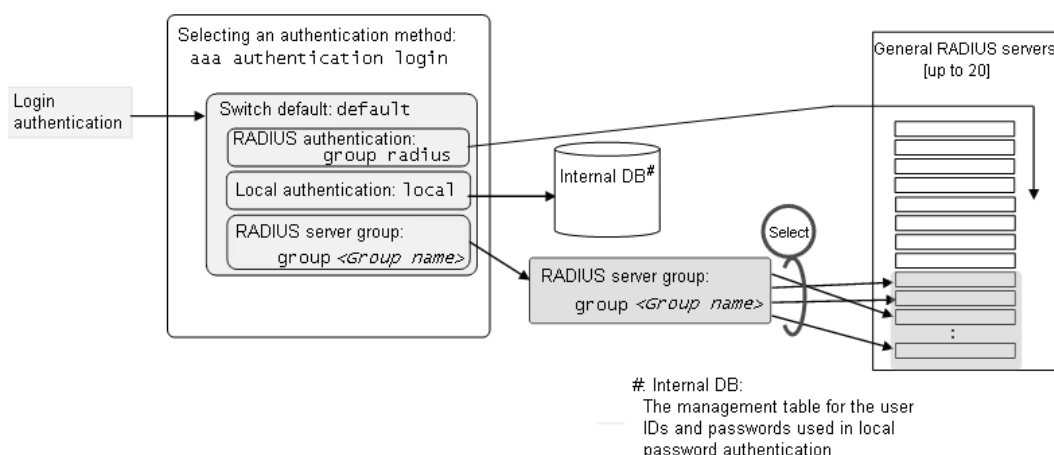
This subsection describes RADIUS authentication used for login authentication.

Selecting a RADIUS server and automatic-restoration functionality, which is described later, can be used in the same way in Layer 2 authentication. For details, see *5 Overview of Layer 2 Authentication* in the *Configuration Guide Vol. 2*.

(1) Selecting login authentication services

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 (the Switch's own authentication function implemented by the `password` command).

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

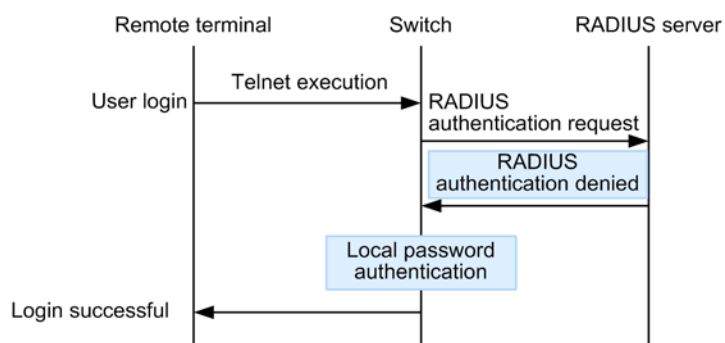
Figure 8-7 Correlation diagram of authentication method configuration

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. When multiple authentication methods are specified, the `aaa authentication login end-by-reject` configuration command can change the behavior of the authentication service performed when the first-specified authentication method fails.

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 when end-by-reject is not set. If authentication fails when using the first specified method when end-by-reject is not set, authentication can be performed using the next specified method regardless of the reason of failure. The figure below shows an example of the authentication sequence. In this example, RADIUS authentication and local password authentication are specified in that order as authentication methods. The RADIUS server authentication is denied, but local password authentication succeeds.

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

In this figure, the user accesses the Switch via Telnet from a remote terminal, and the Switch requests the RADIUS server to perform authentication. If RADIUS server authentication fails because the RADIUS server denied the request, the Switch performs authentication using local password authentication. At this point, authentication is successful and the user is able to log in to the Switch.

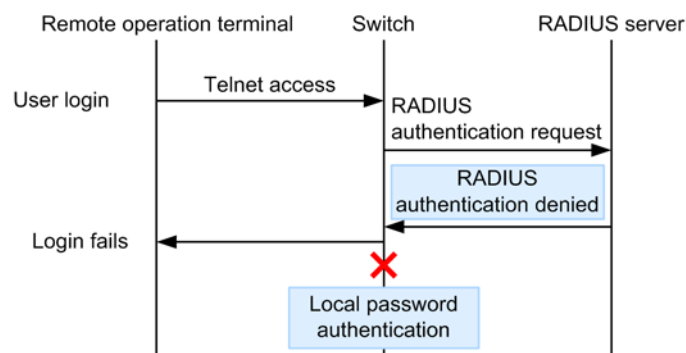
(b) When end-by-reject is set

The following explains how an authentication service is selected when end-by-reject is set.

If authentication fails when using the first specified method when end-by-reject is set, authentication is not performed using the next specified method. The entire authentication process is terminated at the first denial and is treated as a failure. The next specified method is used for authentication only when authentication fails due to an inability to communicate, for example if the RADIUS server does not respond.

The figure below shows an example of the authentication sequence. In this example, RADIUS authentication and local password authentication are specified in that order as authentication methods. The RADIUS server denies authentication.

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



In this figure, the user accesses the Switch via Telnet from a remote terminal, and the Switch requests the RADIUS server to perform authentication. However, the RADIUS server denies the request, and the RADIUS server authentication fails, which means the series of authentications fails and authentication finishes. The next local password authentication is not performed on the Switch. As a result, the user fails to log in to the Switch.

(2) Selection of a RADIUS server and automatic-restoration (dead-interval) functionality

You can specify up to 20 general-use RADIUS servers used for RADIUS authentication for remote logins. If one server is unreachable and its authentication service is unavailable, each of the other servers is attempted in turn.

- Selection of a RADIUS server (the maximum time before the system decides that communication with a RADIUS server is not 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, another attempt is made to connect to it. You can set the maximum number of connection retries that the server makes with each server (three by default). Because of this, the maximum time before the system decides that the RADIUS server is unavailable is as follows: $\text{response-timeout-period} \times (\text{first-try} + \text{number-of-retries}) \times \text{number-of-RADIUS-servers-configured}$.

- Automatic-restoration (dead-interval)

RADIUS authentication used by the Switch detects an effective RADIUS server when it detects a RADIUS authentication request by receiving a frame from a terminal subject to authentication. The following terminals always use the effective RADIUS server. 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 automatic restoration for the first valid RADIUS server (primary RADIUS server). The monitoring timer default is 10 minutes.

(3) Information to be registered in the RADIUS server

To use the RADIUS authentication, register a user ID and a password in the RADIUS server.

Use no more than 8 characters for a user ID, and no more than 16 characters for a password.

8.2.4 Connecting to RADIUS servers

(1) Switch identification on the RADIUS server side

The RADIUS server uses the sender IP address of the request packet to identify the RADIUS client. The Switch uses the IP address of the sender 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 might use port 1645, not port 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

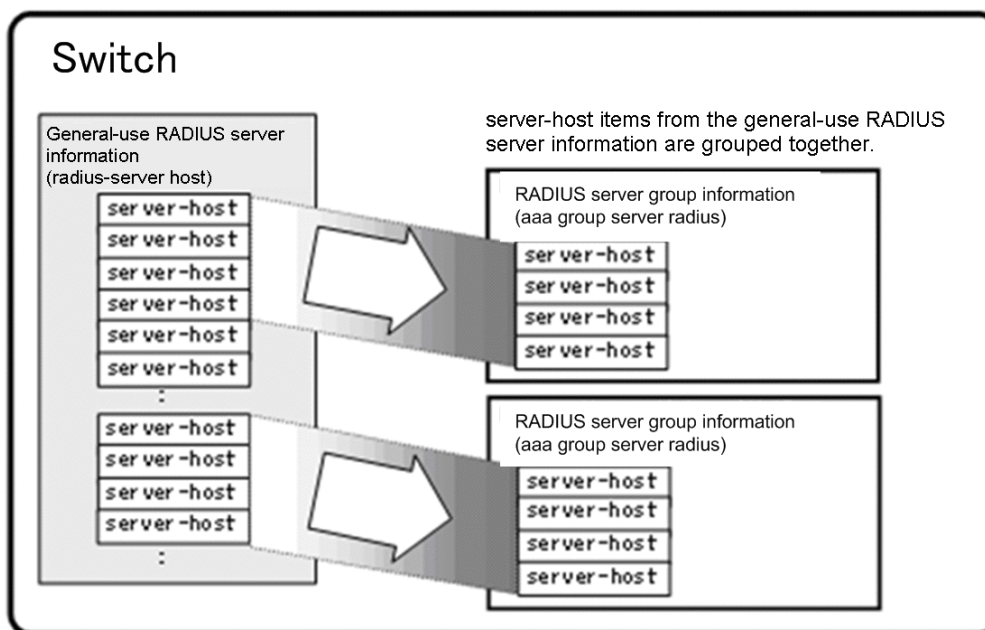
The following RADIUS server information is configurable on the Switch.

- 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 setting and using Layer 2 authentication functionality and RADIUS server information, see *5 Overview of Layer 2 Authentication* in the *Configuration Guide Vol. 2*.

Assign RADIUS server group information by using the general-use RADIUS server information that has been set. The following figure shows the relationship between the RADIUS server group and the general-use RADIUS server.

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



For the IP address, port number for authentication, and port number for accounting that are set for the RADIUS server group, use the same value with the general-use RADIUS server information (set by the `radius-server host` configuration command).

The behavior when selecting a RADIUS server in a RADIUS server group is the same as for other RADIUS servers, but automatic-restoration time is based on the setting of the `radius-server dead-interval` configuration command.

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

The RADIUS server group is also used in the port-based authentication method of Layer 2 authentication and in the user ID-based authentication method of Web authentication. For details, see *5 Overview of Layer 2 Authentication* in the *Configuration Guide Vol. 2*.

8.3 Configuring RADIUS

8.3.1 List of configuration commands

The following table lists and describes the configuration commands related to RADIUS.

Table 8-5 Configuration commands (RADIUS)

Command name	Description
aaa group server radius	Configures a RADIUS server group.
server	Configures a RADIUS server host in the RADIUS server group.
radius-server dead-interval	Configures the monitoring timer used for automatic-restoration of the primary RADIUS server.
radius-server host	Configures information about the general-use RADIUS server used for authentication.
radius-server key	Sets a RADIUS server key for authentication.
radius-server retransmit	Sets the number of allowed retransmissions to the RADIUS server used for authentication.
radius-server timeout	Sets a response timeout value for a RADIUS server used for authentication.
radius-server attribute station-id capitalize	Sends the MAC address that is used for sending data to a RADIUS server with the RADIUS attribute in upper case. (Used in Layer 2 authentication [#] .)

#

For details about the RADIUS attributes for which this command is used in Layer 2 authentication, see the description of authentication in the *Configuration Guide Vol. 2*.

8.3.2 Setting authentication methods

As login authentication methods, the following setting examples are described below:

- Combination of general-use RADIUS server authentication and local password authentication
- Combination of RADIUS server group authentication and local password authentication

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

Points to note

In these examples, RADIUS server authentication and local password authentication are configured as authentication methods. The methods are configured so that if the RADIUS server authentication fails due to an inability to communicate, such as the RADIUS server not responding, then local password authentication is used.

If authentication fails due to denial of RADIUS authentication, the authentication process ends at that point, and local password authentication is not performed.

Information about the general-use RADIUS server used for RADIUS authentication is also configured.

The usual setup for remote access must be completed in advance.

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.
2. `(config)# aaa authentication login end-by-reject`
Configures the settings so that the authentication process ends when denied by RADIUS authentication and local authentication is not performed.
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 sets a shared 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 general-use RADIUS server to be used for RADIUS authentication and sets a shared key for communication with the server.

Note

1. Both `group radius` and `group <group-name>` are treated as the same `<Method>` because the both are RADIUS authentication methods, so you cannot set them both as authentication methods. If you want to specify more than one method, you can specify either of them and you can also specify `local`.

(2) Setting of RADIUS server group authentication and local password authentication

Points to note

In these examples, RADIUS server group authentication and local password authentication are configured as authentication methods. The methods are configured so that if RADIUS server group authentication fails due to an inability to communicate, such as the RADIUS server not responding, then local password authentication is used.

If authentication fails due to denial of the RADIUS authentication, the authentication process ends at that point, and local password authentication is not performed.

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

The usual setup for remote access must be completed in advance.

Command examples

1. `(config)# aaa authentication login default group LOGIN-SEC local`
Sets the RADIUS server group name and local password authentication in that order.
2. `(config)# aaa authentication login end-by-reject`
Configures the settings so that the authentication process ends when denied by RADIUS server group authentication and local authentication is not performed.

Notes

1. Both `group radius` and `group <group-name>` are treated as the same `<Method>` because the both are RADIUS authentication methods, so you cannot set them both as authentication methods. If you want to specify more

than one method, specify either of them and specify `local`.

8.3.3 Configuring a RADIUS server group

Points to note

Configure a RADIUS server group to be used for authentication.

Set addresses to be used in a RADIUS server group from the addresses of the RADIUS servers set by the `radius-server host` configuration command (general-use RADIUS servers).

Information about no more than four RADIUS servers can be set for a group.

Command examples

- ```
(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 IP addresses of the general-use RADIUS servers and shared keys for communication with those servers.

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

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

- ```
(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 addresses of the servers to be used in the group from the addresses of the general-use RADIUS servers set by the `radius-server host` configuration command.

Because the port number for authentication and the port number for accounting are omitted in this example, 1812 is used for the port number for authentication and 1813 is used for the port number for accounting.

#### Notes

- For the group name set by the `aaa group server radius` configuration command, we recommend that you use a capital letter for the first character.
- Settings made by using the `server` configuration command are valid only when all the following conditions are met:
  - Values are the same as the `radius-server host` command configuration (IP address, port number for authentication, and port number for accounting).
  - The `radius-server host` command configuration is enabled with the same values as the `server` command configuration (the key parameter

## 8 Login Security and RADIUS

has been set or the `radius-server key` command has been configured).

## 8.4 RADIUS operations

### 8.4.1 List of operation commands

The following table lists and describes the operation commands related to RADIUS.

**Table 8-6** List of operation commands

| Command name                   | Description                                                                                               |
|--------------------------------|-----------------------------------------------------------------------------------------------------------|
| show radius-server             | Displays the effective RADIUS server information set on the Switch.                                       |
| clear radius-server            | Changes the RADIUS server to which an authentication request is sent, to the initially set RADIUS server. |
| show radius-server statistics  | Displays statistics about the effective RADIUS server set on the Switch.                                  |
| clear radius-server statistics | Clears statistics about the effective RADIUS server from the Switch.                                      |

### 8.4.2 Displaying the effective RADIUS server information

#### (1) Displaying the effective RADIUS server information

Display the RADIUS server information set on the Switch by using the `show radius-server` operation command. If all RADIUS servers are unavailable, `* hold down` is displayed.

**Figure 8-11** Execution results of the show radius-server command (when the effective RADIUS server is used)

```
> show radius-server

Date 2009/10/29 05:13:12 UTC
<common>
 [Authentication]
 IP address Port Timeout Retry Remain
 * 192.168.0.251 1812 5 3 -
 192.168.0.252 1812 5 3 -
 192.168.0.253 1812 5 3 -
 192.168.0.254 1812 5 3 -
 192.168.11.1 1812 10 5 -
 [Accounting]
 IP address Port Timeout Retry Remain
 * 192.168.0.251 1813 5 3 -
 192.168.0.252 1813 5 3 -
 192.168.0.253 1813 5 3 -
 192.168.0.254 1813 5 3 -
 192.168.11.1 1813 10 5 -
<dot1x>
 [Authentication]
 IP address Port Timeout Retry Remain
 * 192.168.11.1 1812 10 5 -
 [Accounting]
 IP address Port Timeout Retry Remain
 * 192.168.11.1 1813 10 5 -
<mac-auth>
 [Authentication]
 IP address Port Timeout Retry Remain
 192.168.11.1 1812 10 5 -
 * hold down
 [Accounting]
```

```

 IP address Port Timeout Retry Remain
* 192.168.11.1 1813 10 5 -
<web-auth>
[Authentication]
 IP address Port Timeout Retry Remain
* 192.168.0.254 1812 5 3 -
[Accounting]
 IP address Port Timeout Retry Remain
* 192.168.0.254 1813 5 3 -
<ra-group-1>
[Authentication]
 IP address Port Timeout Retry Remain
 192.168.0.251 1812 5 3 -
 192.168.0.252 1812 5 3 -
 192.168.0.253 1812 5 3 -
* 192.168.0.254 1812 5 3 541

```

>

\* indicates the IP address of the currently used RADIUS server.

## (2) Displaying statistics of the effective RADIUS server

Display statistics about the effective RADIUS server set on the Switch.

- Use the `show radius-server statistics summary` operation command to display summary information.
- Use the `show radius-server statistics` operation command to display statistics.

**Figure 8-12** Execution results of the `show radius-server statistics summary` command

```

> show radius-server statistics summary

Date 2009/10/29 04:49:05 UTC }
 IP address:192.168.0.254 [Tx] Timeout:2 [Rx] Accept:10, Reject:2
 IP address:192.168.11.1 [Tx] Timeout:2 [Rx] Accept:12, Reject:2
>

```

**Figure 8-13** Execution results of the `show radius-server statistics` command

```

> show radius-server statistics

Date 2009/10/29 04:47:02 UTC
IP address: 192.168.0.254
[Authentication] Current Request: 0
 [Tx] Request : 12 Error : 1
 Retry : 2 Timeout: 2
 [Rx] Accept : 10 Reject : 2 Challenge : 0
 Malformed: 0 BadAuth: 0 UnknownType: 0
[Accounting] Current Request: 0
 [Tx] Request : 19 Error : 1
 Retry : 0 Timeout: 0
 [Rx] Responses: 19
 Malformed: 0 BadAuth: 0 UnknownType: 0
IP address: 192.168.11.1
[Authentication] Current Request: 0
 [Tx] Request : 14 Error : 1
 Retry : 2 Timeout: 2
 [Rx] Accept : 12 Reject : 2 Challenge : 0
 Malformed: 0 BadAuth: 0 UnknownType: 0
[Accounting] Current Request: 0
 [Tx] Request : 23 Error : 1
 Retry : 0 Timeout: 0
 [Rx] Responses: 23
 Malformed: 0 BadAuth: 0 UnknownType: 0
>

```

## 9. Time Settings and NTP

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

---

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 at first deployment of the Switch. Time information is used in the Switch's log entries and in timestamps when files are created. Set the correct time when you begin using the Switch. You can set the time using the [set clock](#) operation command.

You can also use Network Time Protocol (NTP) to synchronize the time to an NTP server on the network.

The following types of NTP client functionality are supported on the Switch.

**Table 9-1** NTP client functionality supported on the Switch

| Functionality                       | Description                                                                                                              |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Unicast mode                        | In this mode, the Switch regularly requests the time from the NTP server.                                                |
| Multicast mode                      | In this mode, the Switch obtains the time sent from the NTP server as a multicast message.                               |
| Broadcast mode                      | In this mode, the Switch obtains the time sent from the NTP server as a broadcast message.                               |
| Manual time acquisition             | You can obtain the time from the NTP server by using the <a href="#">set clock ntp</a> operation command. (Unicast mode) |
| Distribution source restriction     | Not supported                                                                                                            |
| Host name specification (using DNS) | Not supported                                                                                                            |
| Authentication type                 | Not supported                                                                                                            |
| Time adjustment                     | Not supported                                                                                                            |

If the setting for regularly obtaining the time is enabled in the configuration, the Switch requests the time from the NTP server at startup.

You can set more than one mode at the same time, but only one of them is enabled. You can perform manual time acquisition regardless of the following conditions.

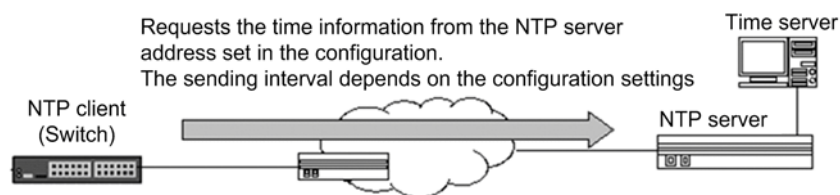
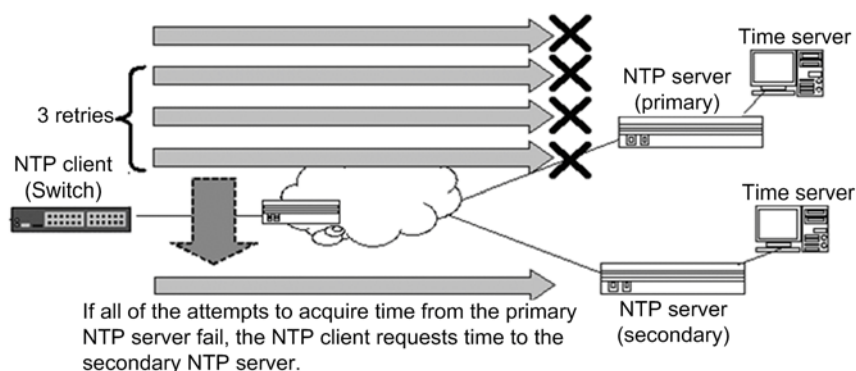
**Table 9-2** Mode to be enabled when multiple modes are set (Y: the mode is set, N: the mode is not set)

| Unicast | Multicast | Broadcast | Mode to be enabled |
|---------|-----------|-----------|--------------------|
| Y       | N         | N         | Unicast            |
| Y       | Y         | N         | Unicast            |
| Y       | N         | Y         | Unicast            |
| Y       | Y         | Y         | Unicast            |
| N       | Y         | N         | Multicast          |
| N       | Y         | Y         | Multicast          |
| N       | N         | Y         | Broadcast          |

**(1) Regularly requesting the time from the specified NTP server (Unicast mode)**

In this mode, set the address of the NTP server from which the Switch requests the time. The Switch regularly requests time information from the NTP server, and updates the local time based on the obtained time information. (You can configure the interval for the requests issued to the NTP server.)

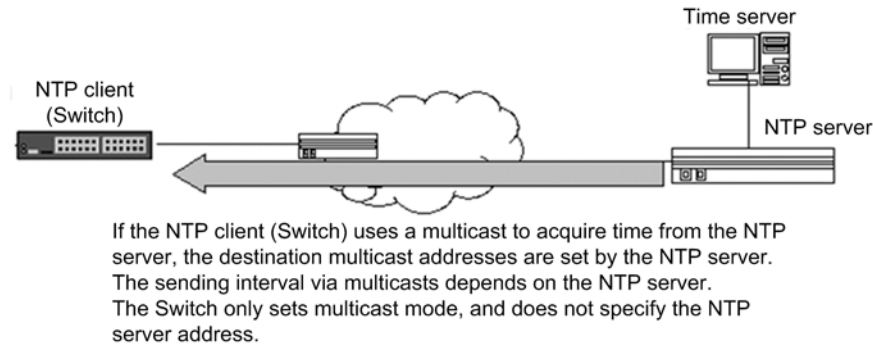
You can register a maximum of two NTP server addresses. The address that is registered first is called the primary address. The address that is registered second is called the secondary address. If the Switch fails to obtain the time from the primary NTP server address, the Switch requests time information from the secondary NTP server address.

**Figure 9-1** Time acquisition in Unicast mode (when the primary address is set)**Figure 9-2** Time acquisition in Unicast mode (when the primary and secondary addresses are set)

## (2) Obtaining the time from a multicast message (Multicast mode)

In Multicast mode, the Switch receives the multicast time distribution from the NTP server, and updates the local time based on the obtained time information.

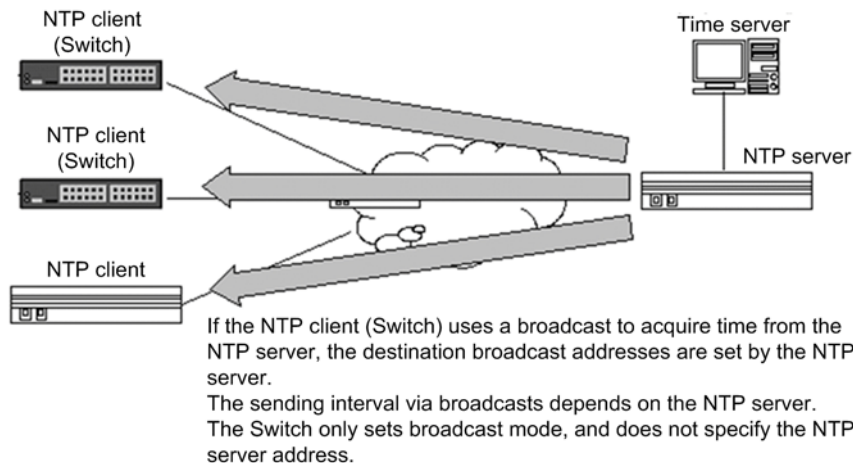
**Figure 9-3** Time acquisition in Multicast mode



## (3) Obtaining the time from a broadcast message (Broadcast mode)

In Broadcast mode, the Switch receives the broadcast time distribution from the NTP server, and updates the local time based on the obtained time information.

**Figure 9-4** Time acquisition in Broadcast mode



## (4) Manual acquisition

Use an operation command to specify an NTP server address. The Switch requests time information from the NTP server, and then updates the local time based on the obtained time information. If an NTP server address is not specified, the NTP server address set in the configuration for regular time update is used.

### 9.1.2 Notes on changing the time

CPU usage in the statistics collected on the Switch is cleared to 0 in the following cases:

- The Switch is restarted or in sleep mode due to the scheduling of the power-saving functionality.
- The time zone is changed by the `clock timezone` configuration command.
- The `set clock` operation command is executed, or the time is changed on the NTP client (only the data displayed in seconds is cleared).



## 9.2 Configuration

### 9.2.1 List of configuration commands

The following table describes the commands used to configure time settings and NTP.

**Table 9-3** List of configuration commands

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

### 9.2.2 Setting the system clock

Points to note

To set the switch's system clock, you must first set the time zone. To set the clock to Japan standard time for example, 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 command 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 `22.02.11`.

### 9.2.3 Regularly obtaining time information from the NTP server

Using the NTP client functionality, the Switch regularly obtains time information from the NTP server.

Points to note

You can set the address of the NTP server from which the Switch requests time information. Use the `ntp interval` configuration command to set the interval of the requests.

Command examples

1. `(config)# ntp client server 192.168.1.100`

Sets the address of the NTP server from which the Switch requests time information.

2. `(config)# ntp interval 7200`

Sets the interval (in seconds) for requesting time information from the NTP server. (If the `ntp interval` configuration command has not been set, the default interval of 3,600 seconds (1 hour) is used for the Switch to request the time information.)

## 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                                            |
|-----------------|--------------------------------------------------------|
| set clock       | Displays and sets the date and time.                   |
| set clock ntp   | Manually obtains time information from the NTP server. |
| show clock      | Displays the currently set date and time.              |
| show ntp-client | Displays 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 9-5** Checking the time

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

### 9.3.3 Displaying the NTP client information

When the Switch obtains time information from the NTP server, you can use the `show ntp-client` operation command to display the NTP client information. An example is shown below:

**Figure 9-6** Displaying the NTP client information

```
> show ntp-client

Date 2009/02/23 11:38:05 UTC
Last NTP Status
 NTP-Server : 192.168.7.1, Source-Address : ---
 Mode : Multicast, Lapsed time : 14(s), Offset : 1(s)

Activate NTP Client
 NTP-Server : ---, Source-Address : ---
 Mode : Multicast

NTP Execute History(Max 10 entry)
 NTP-Server Source-Address Mode Set-NTP-Time Status
 192.168.7.1 --- Multicast 2009/02/23 11:37:51 1
 192.168.7.1 --- Multicast 2009/02/23 11:36:51 1
 192.168.7.1 --- Multicast 2009/02/23 11:35:51 1
 192.168.7.2 --- Command 2009/02/23 11:35:24 Timeout
 192.168.7.1 --- Multicast 2009/02/23 11:34:51 1
 192.168.7.2 --- Command 2009/02/23 11:34:15 Timeout
 192.168.7.1 --- Multicast 2009/02/23 11:33:51 1
 192.168.7.1 --- Multicast 2009/02/23 11:32:51 1
 192.168.7.1 --- Multicast 2009/02/23 11:31:51 1
 192.168.7.1 --- Multicast 2009/02/23 11:30:51 0
>
```



---

## 10. Device Management

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

|      |                                                           |
|------|-----------------------------------------------------------|
| 10.1 | Settings related to status display and system operation   |
| 10.2 | Backing up and restoring device information               |
| 10.3 | Compatibility between AX2200S and AX1200S series switches |
| 10.4 | Failure recovery                                          |

## 10.1 Settings related to status display and system operation

### 10.1.1 Lists of configuration commands and operation commands

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

**Table 10-1** List of configuration commands

| Command name                             | Description                                                                                                                                      |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| system fan mode                          | Sets the operating mode of the fan.                                                                                                              |
| system function<br>[AX1250S] [AX1240S]   | Configures the distribution of system function resources for a Switch.                                                                           |
| system l2-table mode                     | Sets the search method for the Layer 2 hardware table.                                                                                           |
| system recovery                          | When the <code>no system recovery</code> command is set and a failure is detected, the Switch does not restart and remains in the failure state. |
| system temperature-warning-level         | Outputs a warning message when the intake temperature of the switch exceeds the specified temperature.                                           |
| system temperature-warning-level average | Outputs an operation message when the average temperature of the Switch for the specified period exceeds the specified temperature.              |

**Table 10-2** Operation commands (software version and switch status check)

| Command name      | Description                                                                                                                |
|-------------------|----------------------------------------------------------------------------------------------------------------------------|
| show version      | Displays information about the Switch software and the board installed.                                                    |
| show system       | Shows the Switch's operating status.                                                                                       |
| show environment  | Displays the status of the fan and of the power supply unit, the temperature, and the total operating hours of the Switch. |
| reload            | Restarts the switch.                                                                                                       |
| show tech-support | Collects hardware and software status information required for technical support.                                          |

**Table 10-3** Operation commands (memory card and RAMDISK check)

| Command name      | Description                                                   |
|-------------------|---------------------------------------------------------------|
| show mc           | Displays the memory card format and card usage.               |
| show mc-file      | Displays the names and sizes of the files on the memory card. |
| show ramdisk      | Displays the RAMDISK format and usage.                        |
| show ramdisk-file | Displays the names and sizes of the files on the RAMDISK.     |
| format flash      | Initializes the internal flash memory file system.            |
| format mc         | Initializes formats the memory card for use by the Switch.    |

**Table 10-4** Operation commands (logging control)

| Command name           | Description                                                                         |
|------------------------|-------------------------------------------------------------------------------------|
| show logging           | Displays only the messages and the times that operation log entries were acquired.  |
| clear logging          | Erases the operation log entries recorded by the Switch.                            |
| show critical-logging  | Displays the detailed information regarding device failure log data as log records. |
| clear critical-logging | Erases the switch failure log entries recorded by the Switch.                       |

**Table 10-5** Operation commands (resource information check)

| Command name        | Description                                                                                            |
|---------------------|--------------------------------------------------------------------------------------------------------|
| show cpu            | Shows CPU usage.                                                                                       |
| show memory summary | Display the installed capacity, used capacity, and free capacity of the physical memory of the device. |

### 10.1.2 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 10-1** Checking software version

```
> show version

Date 2009/03/17 16:31:29 UTC
Model: AX1240S-24P2C
S/W: OS-LT2 Ver. 2.1 (Build:yy)
H/W: AX-1240-24P2C [ssssssssssssssssssss:0]

>
```

### 10.1.3 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 10-2** Checking the switch status

```
> show system

Date 2012/07/06 10:11:19 UTC

System: AX1240S-48T2C Ver. 2.4 (Build:yy)
 Name : AX1240S-48T225
 Contact : -
 Locate : -
 Machine ID : 0012.e210.0001
 Boot Date : 2012/07/05 21:38:07
 Elapsed time : 0 days 12:33:12
 LED
 ST1 LED : Green
 Brightness mode : normal

Environment
 Fan : active
 Temperature : normal
 Accumulated running time
 total : 808 days and 0 hours
 critical : 0 days and 0 hours

File System
 < RAMDISK information >
 used 9,079,808 byte
 free 3,503,104 byte
 total 12,582,912 byte
 < RAMDISK files >
 File Date Size Name
 2012/07/05 21:38 1,024 oan/
 2012/07/06 10:08 9,011,200 work.img
 2012/07/05 21:38 1,024 oan/wa_files/
 < MC information >
 MC : not connect

System Setting
 set terminal pager : disabled (save: disabled)
 line console speed : 9600 (save: 9600)
 trace-monitor : enabled (save: enabled)
 set exec-timeout : 0 (save: 0)

Device Resources
 IP Routing Entry(static) : 5(max entry=128)
 IP Routing Entry(connected) : 4(max entry=128)
 IP Interface Entry : 4(max entry=128)
 IP ARP Entry : 3(max entry=2048)
 MAC-address Table Entry : 16(max entry=16384)

System Layer2 Table Mode : 1
Flow detection mode : Layer 2-2
 Used resources for filter(Used/Max)
 MAC IPv4
 Port 0/1-50 : - 0/128
 VLAN : - 0/128
 Used resources for QoS(Used/Max)
```



```

MAC IPv4
Port 0/1-50 : - 0/64
VLAN : - 0/64

```

&gt;

You can check the status of the fan and of the 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 by using the `system fan mode` configuration command. An example is shown below:

**Figure 10-3** Checking the Switch environment

```
> show environment
```

```
Date 2012/07/06 10:10:45 UTC
```

```
Fan environment
```

```
Fan : active
```

```
Mode : 1 (silent)
```

```
Temperature environment
```

```
Main : 30 degrees C
```

```
Warning level : normal
```

```
Temperature-warning-level current status : 30/40 degrees C
```

```
Temperature-warning-level average status : 27/35 degrees C period 30 day(s)
```

```
Accumulated running time
```

```
total : 808 days and 0 hours
```

```
critical : 0 days and 0 hours
```

&gt;

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

**Figure 10-4** Checking temperature log data

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

```
Date 2011/02/16 21:54:23 UTC
```

```
Date 0:00 6:00 12:00 18:00
```

```
2011/02/16 30.0 30.3 28.0 27.8
```

```
2011/02/15 31.0 32.0 29.8 31.1
```

```
2011/02/14 - - 29.2 30.0
```

```
2011/02/13 29.0 30.2 28.0 15.0
```

```
2011/02/12 28.8 30.0 30.0 28.0
```

```
2011/02/11 31.6 32.0 28.0 28.0
```

```
2011/02/10 31.0 30.1 28.9 29.8
```

```
2011/02/09 - - - 30.1
```

&gt;

### (1) Notes about support for a long life solution

Note the following if you set the `system temperature-warning-level` configuration command or check temperature information in the temperature log data when a long life solution is supported:

1. For the temperature to be specified in the `system temperature-warning-level` configuration command, specify the Switch air intake temperature. As a result, 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 being used or the SFP type on the Switch.
2. The functionality supporting a long life solution starts monitoring 60 minutes after all configurations are applied at startup.

### 10.1.4 Displaying and stopping display of the operation log on the monitor

By setting the `trace-monitor` operation command, you can make the Switch display, on the monitor, operating information and failure information as operation logs on the operation terminal (console). For example, if communication becomes enabled, an operation log that shows communication is enabled is displayed; if communication becomes disabled, an operation log that shows communication is disabled is displayed.

**Figure 10-5** Displaying an operation log on the monitor

```
> trace-monitor enable save
>
```

If you enter the `save` option, operation logs will be displayed on the monitor even after the Switch is restarted.

**Figure 10-6** Stopping display of an operation log on the monitor

```
> trace-monitor disable save
>
```

Note

When a large number of operation logs are generated in succession, the following message might be displayed on the console or remote operation terminal:

`WARNING!! There are too many messages to output.` This message indicates that some operation logs could not be displayed, so check them by executing the `show logging` operation command.

### 10.1.5 Viewing logged data

You can save operation log data in the Switch, as well as displaying it on the operation terminal (console). You can use this information to manage the operating status of switches and failures.

The operation log records information about events that occur during switch operation in chronological order. This information is the same as the operation logs displayed on the monitor. The following information is saved as an operation log:

- User command operations and response messages (not displayed on the monitor)
- Operation information output by the switch
- Device failure logs

This data is logged in text format inside the switch. To view the entries, use the `show logging` operation command. In addition, device failure logs can be checked via the operation command `show critical-logging`.

### 10.1.6 Functions that use system function resources [AX1250S] [AX1240S]

All functions of AX1250S and AX1240S series switches can be used even if the `system function` configuration command has not been set. The `system function` configuration command can be input on the AX1250S and AX1240S series switches for compatibility with AX1230S series switches.

## 10.2 Backing up and restoring device information

When a Switch fault occurs or a Switch is replaced, you can restore the Switch by restoring the device information from a backup file.

Carry out the tasks described in *10.2.2 Target information to be backed up and restored*. You can also restore all information manually, but we do not recommend this because the Switch handles a wide variety of operating information which is complicated to manage and cannot be fully restored.

### 10.2.1 List of operation commands

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

**Table 10-6** List of operation commands

| Command name | Description                                                                 |
|--------------|-----------------------------------------------------------------------------|
| backup       | Saves information about the running software and device to the memory card. |
| restore      | Restores the device information saved on the memory card to the Switch.     |

### 10.2.2 Target information to be backed up and 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 below, which is required for switch operation, in one file, and then saves the file to a memory card.

We recommend that you create a backup file when updating such information.

**Table 10-7** Device information to be saved in a backup file

| Device information type                       | Remarks                                                                               |
|-----------------------------------------------|---------------------------------------------------------------------------------------|
| Running software                              |                                                                                       |
| Startup configuration file                    |                                                                                       |
| User ID and password for login authentication | <code>rename user</code> operation command<br><code>password</code> operation command |
| Administrator mode password                   | <code>password enable-mode</code> operation command                                   |
| Auto-logout setting                           | <code>set exec-timeout</code> operation command                                       |
| Paging setting                                | <code>set terminal pager</code> operation command                                     |
| Console port speed setting                    | <code>line console speed</code> operation command                                     |
| Setting of monitor display of operation logs  | <code>trace-monitor</code> operation command                                          |
| Device fault logs                             | <code>show critical-logging</code> operation                                          |

| Device information type                                                                                        | Remarks                                                                                                             |
|----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
|                                                                                                                | command                                                                                                             |
| Web authentication database                                                                                    | Internal Web authentication DB                                                                                      |
| Registered HTML files for Web authentication pages<br>(Registered custom file set for the authentication page) | Custom file set for the basic Web authentication page<br>Custom file set for the individual Web authentication page |
| Certificate for Web authentication                                                                             |                                                                                                                     |
| MAC-based authentication database                                                                              | Internal MAC-based authentication DB                                                                                |
| DHCP snooping binding database                                                                                 |                                                                                                                     |
| Optional licenses                                                                                              |                                                                                                                     |
| Secure Wake-on-LAN terminal information database<br>[OP-WOL]                                                   | WOL terminal information DB                                                                                         |
| Secure Wake-on-LAN user authentication database<br>[OP-WOL]                                                    | WOL user authentication DB                                                                                          |

Note that the [backup](#) operation command does not save operation logs displayed as a result of 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. At update completion, the Switch restarts automatically, and the restoration is completed.

Note that the [restore](#) operation command does not restore failure information displayed as a result of the [show critical-logging](#) operation command.

### (a) Custom file set when changing the version

When the Switch is changed from version 2.2 or later to a version earlier than version 2.2 or when a file backed up with version 2.2 or later is restored in a switch that has a version earlier than 2.2, all the registered custom file sets are deleted. This means that the basic Web authentication page custom file sets and the individual Web authentication page custom file sets are all deleted, and the default file set is restored.

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

## 10.3 Compatibility between AX2200S and AX1200S series switches

### 10.3.1 Compatibility between AX2200S and AX1200S series switches

AX2200S series switches and AX1250S/AX1240S series switches have compatibility in some device information as shown in the following table.

**Table 10-8** Compatibility of device information between AX2200S series switches and AX1250S/AX1240S series switches

| Device information                                                                                             | AX2200S →<br>AX1250S/AX1240S | AX1250S/AX1240S<br>→ AX2200S |
|----------------------------------------------------------------------------------------------------------------|------------------------------|------------------------------|
| Web authentication database                                                                                    | Y                            | Y                            |
| Registered HTML files for Web authentication pages<br>(Registered custom file set for the authentication page) | Y                            | Y                            |
| MAC-based authentication database                                                                              | Y                            | Y                            |
| Secure Wake-on-LAN terminal information database<br>[OP-WOL]                                                   | Y                            | Y                            |
| Secure Wake-on-LAN user authentication database<br>[OP-WOL]                                                    | Y                            | Y                            |

Legend:

Y: Compatible.

→: Copy destination of the file saved in a memory card

### 10.3.2 Compatibility of input commands between AX1250S/AX1240S series switches and AX1230S series switches

#### (1) Configuration commands

The configuration commands below have been changed in AX1250S and AX1240S series switches. For example, there have been changes in input format.

Commands in AX1230S format can be input in AX1250S and AX1240S series switches, but they are supported with some restrictions as follows:

- Help, command line completion and abbreviated commands in AX1230S format are not supported.
- Commands input in AX1230S format are automatically converted to AX1250S and AX1240S format in the Switch.
- The configuration is displayed and saved in AX1250S and AX1240S format.

**Table 10-9** Configuration commands

| AX1250S/AX1240S command | Change from AX1230S                                                  |
|-------------------------|----------------------------------------------------------------------|
| system function         | Behavior when the command is omitted has been changed <sup>#</sup> . |

| AX1250S/AX1240S command                                                                                                                                                                                                                                                                  | Change from AX1230S                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| deny (ip access-list extended)<br>deny (ip access-list standard)<br>deny (mac access-list extended)<br>permit (ip access-list extended)<br>permit (ip access-list standard)<br>permit (mac access-list extended)<br>qos (ip qos-flow-list)<br>qos (mac qos-flow-list)<br>monitor session | The input format has been changed. |
| ip qos-flow-list<br>mac qos-flow-list                                                                                                                                                                                                                                                    | The command has been changed.      |
| ip qos-flow-list resequence<br>mac qos-flow-list resequence                                                                                                                                                                                                                              | The input mode has been changed.   |

#

If the configuration file in which the `system function` command has been set on an AX1230S series switch is restored on the Switch, the setting value is inherited. In this case, if the `system function` command has not been set, the default value on the AX1250S and AX1240S series switch is used. For details, see *10.1.6 Functions that use system function resources [AX1250S] [AX1240S]*.

For details about each command, see the *Configuration Command Reference*.

## (2) Operation commands

The operation commands below have been changed in AX1250S and AX1240S series switches. This includes changes in command names and input format. Displayed information and behavior have not been changed.

**Table 10-10** Operation commands

| AX1250S/AX1240S command                                                                                                            | Change from AX1230S                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| show logging                                                                                                                       | <code>show event-trace</code> has been changed to <code>show logging</code> .<br><code>show event-trace additional</code> has been abolished. |
| clear logging                                                                                                                      | <code>clear event-trace</code> has been changed to <code>clear logging</code> .                                                               |
| show critical-logging                                                                                                              | <code>show log</code> has been changed to <code>show critical-logging</code> .                                                                |
| clear critical-logging                                                                                                             | <code>clear log</code> has been changed to <code>clear critical-logging</code> .                                                              |
| set clock<br>show vlan mac-vlan<br>show access-filter<br>show qos-flow<br>show qos queueing<br>clear mac-authentication auth-state | The input format has been changed.                                                                                                            |

For details about each command, see the *Operation Command Reference*.

### 10.3.3 Compatibility of device information between AX1250S series switches and AX1240S series switches

The table below shows the compatibility of device information between AX1250S series switches and AX1240S series switches.

- The left side of an arrow (→) indicates the device on which the backup file was created.
- The right side of an arrow (→) indicates the device on which the file is restored.

**Table 10-11** Compatibility of device information between X1250S series switches and AX1240S series switches

| Device information type                                                                                        | AX1240S→AX1250S | AX1250S→AX1240S |
|----------------------------------------------------------------------------------------------------------------|-----------------|-----------------|
| Running software                                                                                               | N               | N               |
| Startup configuration file                                                                                     | R <sup>#1</sup> | Y               |
| User ID and password for login authentication                                                                  | Y               | Y               |
| Administrator mode password                                                                                    | Y               | Y               |
| Auto-logout setting                                                                                            | Y               | Y               |
| Paging setting                                                                                                 | Y               | Y               |
| Console port speed setting                                                                                     | Y               | Y               |
| Setting of monitor display of operation logs                                                                   | Y               | Y               |
| Device fault logs                                                                                              | N <sup>#2</sup> | N <sup>#2</sup> |
| Web authentication database                                                                                    | Y               | Y               |
| Registered HTML files for Web authentication pages<br>(Registered custom file set for the authentication page) | Y               | Y               |
| Certificate for Web authentication                                                                             | Y               | Y               |
| MAC-based authentication database                                                                              | Y               | Y               |
| DHCP snooping binding database                                                                                 | Y               | Y               |
| Optional licenses                                                                                              | Y               | Y               |
| Secure Wake-on-LAN terminal information database<br>[OP-WOL]                                                   | Y               | Y               |
| Secure Wake-on-LAN user authentication database<br>[OP-WOL]                                                    | Y               | Y               |

Legend:

Y: Compatible.

N: Not compatible.

R: With some restrictions

→: Restore destination of the created file

#1

Commands that are not supported on AX1250S series switches cannot be read.

#2

Cannot be restored by the [restore](#) operation command.

### 10.3.4 Compatibility of device information between AX1250S/AX1240S series switches and AX1230S series switches

The table below shows the compatibility of device information between AX1250S and AX1240S series switches and AX1230S series switches.

When restoring AX1250S and AX1240S device information (other than software) on an AX1230S series switch, execute the [backup](#) operation command with the [AX1230](#) option specified to create a backup file. (If the [AX1230](#) option is not specified, the created backup file cannot be restored on an AX1230S series switch.)

- The left side of an arrow (→) indicates the device on which the backup file was created.
- The right side of an arrow (→) indicates the device on which the file is restored.

**Table 10-12** Compatibility of device information between AX1250S and AX1240S series switches and AX1230S series switches

| Device information type                                                                                        | AX1230S→<br>AX1250S/AX1240S | AX1250S/AX1240S<br>→AX1230S |
|----------------------------------------------------------------------------------------------------------------|-----------------------------|-----------------------------|
| Running software                                                                                               | N                           | N                           |
| Startup configuration file                                                                                     | Y                           | R <sup>#1</sup>             |
| User ID and password for login authentication                                                                  | Y                           | Y                           |
| Administrator mode password                                                                                    | Y                           | Y                           |
| Auto-logout setting                                                                                            | Y                           | Y                           |
| Paging setting                                                                                                 | Y                           | Y                           |
| Console port speed setting                                                                                     | Y                           | Y                           |
| Setting of monitor display of operation logs                                                                   | Y                           | Y                           |
| Device fault logs                                                                                              | N <sup>#2</sup>             | N <sup>#2</sup>             |
| Web authentication database                                                                                    | Y                           | R <sup>#4, #5</sup>         |
| Registered HTML files for Web authentication pages<br>(Registered custom file set for the authentication page) | R <sup>#3</sup>             | R <sup>#6</sup>             |
| Certificate for Web authentication                                                                             | Y                           | R <sup>#4</sup>             |
| MAC-based authentication database                                                                              | Y                           | R <sup>#4</sup>             |
| DHCP snooping binding database                                                                                 | Y                           | R <sup>#4</sup>             |
| Optional licenses                                                                                              | --                          | N                           |



| Device information type                                   | AX1230S→<br>AX1250S/AX1240S | AX1250S/AX1240S<br>→AX1230S |
|-----------------------------------------------------------|-----------------------------|-----------------------------|
| Secure Wake-on-LAN terminal information database [OP-WOL] | --                          | N                           |
| Secure Wake-on-LAN user authentication database [OP-WOL]  | --                          | N                           |

Legend:

Y: Compatible.

N: Not compatible.

R: With some restrictions

--: Not supported and not be included in the backup file.

→: Restore destination of the created file

#1

Commands that are not supported in AX1230S series switches cannot be read.

#2

Cannot be restored by the [restore](#) operation command.

#3

Depending on the software version of the AX1230S series switch, it might be necessary to add tags specific to Web authentication to the Web authentication replacement window file.

**Table 10-13** Adding tags specific to Web authentication to the Web authentication replacement window file

| Version of AX1230S   | Tags to be added specific to Web authentication                                                                                                                                                                                                                                                                                                |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version 1.2 to 1.2.x | Write the following: tags specific to Web authentication (" <a href="#">&lt;!-- Redirect_URL --&gt;</a> "), which is used to automatically display URL, and the URL to be displayed after a successful login and the time to move to the URL (configuration setting in the <a href="#">web-authentication jump-url</a> configuration command). |
| Version 1.3 to 1.3.x | Write the time to move to the specified URL under the tags specific to Web authentication (" <a href="#">&lt;!-- Redirect_URL --&gt;</a> "), which is used to automatically display URL. Set the time to the value of the <a href="#">delay</a> parameter in the <a href="#">web-authentication jump-url</a> configuration command.            |
| Version 1.4 or later | Adding of tags is not necessary.                                                                                                                                                                                                                                                                                                               |

When one-time password authentication is used, the Web authentication replacement window file and tags specific to Web authentication are added. For more details, see *14 One-time Password Authentication [OP-OTP]* in the *Configuration Guide Vol. 2*.

#4

Restoration is available if the software version of the AX1230S series switch is version 1.3 or later.

### #5

When you restore the internal Web authentication DB on an AX1230S series switch, note the behaviors below. Note the following, also when you restore a backup file created by using the [store web-authentication](#) operation command:

1. The internal Web authentication DB cannot be read to an AX1230S series switch if the DB has an entry with a user ID of 17 characters or more.
2. The internal Web authentication DB can be read to an AX1230S series switch if the user IDs contained in all entries in the DB are in no more than 16 characters. However, users whose passwords are 17 characters or more cannot be authenticated.

### #6

The custom file set (of basic Web authentication page and individual Web authentication page) format of version 2.2 or later is not supported on AX1230S series switches, so the custom file set is deleted and the initial default file set is used.

## 10.4 Failure recovery

### 10.4.1 Error locations and recovery processing

Recovery processing differs according to the nature of the problem. The following table describes error locations and the recovery performed.

**Table 10-14** Error locations and recovery processing

| Error location       | Switch response                                                                                                                                                            | Recovery processing                                    | Scope of effect                                         | AX2200S<br>AX1250S<br>AX1240S |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|---------------------------------------------------------|-------------------------------|
| Main board           | Restarts the switch for restoration.                                                                                                                                       | Restarts the switch. <sup>#</sup>                      | Communication via all ports on the switch is suspended. | Y                             |
| SW chip              | Starts automatic-restoration when a parity error occurs in internal memory. If the fault continues after restoration, the switch is restarted to complete the restoration. | Sets the error location to normal status. <sup>#</sup> | Yes                                                     | Y                             |
| Port failure         | Nothing is executed.                                                                                                                                                       | There is no means of auto-recovery.                    | Communication via the relevant port might be affected.  | --                            |
| Abnormality in power | Restarts the switch when the power required to run the switch ceases to be supplied.                                                                                       | Restarts the switch.                                   | Communication via all ports on the switch is suspended. | Y                             |
| FAN                  | Nothing is executed.                                                                                                                                                       | There is no means of auto-recovery.                    | No effect.                                              | --                            |

Legend:

Y: Automatic-restoration is performed.

--: Automatic-restoration is not performed.

#

When the `no system recovery` configuration command has been set so that no restoration processing is performed, even if a critical failure occurs (when a FATAL-level error log is collected), automatic-restoration is not performed.

#### (2) Automatic restoration disabled status

Automatic restoration stops when system recovery is disabled (`no system-recovery`). If a critical failure (FATAL-level error) occurs, the Switch is not restarted after the error log is collected. In such cases, the ST1 LED lights red, all ports are placed in the link-down status, and communication stops.

If the power saving functionality based on scheduling is configured, the scheduling is stopped to restrain the power saving operation (LED operation, port power saving, or sleep mode).

##### (a) Collecting the device status information while automatic restoration is disabled

If automatic restoration is disabled, execute the `show tech-support` operation command

on the console terminal to collect device status information, and then restore the Switch.

When executing the `show tech-support` operation command while automatic restoration is disabled, only display to the console terminal is permitted. Therefore, do not specify the `ramdisk` or `page` option in this command. For information displayed on the console screen by executing this command, use the capture function of the console terminal to collect the information.

Note the following when automatic restoration is disabled on the Switch:

- Do not update software while automatic restoration is disabled. Restore the Switch, and then start updating.
- You might not be able to execute commands normally while automatic restoration is disabled.

### **(b) Restoration of the Switch**

Perform the following to restore the Switch from the status of automatic restoration being disabled:

- Restart the Switch by turning off and on the power, or by pressing the RESET button.
- If software is hung up while automatic restoration is disabled, reset the hardware to restart the Switch.

---

# 11. Power Saving Functionality

This chapter describes functionality and settings on the Switch for saving power.

---

11.1 Description of the power saving functionality

---

11.2 Power control configuration

---

11.3 Power control operation

---

## 11.1 Description of the power saving functionality

You can reduce power consumption of the Switch by using power saving functionality to put the Switch in sleep mode during the scheduled period, such as at night or during long holidays.

### 11.1.1 Supported functionality

When using the power saving functionality supported by the Switch, you can operate the Switch always in power saving mode, or set a schedule to specify the time period when the Switch is to operate in power saving mode. The table below describes power saving functionality that operate in normal time ranges and in scheduled time ranges.

A time period for which power saving is set is referred to as a scheduled time range and a time period for which power saving is not set is referred to as a normal time range.

**Table 11-1** Supported power saving functionality

| Functionality                                                            | Description                                                         | Setting for the normal time range | Setting for the scheduled time range | AX2200S         | AX1250S<br>AX1240S |
|--------------------------------------------------------------------------|---------------------------------------------------------------------|-----------------------------------|--------------------------------------|-----------------|--------------------|
| LED behavior                                                             | Normal brightness, power saving brightness, and Off                 | Y                                 | Y                                    | Y <sup>#3</sup> | Y                  |
|                                                                          | Trigger for automatic operation                                     | Y                                 | N                                    | Y <sup>#3</sup> | Y                  |
| Port power saving                                                        | Power saving for ports in the link-down status <sup>#1</sup>        | Y                                 | Y                                    | Y               | Y                  |
|                                                                          | Extended power saving for Gigabitethernet ports <sup>#1</sup>       | Y                                 | Y                                    | N               | Y                  |
|                                                                          | Port blocking (setting for ports not to be used)                    | Y                                 | Y                                    | Y               | Y                  |
| Sleep mode                                                               | Turning off and automatic turning on of the Switch power            | N                                 | Y                                    | N               | Y                  |
| Cooling fan control functionality (Semi-fanless operation) <sup>#2</sup> | Turning the cooling fan off and on according to temperature changes | Y                                 | N                                    | N               | Y                  |

Legend:

Y: Supported

N: Not supported

<sup>#1</sup>

Applicable ports are Fastethernet ports and Gigabitethernet ports. SFP ports are not applicable.

<sup>#2</sup>

Applied to AX1240S-48T2C only.

#3

Normal brightness and Off are supported. Power saving brightness is not supported.

In this chapter, ports are referred as follows:

- 10BASE-T or 100BASE-TX port: Fastethernet port
- 10BBASE-T, 100BASE-TX, or 1000BASE-T: Gigabitethernet port
- 100BASE-FX [AX1250S] or 1000BASE-X port: SFP port

### 11.1.2 LED behavior

This configuration function controls LED behavior in two steps for AX2200S series switches or in three steps for AX1250S and AX1240S series switches. Also, LED behavior can be automatically changed if you set a trigger for automatic operation in the Switch's configuration.

#### (1) LED behaviors

Use the `system port-led` configuration command to set either of the following LED behaviors:

- Normal brightness: The LEDs operate at normal brightness.
- Power saving brightness: The LEDs operate at a lower brightness level than normal.
- Off: The LEDs of all ports are turned off. (ST1 and ACC also operate in a state of reduced brightness.)

The LEDs below can be controlled by the configuration. The PWR LED is not subject to control. The PWR LED always illuminates with normal brightness. For details about the LEDs, see the *Hardware Instruction Manual*.

- ST1
- ACC
- LINK
- T/R
- 1 to 24: AX2230S-24T, AX2230S-24P, AX1250S-24T2C, AX1240S-24T2C and AX1240S-24P2C
- 1 to 48: AX1240S-48T2C

The following table describes LED status for each LED behavior setting configured by the `system port-led` configuration command.

**Table 11-2** LED status for each configuration setting of LED behavior [AX2200S]

| LED type | Device status           | LED behavior setting configured by the system port-led configuration command |                   |                                  |                   |
|----------|-------------------------|------------------------------------------------------------------------------|-------------------|----------------------------------|-------------------|
|          |                         | Normal brightness (enable)                                                   |                   | Off (disable)                    |                   |
|          |                         | LED status                                                                   | Brightness status | LED status                       | Brightness status |
| ST1      | Available for operation | Green                                                                        | Regular           | Blinking green at long intervals | Regular           |
|          | Under preparation       | Blinking green                                                               | Regular           | Blinking green                   | Regular           |

## 11 Power Saving Functionality

| LED type               | Device status               | LED behavior setting configured by the system port-led configuration command |                   |               |                   |
|------------------------|-----------------------------|------------------------------------------------------------------------------|-------------------|---------------|-------------------|
|                        |                             | Normal brightness (enable)                                                   |                   | Off (disable) |                   |
|                        |                             | LED status                                                                   | Brightness status | LED status    | Brightness status |
|                        | Initial state               | Orange                                                                       | Regular           | Orange        | Regular           |
|                        | Partial fault               | Blinking red                                                                 | Regular           | Blinking red  | Regular           |
|                        | fatal failure               | Red                                                                          | Regular           | Red           | Regular           |
|                        | Power off/<br>power failure | Off                                                                          | --                | Off           | --                |
| ACC                    | Accessing                   | Green                                                                        | Regular           | Green         | Regular           |
|                        | Idling                      | Off                                                                          | --                | Off           | --                |
| LINK/T/R <sup>#1</sup> | Link established            | Green                                                                        | Regular           | Off           | --                |
|                        | Sending and receiving       | Blinking green                                                               | Regular           | Off           | --                |
|                        | Link not established        | Off                                                                          | --                | Off           | --                |
|                        | Failed                      | Off                                                                          | --                | Off           | --                |
| 1 to 24 <sup>#2</sup>  | Link established            | Green                                                                        | Regular           | Off           | --                |
|                        | Sending and receiving       | Blinking green                                                               | Regular           | Off           | --                |
|                        | Failed                      | Off                                                                          | --                | Off           | --                |

#1

SFP ports

#2

Gigabitethernet ports

**Table 11-3** LED status for each configuration setting of LED behavior [AX1250S]  
[AX1240S]

|  |  | LED behavior setting configured by the system port-led configuration command |                                   |               |
|--|--|------------------------------------------------------------------------------|-----------------------------------|---------------|
|  |  | Normal brightness (enable)                                                   | Power saving brightness (economy) | Off (disable) |



| LED type                                       | Device status               | LED status     | Brightness status | LED status     | Brightness status  | LED status                       | Brightness status  |
|------------------------------------------------|-----------------------------|----------------|-------------------|----------------|--------------------|----------------------------------|--------------------|
| ST1                                            | Available for operation     | Green          | Regular           | Green          | Reduced brightness | Blinking green at long intervals | Reduced brightness |
|                                                | Under preparation           | Blinking green | Regular           | Blinking green | Regular            | Blinking green                   | Regular            |
|                                                | Initial state               | Orange         | Regular           | Orange         | Regular            | Orange                           | Regular            |
|                                                | Partial fault               | Blinking red   | Regular           | Blinking red   | Reduced brightness | Blinking red                     | Reduced brightness |
|                                                | fatal failure               | Red            | Regular           | Red            | Reduced brightness | Red                              | Reduced brightness |
|                                                | Power off/<br>power failure | Off            | --                | Off            | --                 | Off                              | --                 |
| ACC                                            | Accessing                   | Green          | Regular           | Green          | Reduced brightness | Green                            | Reduced brightness |
|                                                | Idling                      | Off            | --                | Off            | --                 | Off                              | --                 |
| LINK <sup>#1</sup>                             | Link not established        | Green          | Regular           | Green          | Reduced brightness | Off                              | --                 |
|                                                | Link established            | Off            | --                | Off            | --                 | Off                              | --                 |
|                                                | Failed                      | Off            | --                | Off            | --                 | Off                              | --                 |
| T/R <sup>#1</sup>                              | Sending and receiving       | Blinking green | Regular           | Blinking green | Reduced brightness | Off                              | --                 |
|                                                | Problem                     | Off            | --                | Off            | --                 | Off                              | --                 |
| 1 to 24 <sup>#2</sup><br>1 to 48 <sup>#2</sup> | Link established            | Green          | Regular           | Green          | Reduced brightness | Off                              | --                 |
|                                                | Sending and receiving       | Blinking green | Regular           | Blinking green | Reduced brightness | Off                              | --                 |

| LED type | Device status | LED behavior setting configured by the system port-led configuration command |                   |                                   |                   |               |                   |
|----------|---------------|------------------------------------------------------------------------------|-------------------|-----------------------------------|-------------------|---------------|-------------------|
|          |               | Normal brightness (enable)                                                   |                   | Power saving brightness (economy) |                   | Off (disable) |                   |
|          |               | LED status                                                                   | Brightness status | LED status                        | Brightness status | LED status    | Brightness status |
|          | Failed        | Off                                                                          | --                | Off                               | --                | Off           | --                |

#1

Gigabitethernet or SFP ports

#2

Fastethernet ports

## (2) Trigger for LED automatic operation

By using the `system port-led trigger` configuration command to set the trigger for automatic operation shown in *Table 11-4 Trigger for automatic operation and the resulting behavior*, you can make LED behavior automatically changed. Execute the `system port-led` configuration command with normal brightness (enable) specified.

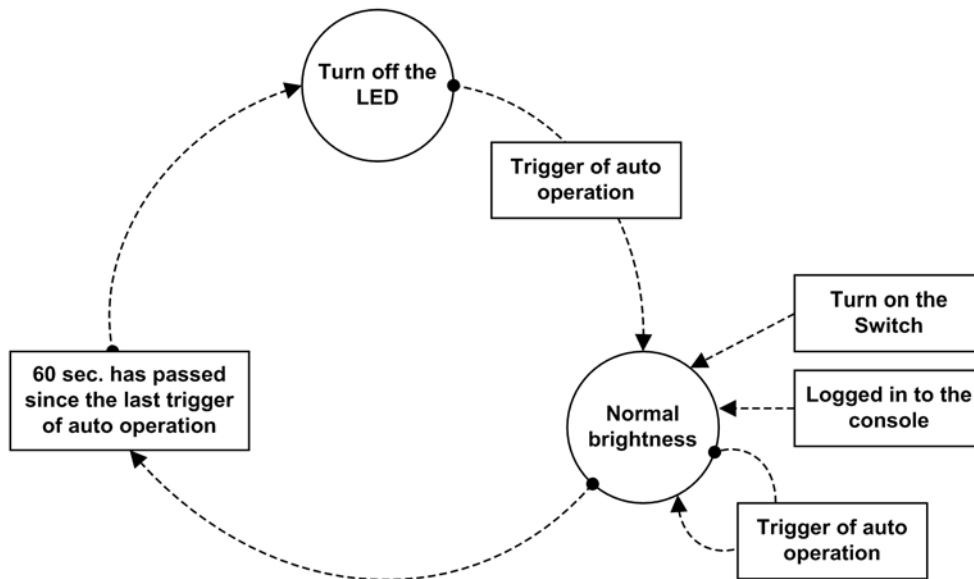
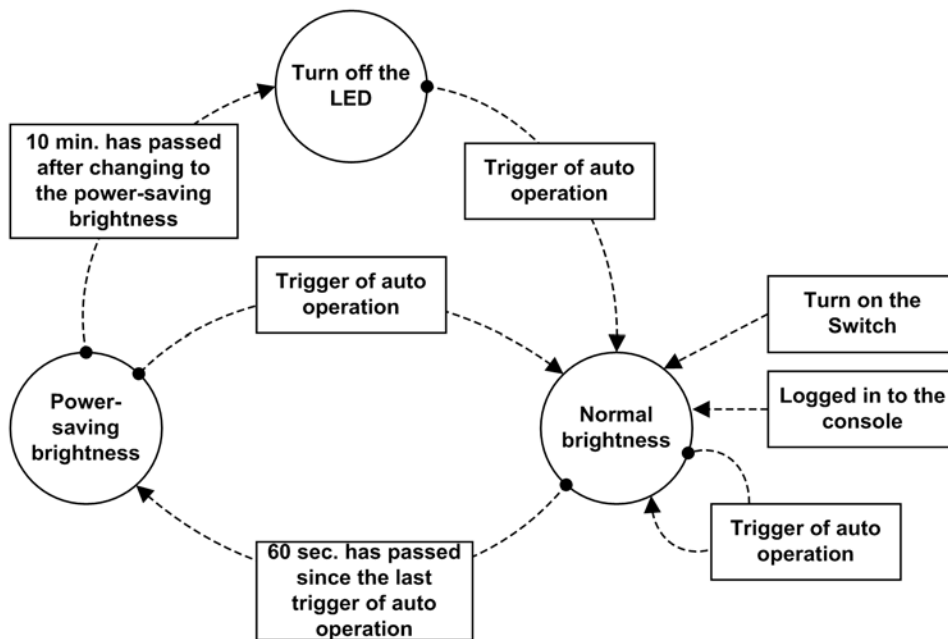
The table below describes the trigger for automatic operation and the resulting behavior.

**Table 11-4** Trigger for automatic operation and the resulting behavior

| Trigger for automatic operation | Behavior                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Console (RS232C)                | Triggered by login to the Switch via a console connection, LEDs turn on with normal brightness.<br>While a user is logging in from the console, the Switch stops timer control and LEDs continue turning on with normal brightness.<br>After the user logs out, LEDs change to power saving brightness or Off based on the timer control. |
| MC                              | Triggered by insertion or removing of a memory card, LEDs turn on with normal brightness.<br>LEDs change to power saving brightness or Off based on the timer control.                                                                                                                                                                    |
| Physical ports                  | Triggered by link-up or link-down of the specified physical port, LEDs turn on with normal brightness.<br>LEDs change to power saving brightness or Off based on the timer control.                                                                                                                                                       |

You can set multiple triggers for automatic operation.

The following figures show the transitions of automatic LED operation.

**Figure 11-1** Transitions of automatic LED operation [AX2200S]**Figure 11-2** Transitions of automatic LED operation [AX1250S] [AX1240S]

The trigger for automatic operation depends on *Table 11-4 Trigger for automatic operation and the resulting behavior*. Transition conditions include trigger for automatic operation and timer control.

1. Conditions for transition to normal brightness

Transition to normal brightness occurs according to any of the triggers shown in *Table 11-4 Trigger for automatic operation and the resulting behavior*.

2. Conditions for transition to power saving brightness [AX1250S] [AX1240S]

Timer control is used for transition from normal brightness to power saving brightness. LEDs transition to power saving brightness 60 seconds after the last trigger for automatic operation.

This is performed even when triggers for automatic operation of transition to normal brightness continuously occur.

## 11 Power Saving Functionality

### 3. Conditions for transition to Off

Timer control is used for transition to Off. LEDs transition to Off 60 seconds after the last transition to normal brightness. [AX2200S]

Timer control is used for transition to Off. LEDs transition to Off 10 seconds after the last transition to power saving brightness. [AX1250S] [AX1240S]

LEDs do not transition from normal brightness to Off.

The following table lists and describes the behavior of LEDs subject to the control of automatic operation. The PWR LED is not subject to the control. The PWR LED always illuminates with normal brightness.

**Table 11-5** LEDs subject to the control of automatic operation and the scope of behavior [AX2200S]

| LED type                | LED behavior type and the scope of automatic operation |     | Behavior                                                               |
|-------------------------|--------------------------------------------------------|-----|------------------------------------------------------------------------|
|                         | Normal brightness                                      | Off |                                                                        |
| ST1                     | Y                                                      | --  | Always turns on with normal brightness.                                |
| ACC                     |                                                        |     |                                                                        |
| LINK/ T/R <sup>#1</sup> |                                                        | Y   | Turned-on status changes depending on the two step brightness control. |
| 1 to 24 <sup>#2</sup>   |                                                        |     |                                                                        |

Legend:

Y: Subject to control

--: Not subject to control

#1

LEDs for SFP ports

#2

LEDs for Gigabitethernet ports

**Table 11-6** LEDs subject to the control of automatic operation and the scope of behavior [AX1250S] [AX1240S]

| LED type                                       | LED behavior type and the scope of automatic operation |                         |     | Behavior                                                                               |
|------------------------------------------------|--------------------------------------------------------|-------------------------|-----|----------------------------------------------------------------------------------------|
|                                                | Normal brightness                                      | Power saving brightness | Off |                                                                                        |
| ST1                                            | Y                                                      | Y                       | --  | Turns on with power saving brightness in the states of power saving brightness or Off. |
| ACC                                            |                                                        |                         |     |                                                                                        |
| LINK <sup>#1</sup>                             |                                                        |                         | Y   | Turned-on status changes depending on the three step brightness control.               |
| T/R <sup>#1</sup>                              |                                                        |                         |     |                                                                                        |
| 1 to 24 <sup>#2</sup><br>1 to 48 <sup>#2</sup> |                                                        |                         |     |                                                                                        |

Legend:

Y: Subject to the control

--: Not subject to the control

#1

LEDs for Gigabitethernet or SFP ports

#2

LEDs for Fastethernet ports

### 11.1.3 Port power saving

When Ethernet ports are inactive, this functionality lowers the power on the ports and reduces the power consumption

Port power saving does the following:

- Power saving for ports in the link-down status (Fastethernet and Gigabitethernet ports)
- Extended power saving for Gigabitethernet ports (Gigabitethernet ports) [AX1250S] [AX1240S]
- Blocking ports (Fastethernet, Gigabitethernet and SFP ports)

#### (1) Power saving for ports in the link-down status

This functionality limits the power supplied to ports until an electrical signal is detected, allowing you to reduce power consumed by ports in link-down status due to LAN cable disconnection or remote devices being powered off. Although use of this functionality reduces power consumed by ports in link-down status, more time is required to place these ports in link-up status.

To use link-down port power saving, 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.

Moreover, only Fastethernet and Gigabitethernet ports can be configured for power saving during link-down status. Link-down port power saving is not applied to SFP ports.

The following table lists and describes the conditions for power saving operation on the link-down ports.

**Table 11-7** Conditions for power saving operation on the link-down ports

| Configuration settings             | shutdown <sup>#</sup>             |                  | no shutdown                       |                 |
|------------------------------------|-----------------------------------|------------------|-----------------------------------|-----------------|
|                                    | Detection of an electrical signal |                  | Detection of an electrical signal |                 |
|                                    | None                              | Yes              | None                              | Yes             |
| power-control port cool-standby    | Y<br>(Link down)                  | Y<br>(Link down) | Y<br>(Link down)                  | --<br>(Link up) |
| no power-control port cool-standby | Y<br>(Link down)                  | Y<br>(Link down) | --<br>(Link down)                 | --<br>(Link up) |

Legend:

Y: Link-down port power saving is enabled, and the Switch operates in power saving manner.

--: Link-down port power saving is disabled, and the Switch operates with normal power consumption.

#

When the [shutdown](#) configuration command is set, or when [Set](#) of [ifAdminStatus](#) is executed by the [SetRequest](#) operation of SNMP from the SNMP manager

**(2) Extended power saving for Gigabitethernet ports [AX1250S] [AX1240S]**

Extended power saving is enabled when **shutdown** is set for both Gigabitethernet ports on the Switch regardless of the **power-control port cool-standby** configuration command setting. Extended power saving reduces power consumption more than the setting by the **power-control port cool-standby** configuration command.

Moreover, only Gigabitethernet ports can be configured for extended power saving. Extended power saving is not applied to SFP ports.

**Table 11-8** Gigabitethernet port extended power saving operation

| Setting of Gigabitethernet port 0/25 <sup>#</sup> | Setting of Gigabitethernet port 0/26 <sup>#</sup> |             |
|---------------------------------------------------|---------------------------------------------------|-------------|
|                                                   | shutdown                                          | no shutdown |
| shutdown                                          | Y                                                 | --          |
| no shutdown                                       | --                                                | --          |

Legend:

Y: Gigabitethernet port extended power saving is enabled, and the Switch operates in power saving manner.

--: Gigabitethernet port extended power saving is disabled, and the Switch operates with normal power consumption.

#

For AX1240S-48T2C, extended power saving is applied to ports 0/49 and 0/50.

**(3) Port blocked**

By shutting down ports by using the **shutdown** configuration command, power supplies to unused ports or unintended PoE power-receiving devices are stopped for power saving.

This can reduce the power consumption on ports together with (1) *Power saving for ports in the link-down status* and (2) *Extended power saving for Gigabitethernet ports [AX1250S] [AX1240S]* described above.

**11.1.4 Sleep mode [AX1250S] [AX1240S]**

The Switch is placed to sleep mode by the scheduling of the power-saving functionality. For details about scheduling, see *11.1.6 Power saving scheduling*.

In sleep mode, the power of the Switch is automatically turned off during the scheduled periods. It is automatically turned back on at the times specified to start the Switch. The PWR LED blinks green at long intervals during sleep mode. The Switch stops all functionality including switching (frame forwarding) and remote access.

To release the Switch from sleep mode, the administrator can intentionally start the Switch (forcible cancellation of sleep mode). Also, the Switch starts itself when it is released from sleep mode after the scheduled time expires.

**(1) Forcible cancellation of sleep mode**

While the Switch is in sleep mode, hold down the **RESET** button on the front of the Switch for at least three seconds until all LEDs on the front of the Switch turn on. The sleep mode will be canceled and the Switch will start in schedule-disabled mode.

### 11.1.5 Cooling fan control (Semi-fanless operation) [AX1240S]

Semi-fanless operation stops the 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. It also turns on the fans to start forced cooling (semi-fanless operation) when the ambient temperature is too high. 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 47 degrees Celsius or higher is detected
- Stop conditions: When an internal temperature of 46 degrees Celsius or lower continues for 10 minutes after detection

This functionality is supported by the AX1240S-48T2C 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.

If semi-fanless operation and the operation mode of the fan that supports a long life solution (`system fan mode`) are set at the same time, the latter takes precedence.

The following table describes the operating status of fans when semi-fanless operation and the operation mode of the fan are set at the same time.

**Table 11-9** Operating status of fans when semi-fanless operation and the operation mode of the fan are set at the same time

| Setting of semi-fanless operation<br>( <code>system fan-control</code> ) | Setting of the operation mode of the fan<br>( <code>system fan mode</code> ) | Fan operating status   | Remarks                                                                                     |
|--------------------------------------------------------------------------|------------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------|
| Yes                                                                      | system fan mode 2                                                            | Always operating       | Same setting as the low-temperature setting ( <code>system fan-control</code> is disabled.) |
|                                                                          | system fan mode 1 or no setting                                              | Semi-fanless operation |                                                                                             |
| No                                                                       | system fan mode 2                                                            | Always operating       | Same setting as the low-temperature setting                                                 |
|                                                                          | system fan mode 1 or no setting                                              | Always operating       |                                                                                             |

### 11.1.6 Power saving scheduling

You can schedule the power saving functionality to run for a specific period of time. For a schedule, specify a combination of power saving functionalities and the period of time during which they are to be run. When the specified start time arrives, power control is initiated automatically. Once you have scheduled the power saving functionality, you can also disable it for a particular period. A set period when power control is enabled is referred to as a scheduled time range and a time when power control is not enabled is referred to as a normal time range.



**(1) Specifiable power saving functionality**

To set up power saving functions, specify the function and the period when it is to apply. The power saving functions available for user-defined power saving are listed below. To schedule power saving, select one or more of the functionalities according to your requirements to determine the combination of functionalities to be run at the same time.

A Switch only allows one combination of functions to be specified for scheduling.

- LED behavior
- Port power saving
- Sleep mode [AX1250S] [AX1240S]

**(a) LED behavior based on scheduling**

This function changes LED behavior during a scheduled time range according to the specified schedule.

You can set LED behavior for a normal time range and a scheduled time range separately. The trigger for automatic LED operation is set commonly to a normal time range and a scheduled time range.

**Table 11-10** LED behavior setting for a scheduled time range and the resulting behavior

| LED behavior setting for a scheduled time range | Configuration common to a normal time range and a scheduled time range |                                                |
|-------------------------------------------------|------------------------------------------------------------------------|------------------------------------------------|
|                                                 | Trigger for automatic LED operation is set                             | Trigger for automatic LED operation is not set |
| No command specified                            | Automatic operation                                                    | Normal brightness                              |
| Normal brightness                               | Automatic operation                                                    | Normal brightness                              |
| Power saving brightness                         | Power saving brightness                                                | Power saving brightness                        |
| Off                                             | Off                                                                    | Off                                            |

**(b) Port power saving based on scheduling**

This function operates according to a specified schedule, performing port power saving during a scheduled time range.

**(c) Sleep mode [AX1250S] [AX1240S]**

This function operates according to a specified schedule, by putting the Switch in sleep mode when a scheduled time range begins, and by cancelling the sleep mode and starting the Switch when a normal time range begins. The Switch can be scheduled to be in operation or in sleep mode (for example, on Sundays, Saturdays, long weekends, national holidays, or nights).

### (2) Start mode for the scheduling functionality

You can use the `set power-control schedule` operation command to select either of the following two modes as the start mode for the scheduling functionality:

- Schedule-enabled mode

In this mode, both settings for a normal time range and a scheduled time range are applied. The setting for a scheduled time range is applied when the operating time is in the scheduled time range. The setting for a normal time range is applied when the operating time is outside the scheduled time range.

When the Switch starts due to expiration of the scheduled time, the Switch operates in schedule-enabled mode.

- Schedule-disabled mode

In this mode, only the setting for a normal time range is applied. The setting for a normal time range is applied even when the operating time is within the scheduled time range.

When sleep mode is forcibly cancelled after you held down the RESET button on the Switch, the Switch operates in schedule-disabled mode.

However, schedule-disabled mode automatically changes to schedule-enabled mode when the operating time enters the normal time range.

### (3) Scheduling power control

Set the period when the switch is to operate in power control mode. Specify the start time and end time in any of the following ways:

- Enabling power control by date and time
- Enabling power control by day of the week and time
- Enabling power control by daily time range
- Disabling power control by specific date and time

You can use these methods in combination to enable or disable power control at various times.

You can use the `schedule-power-control time-range` configuration command to set a maximum of 50 schedule time ranges.

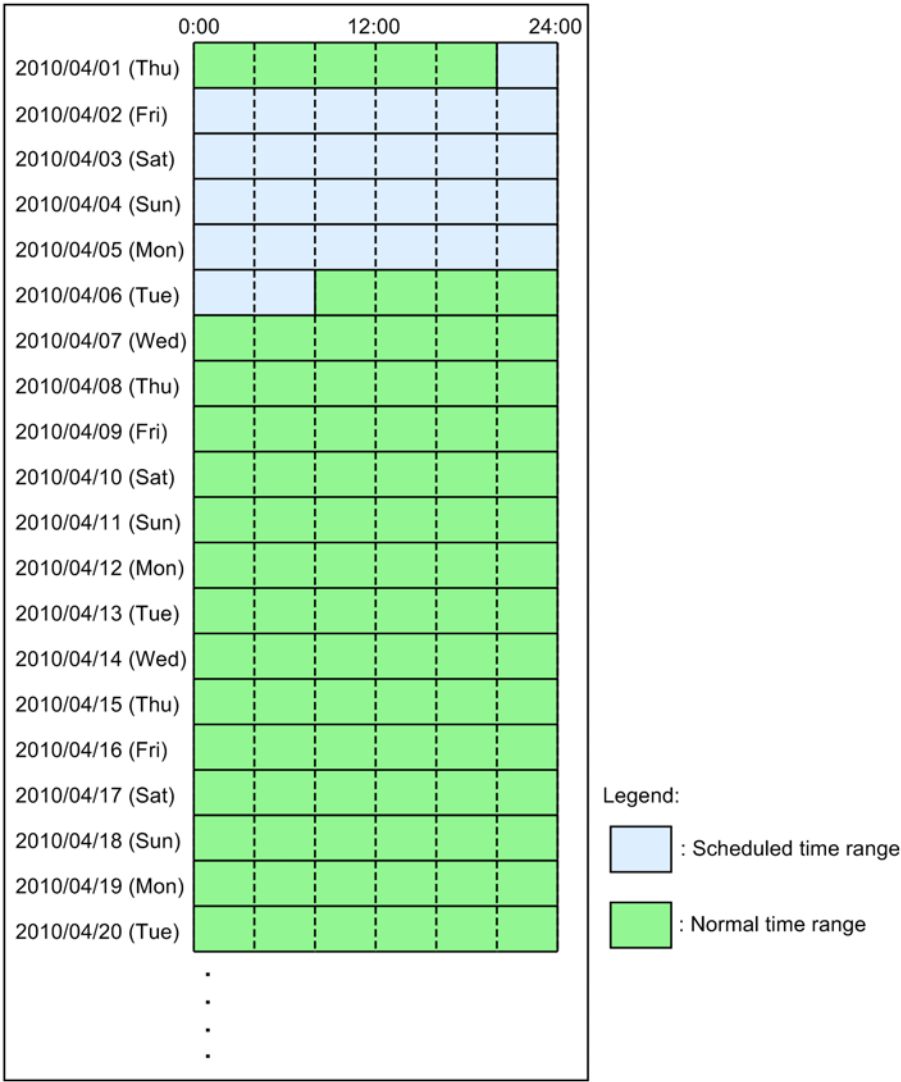
(a) Enabling power control by date and time

Specify the start and end dates and times for implementing power control.

Example:

From April 2 to April 5, 2009, the business system will have a reduced workload. In line with this expectation, schedule power control from 20:00 on April 1 to 8:00 on April 6, 2009. The following figure shows the operation schedule.

Figure 11-3 Power control schedule (by date)



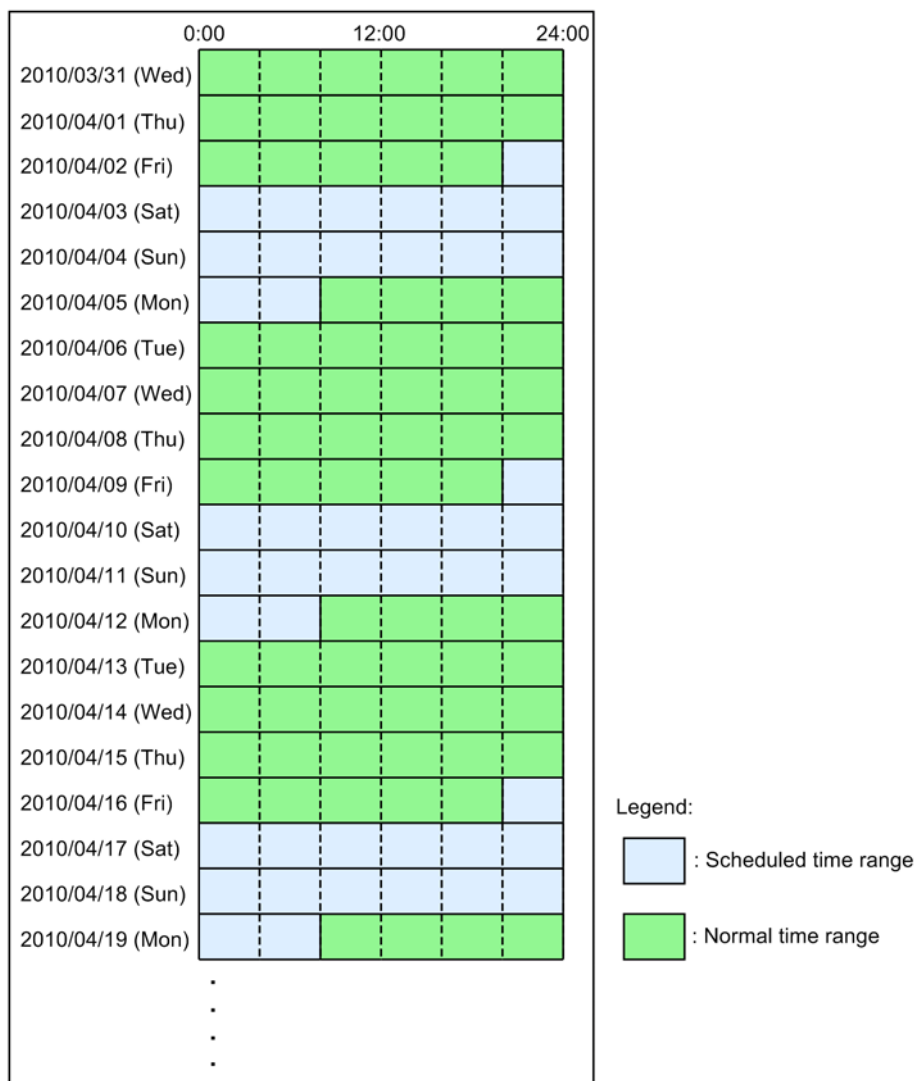
**(b) Enabling power control by day of the week and time**

Specify the start and end days of the week and times for implementing power control.

Example:

The office is closed every Saturday and Sunday, and the business system has a reduced workload on these two days. Therefore, schedule power control from 20:00 every Friday to 8:00 every Monday. The following figure shows the operation schedule.

**Figure 11-4** Power control schedule (by day of the week)



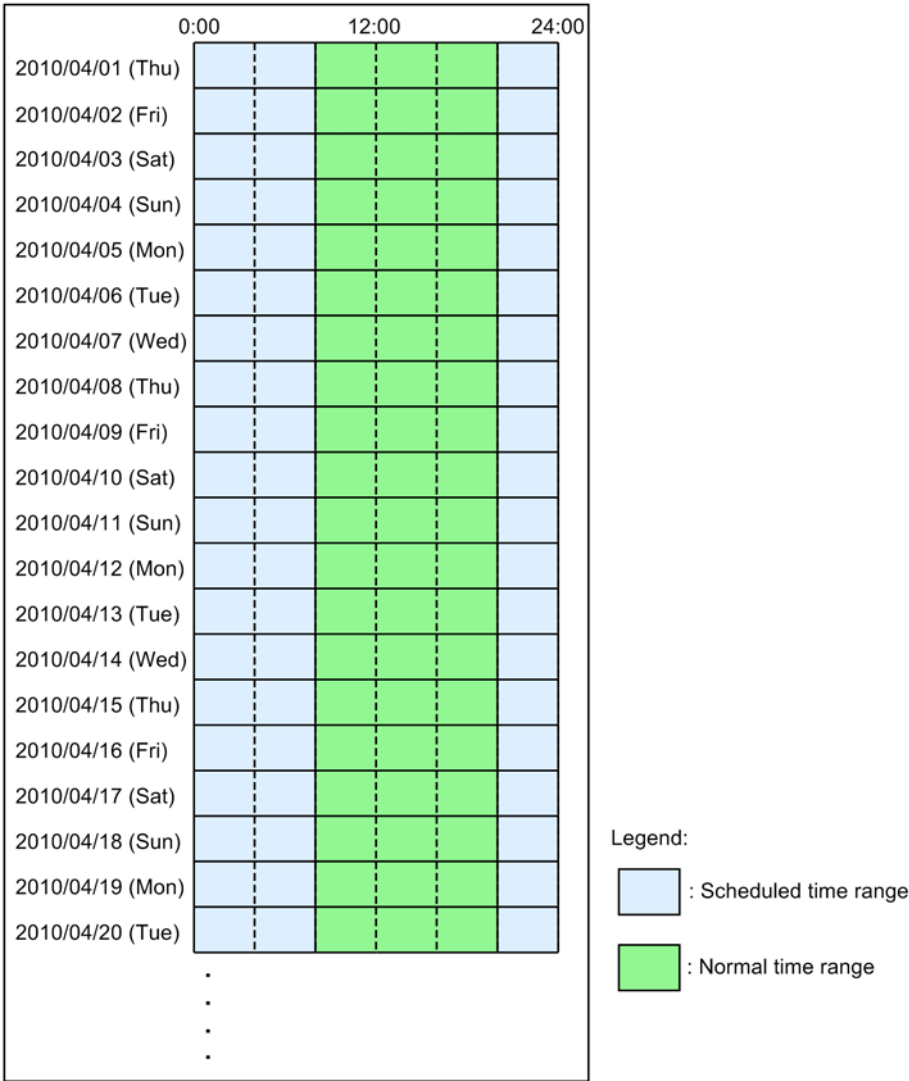
(c) Enabling power control by daily time range

Specify the start time and end time for implementing power control.

Example:

Normal office hours are from 8:30 to 17:00 every day, so the business system needs to operate at normal power from 8:00 to 20:00. Schedule power control from 20:00 every day to 8:00 the following day. The following figure shows the operation schedule.

Figure 11-5 Power control schedule (daily)



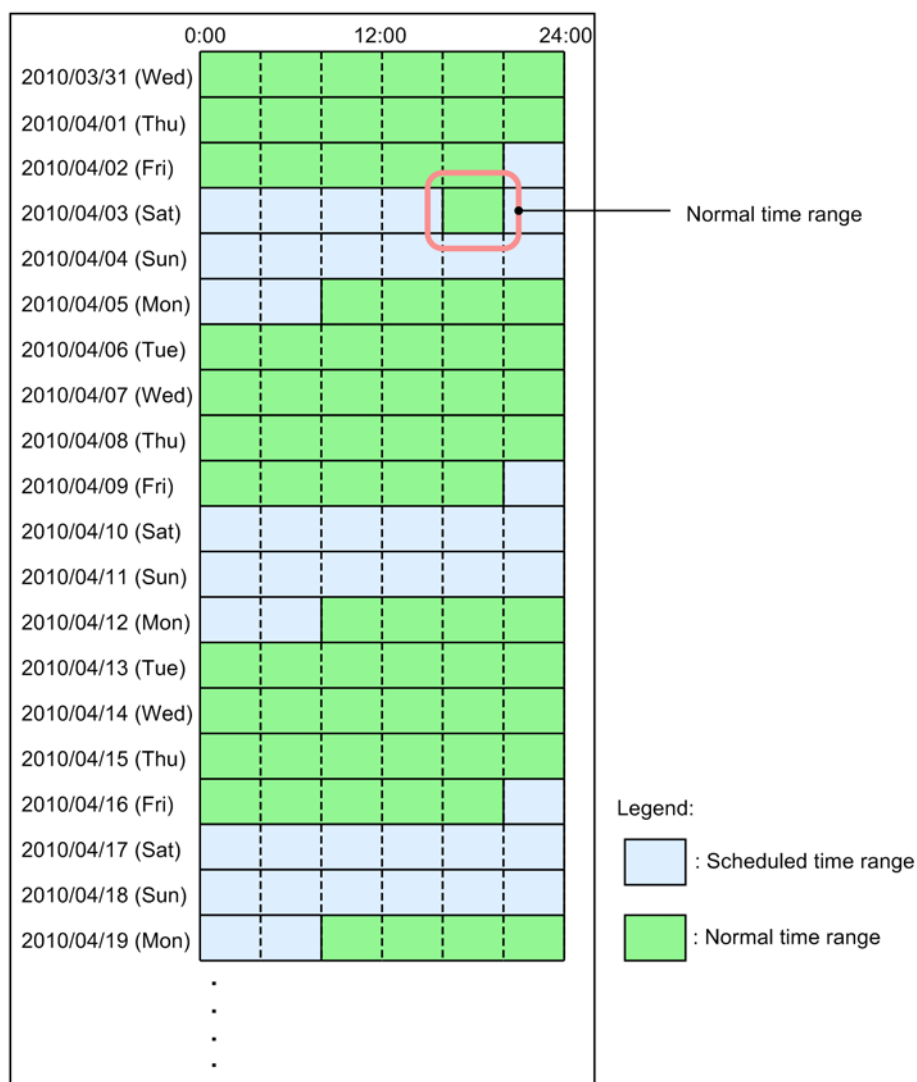
**(d) Disabling power control by specific date and time**

You can disable power control for a specified time during a scheduled time range. Specify the start and end times for disabling the functionality. You can specify particular dates or days of the week, or certain times every day.

Example:

The office is closed every Saturday and Sunday, and power control is scheduled from 20:00 every Friday to 8:00 every Monday. However, the business system needs to run at normal power to perform batch processing from 16:00 to 20:00 on 04.04.09. The following figure shows the operation schedule.

**Figure 11-6** Power control schedule (disable)



### 11.1.7 Notes when the power saving functionality is used

#### (1) When port power saving is used [AX1250S] [AX1240S]

Port power saving takes from 3 to 5 seconds to place ports in the link-up status.

#### (2) Scheduling power control

To use the same power saving functionality during a normal time range and a scheduled time range, perform the setting for both periods.

Example:

Suppose you use the `shutdown` configuration command to block a particular port during a normal time range. To also block a particular port during a scheduled time range, use the `schedule-power-control shutdown interface` configuration command.

#### (3) Time lag in starting and ending power control

Because scheduling uses a software timer, a situation such as a high CPU load might cause a time lag before the set start or end of a scheduled time range takes effect. This time lag is less than one minute. Also, depending on the network configuration, there could be a time lag before communication with the port resumes at the end of a scheduled time range in which the port has been blocked. Allow a certain margin when you schedule power control.

#### (4) When running sleep mode [AX1250S] [AX1240S]

If you are running sleep mode using the scheduling functionality, note the following:

1. The Switch does not switch to the sleep state if the scheduled time of execution arrives 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 period during software update or restoration, the Switch does not go into sleep mode. The Switch goes into sleep mode after the software update or restoration finishes.
3. A configuration that is not saved is lost if the Switch switches to the sleep state. As a result, the following messages appear when configuration command mode ends:  
  
 Unsaved changes would be lost when the machine goes to sleep!  
  
 Do you exit "configure" without save ? (y/n):  
  
 Press `n` to execute the save command.
4. If no key input operations are performed for certain period of time (30 minutes by default), you are automatically logged out. If you are automatically logged out while editing the configuration and the Switch switches to the sleep state, an unsaved configuration will be lost.
5. If the sleep state continues for 20 days, the sleep state is canceled and the Switch is started.  
  
 Then, it goes into sleep mode again after startup.
6. After the sleep period ends, communication will not resume immediately because the Switch requires the usual amount of time to start up. Leave a margin to the scheduled time range and the normal time range.

7. If sleep mode is set, the Switch switches to the sleep state when the scheduled execution time arrives. As a result, the following command settings are not applied:
  - `schedule-power-control port-led`
  - `schedule-power-control port cool-standby`
  - `schedule-power-control shutdown interface`

### **(5) Interoperability of sleep mode and DHCP snooping [AX1250S] [AX1240S]**

If both sleep mode and DHCP snooping are enabled, set the time the Switch stays in sleep mode to longer than the lease time for IP addresses assigned by the DHCP server. If the time the Switch stays in sleep mode is shorter than the lease time, the DHCP client might not be able to communicate with the Switch because the binding database cannot be restored when the Switch is released from sleep mode.

If this occurs, release and update the IP addresses on the DHCP clients. In Windows, for example, in the Command Prompt window, execute `ipconfig /release` and then execute `ipconfig /renew`. This re-registers terminal information in the binding database and enables communication by DHCP clients.



## 11.2 Power control configuration

### 11.2.1 List of configuration commands

The following table describes the configuration commands for implementing power control.

**Table 11-11** List of configuration commands

| Command name                                   |                                                            | Description                                                                                                        |
|------------------------------------------------|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| For setting a normal time range                | For setting a scheduled time range                         |                                                                                                                    |
| system port-led                                | schedule-power-control port-led                            | Configures a Switch's LED operation.                                                                               |
| system port-led trigger interface <sup>#</sup> |                                                            | Adds link-up and link-down of the specified physical port a trigger for automatic LED operation.                   |
| system port-led trigger console <sup>#</sup>   |                                                            | Adds login to and logout from a Switch via a console (RS232C) connection as a trigger for automatic LED operation. |
| system port-led trigger mc <sup>#</sup>        |                                                            | Adds insertion and removal of a memory card as a trigger for automatic LED operation.                              |
| power-control port cool-standby                | schedule-power-control port cool-standby                   | Enables power saving for ports in the link-down status                                                             |
| system fan-control <sup>#</sup><br>[AX1240S]   |                                                            | Enables cooling fan control (Semi-fanless operation)                                                               |
| shutdown                                       | schedule-power-control shutdown interface                  | Sets the port blocking operation.                                                                                  |
| n/a                                            | schedule-power-control system-sleep<br>[AX1250S] [AX1240S] | Sets sleep mode.                                                                                                   |
| n/a                                            | schedule-power-control time-range                          | Sets the power control scheduled time range.                                                                       |

Legend:

n/a: Not applicable

#

The setting is common to the normal time range and the scheduled time range.

### 11.2.2 LED behavior setting

#### (1) LED behavior setting

Points to note

In this setting, you set a Switch's LED behavior to power saving brightness.

Command examples

1. `(config)# system port-led economy`

Sets the Switch's LED behavior to power saving brightness.

Notes

Power saving brightness is not supported by AX2200S. Set normal brightness or Off instead.

#### (2) Setting a trigger for LED automatic operation

You can make LED behavior automatically change, adding a trigger for automatic operation to the LED setting.

Points to note

In this setting, you set the console port and physical ports (link-up or link-down), and a memory card (insert or remove) as triggers for automatic LED operation on the Switch.

Command examples

1. `(config)# system port-led enable`

Sets the LED behavior to normal brightness.

2. `(config)# system port-led trigger console`

`(config)# system port-led trigger interface 0/1,0/20`

`(config)# system port-led trigger mc`

Sets the console port and ports 0/1 and 0/20 (link-up or link-down), and a memory card (insert or remove).

### 11.2.3 Setting power saving for ports in link-down status

Points to note

In this setting, you set the power saving for ports in the link-down status.

Command examples

1. `(config)# power-control port cool-standby`

Sets power saving for link-down for all ports.

### 11.2.4 Setting cooling fan control (Semi-fanless operation) [AX1240S]

Points to note

This setting lets you configure operation so that the fans stop when internal temperature monitoring determines that forcible cooling is unnecessary.

Command examples

1. `(config)# system fan-control`

Configures the setting so that the fans stop at a temperature where forcible cooling is unnecessary.

### 11.2.5 Setting power saving based on scheduling

This functionality operates under the power saving settings for sleep mode or for operations other than sleep mode.

- Sleep mode (such as the year-end and New Year holidays, and other long holidays) [AX1250S] [AX1240S]
- Power saving settings for LED behavior and link-down ports where sleep mode is not enabled

#### (1) Sleep mode setting for the year-end and New Year holidays [AX1250S] [AX1240S]

Points to note

You can set the Switch to go to sleep mode during the year-end and New Year holidays.

Command examples

1. `(config)# schedule-power-control system-sleep`  
Sets power saving for a scheduled time range. This example sets sleep mode for the Switch.
2. `(config)# schedule-power-control time-range 1 date start-time 091228 2300 end-time 100104 0600 action enable`  
Sets a power control schedule that runs from 23:00 on December 28, 2009 to 6:00 on January 4, 2010.
3. `(config)# schedule-power-control time-range 2 date start-time 101228 2300 end-time 110104 0600 action enable`  
Sets a power control schedule that runs from 23:00 on December 28, 2010 to 6:00 on January 4, 2011.
4. `(config)# schedule-power-control time-range 3 date start-time 111228 2300 end-time 120104 0600 action enable`  
Sets a power control schedule that runs from 23:00 on December 28, 2011 to 6:00 on January 4, 2012.
5. `(config)# end`  
Unsaved changes would be lost when the machine goes to sleep!  
Do you exit "configure" without save ? (y/n):  
The above message appears when you exit the command mode because sleep mode has been set to the scheduled object.
6. `Do you exit "configure" without save ? (y/n): n`  
`(config)# save`  
Press `n` to execute the save command.

Notes

See (4) *When running sleep mode [AX1250S] [AX1240S] in 11.1.7 Notes when the power saving functionality is used.*

**(2) Setting power saving for LED behavior and link-down ports during scheduled time range**

## Points to note

You can set LED behavior to Off, power saving for link-down ports, and blocking of unused ports.

The following table describes the operating status before the configuration is set (normal time range) and after the configuration is set (scheduled time range).

**Table 11-12** Configuration setting example

| Item                                           | Normal time range                           | Scheduled time range                                       |
|------------------------------------------------|---------------------------------------------|------------------------------------------------------------|
| LED behavior                                   | Normal brightness                           | Off                                                        |
| Power saving for ports in the link-down status | Normal operation is applied to all ports.   | Link-down ports operate in power saving mode.              |
| Port blocked                                   | All ports are in <b>no shutdown</b> status. | Unused ports 0/21 to 0/24 are blocked ( <b>shutdown</b> ). |

## Command examples

- ```
(config)# schedule-power-control port-led disable
(config)# schedule-power-control port cool-standby
(config)# schedule-power-control shutdown interface 0/21-24
```

Sets the power saving functionality for a scheduled time range. This example sets LED behavior to Off, power saving for link-down ports, and blocking of ports.
- ```
(config)# schedule-power-control time-range 1 weekly start-time fri 2000 end-time mon 0800 action enable
```

Sets a power control schedule that runs from 20:00 every Friday to 8:00 every Monday.
- ```
(config)# schedule-power-control time-range 2 date start-time 090404 1600 end-time 090404 2000 action disable
```

Disables the power control schedule for the period from 16:00 to 20:00 on April 4, 2009.

Notes

- You can set more than one scheduled time. During the scheduled time range, all operations for the scheduled targets set by the **schedule power-control** configuration command are executed. The targets to be scheduled cannot be set separately for each execution time.
- If there is an overlap of time of execution between different **action** parameters, the **action disable** setting has precedence.

11.3 Power control operation

11.3.1 List of operation commands

The following table describes the operation commands for implementing power control.

Table 11-13 List of operation commands

Command name	Description
show power-control port	Display the status of port power saving control.
show power-control schedule	Displays the operating status of the scheduling functionality.
set power-control schedule	Changes the start mode of the scheduling functionality.

11.3.2 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 [10.1.3 Checking the switch status](#).

11.3.3 Displaying the status of port power saving control

You can check the status of port power saving control by using the [show power-control port](#) operation command.

Figure 11-7 Execution result of the show power-control port command

```
> show power-control port

Date 2009/03/24 22:55:17 UTC
Port  status  cool-standby
0/1   up      -
0/2   down    applied
0/3   up      -
0/4   up      -
0/5   up      -
0/6   up      -
0/7   up      -
0/8   up      -
0/9   down    applied
0/10  down    applied
      :
      :
```

11.3.4 Displaying the status of cooling fan control [AX1240S]

You can check the settings of cooling fan control by using the [show system](#) operation command and viewing [Fan](#). For details, see [10.1.3 Checking the switch status](#).

11.3.5 Displaying the operating status of the schedule

Display the current status of the power saving schedule and the dates and times the power saving schedule has been enabled by using the `show power-control schedule` operation command.

Figure 11-8 Execution result of the show power-control schedule command

```
> show power-control schedule

Date 2009/05/01(Fri) 18:36:57 UTC
Current Schedule Status : Disable
Schedule Power Control Date :
  2009/05/01(Fri) 20:00 UTC - 2009/05/04(Mon) 06:00 UTC
  2009/05/04(Mon) 20:00 UTC - 2009/05/05(Tue) 06:00 UTC
  2009/05/05(Tue) 20:00 UTC - 2009/05/06(Wed) 06:00 UTC
  2009/05/06(Wed) 20:00 UTC - 2009/05/07(Thu) 06:00 UTC
  2009/05/07(Thu) 20:00 UTC - 2009/05/08(Fri) 06:00 UTC
>
```

12. Software Management

This chapter describes how to update, back up, and restore the Switch's software. For further details, see the *Software Update Guide*.

12.1 List of operation commands

12.2 Software update

12.1 List of operation commands

The following table describes the operation commands related to software management.

Table 12-1 List of operation commands

Command name	Description
ppupdate	Updates the software to a newer version. The newer version can be copied from a memory card to the RAMDISK or downloaded via FTP or a similar method.

12.2 Software update

Software update means updating an older version of your software to a later version. To update the software, copy the update file from a memory card to the RAMDISK on the Switch and execute the `ppupdate` operation command, or transfer the update file from a remote operation terminal, such as a PC, to the Switch and execute the `ppupdate` operation command. During the update process, the switch management configuration and user information (such as login accounts and passwords) remain in effect. For details, see the *Software Update Guide*.

The following figure provides an overview of software update.

Figure 12-1 Overview of software update (from the memory card)

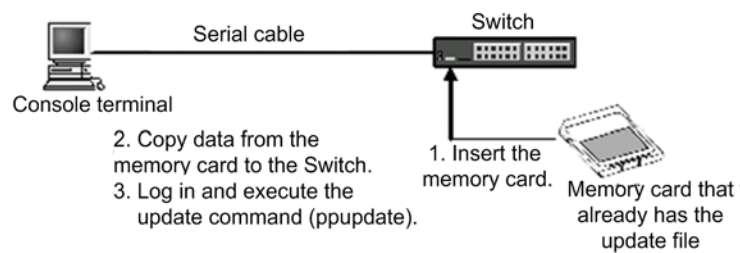
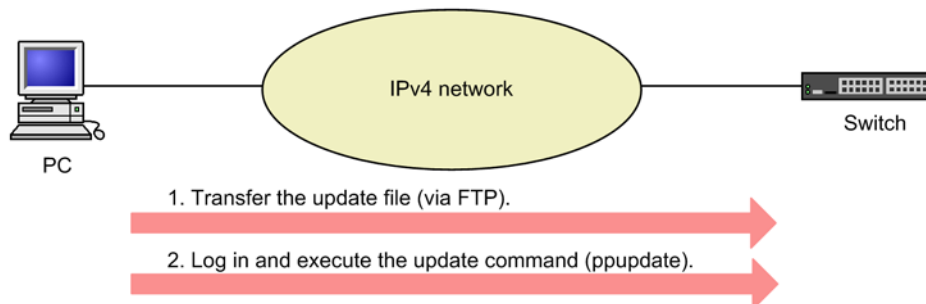


Figure 12-2 Overview of software update (via FTP)



12.2.1 Notes on updating the software

When the Switch is in sleep mode, first restart the Switch by forcing cancellation of sleep mode, and then update the software. [AX1250S] [AX1240S]

13. Ethernet

This chapter describes Ethernet as used with the Switch.

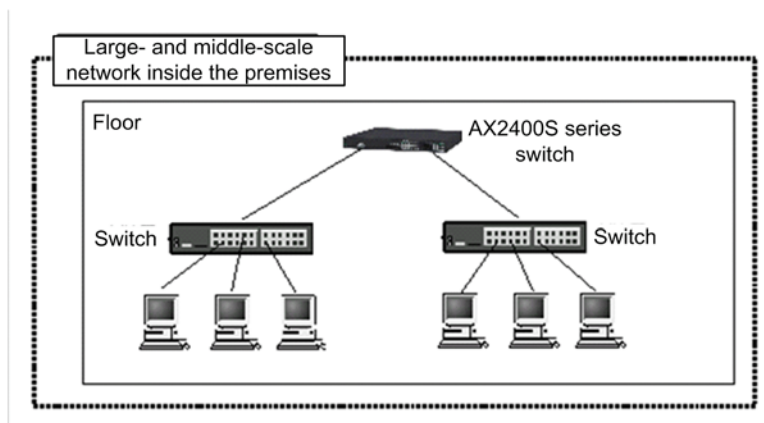
13.1	Information common to all Ethernet interfaces
13.2	Configuration common to all Ethernet interfaces
13.3	Operations common to all Ethernet interfaces
13.4	Description of Fastethernet [AX1250S] [AX1240S]
13.5	Configuration of Fastethernet [AX1250S] [AX1240S]
13.6	Description of Gigabitethernet (RJ45)
13.7	Configuration of Gigabitethernet (RJ45)
13.8	Description of Gigabitethernet (RJ45)
13.9	Configuration of Gigabitethernet (RJ45)
13.10	Description of PoE [AX2200S] [AX1240S]
13.11	Configuration of PoE [AX2200S] [AX1240S]
13.12	Operation of PoE [AX2200S] [AX1240S]

13.1 Information common to all Ethernet interfaces

13.1.1 Network configuration example

The figure below shows an example of a typical Ethernet configuration that uses Switches. The AX2200S series switches for gigabit Ethernet and AX1250S/AX1240S series switches for fast Ethernet serve as line concentrators which connect the terminals on the floor.

Figure 13-1 Ethernet configuration example



13.1.2 Physical interfaces

There are three types of Ethernet interfaces:

- Interface using a 10BASE-T or 100BASE-TX twisted pair cable (UTP) compliant with IEEE 802.3
- 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[#]

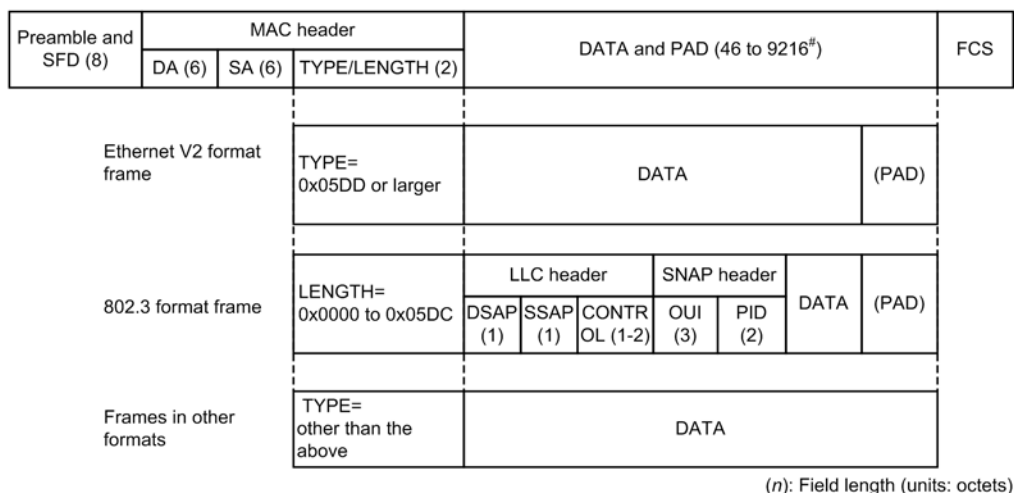
#

Includes IEEE 802.3ah.

13.1.3 Control on the MAC and LLC sublayers

The following figure shows frame formats.

Figure 13-2 Frame formats



[#]: The maximum length of the DATA and PAD field is 9216 only when the frame format is Ethernet V2. For 802.3 and other formats, the maximum length is 1500.

(1) MAC sublayer frame format

(a) Preamble and SFD field

The Preamble and SFD field contains a 64-bit binary number. The first 62 bits are repetitions of 10, and the last two bits are 11 (1010...1011). 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 16-bit or local address formats.

(c) TYPE/LENGTH field

The following table describes how the TYPE/LENGTH field is handled.

Table 13-1 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

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. The values to be padded are undefined.

13.1.4 MAC address of the Switch

(1) Switch MAC addresses

The Switch has one MAC address as a device identifier. This MAC address is called the *device MAC address*. The device MAC address is used as the device ID used for protocols, such as a Spanning Tree Protocol.

(2) Functionality that uses a device MAC address

The following table shows the types of functionality that use the device MAC address.

Table 13-2 Functionality that uses a device MAC address

Functionality	Purpose
VLAN	MAC addresses of VLAN interfaces
LACP for link aggregation	Device identifier
Spanning Tree Protocol	Device identifier
LLDP	Device identifier
IEEE 802.3ah/UDLD	Device identifier
Uplink redundancy (sending flush control frames)	Device identifier
L2 Loop Detection	Device identifier
CFM	Device identifier

13.1.5 Order of Ethernet frames

The Switch forwards some frames using software. Therefore, the order of the frames might be changed due to forwarding. Also, the order of the frames might be changed when priority control based on the CoS values[#] is applied.

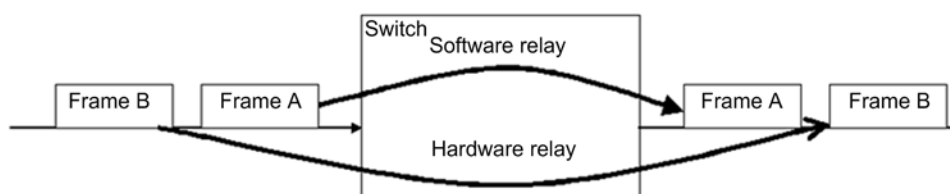
#

CoS values are used as an index for indicating the priority of frames in the Switch.

(1) Order change of the forwarded frames due to software forwarding

Some IGMP or MLD snooping frames, such as query frames, are subject to software forwarding on the Switch

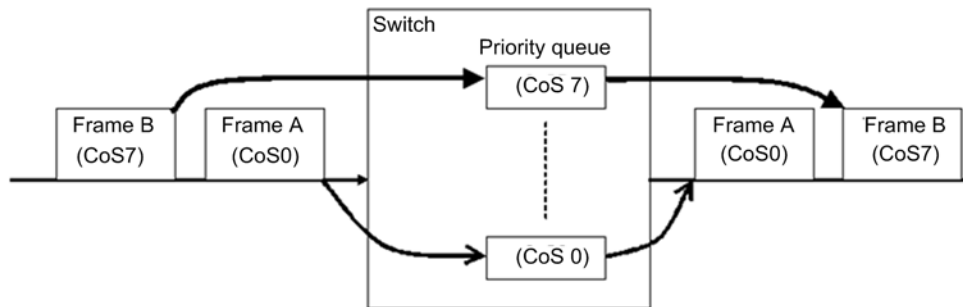
Figure 13-3 Order change of frames due to software forwarding



(2) Order change of frames due to priority control

Priority control based on CoS values is enabled by default on the Switch. Therefore, if received frames have different CoS values, the order of those frames might change.

Figure 13-4 Order change of frames due to priority control



13.2 Configuration common to all Ethernet interfaces

13.2.1 List of configuration commands

The following table describes the configuration commands common to all Ethernet interfaces.

Table 13-3 List of configuration commands

Command name	Description
bandwidth	Sets the port bandwidth.
description	Sets a supplementary description of the port.
duplex	Sets the duplex mode of a port.
flowcontrol	Sets the flow control for the port.
interface fastethernet [AX1250S] [AX1240S]	Sets the configuration of the Fastethernet port (10BASE-T or 100BASE-TX interface).
interface gigabitethernet	Sets the configuration of the Gigabitethernet port (10BASE-T/100BASE-TX/1000BASE-T, 100BASE-FX, or 1000BASE-X interface).
link debounce	Sets the link-down detection time after a link failure is detected for the port until the actual link-down occurs.
linkscan-mode	Sets the operating mode for monitoring the link status of a Switch.
mdix auto	Sets automatic MDIX for the port.
media-type [AX1250S] [AX1240S]	Selects a port with the media type to be used as a port that can be switched between an RJ45 Gigabitethernet port (10BASE-T, 100BASE-TX or 1000BASE-T interface) and an SFP port (100BASE-FX or 1000BASE-X interface).
mtu	Sets the MTU for ports.
shutdown	Shuts down the port.
speed	Sets the port speed.
system mtu	Sets the MTU common to all ports.

13.2.2 Setting Ethernet interface ports [AX2200S]

Points to note

To configure Ethernet, specify the interface port number, and then move to config-if mode to set up the information.

Command examples

1. `(config)# interface gigabitethernet 0/1`
`(config-if)# exit`

Specifies the setting for the Gigabitethernet port 0/1.

In the setting examples below, `interface fastethernet` is specified. For AX2200S series switches, however, use `interface gigabitethernet` instead.

13.2.3 Setting Ethernet interface ports [AX1250S] [AX1240S]

Points to note

To configure Ethernet, specify the interface port number, and then move to config-if mode to set up the information.

Command examples

1. `(config)# interface fastethernet 0/1`
`(config-if)# exit`
Specifies the setting for Fastethernet port 0/1.
2. `(config)# interface gigabitethernet 0/25`
`(config-if)# exit`

Specifies the setting for Gigabitethernet port 0/25.

13.2.4 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 fastethernet 0/1-10,0/15-20`
Specifies the settings for ports 0/1 to 0/10, and 0/15 to 0/20.
2. `(config-if-range)# *****`
`(config-if-range)# exit`

Performs the same configuration for all the ports.

13.2.5 Shutting down a port

Points to note

Configuring an Ethernet interface might require the execution of multiple commands. In such a case, if the port enters a link-up state before the configuration is complete, the Switch cannot communicate as expected. Therefore, we recommend that you shut down the port first, and then after the configuration is complete, exit the port from the shutdown state. Always make sure that ports that will not be used are shut down.

The following shows a configuration example for a FastEthernet port.

Command examples

1. `(config)# interface fastethernet 0/10`

Specifies the setting for port 0/10.

2. `(config-if)# shutdown`

Shuts down the port.

3. `(config-if)# *****`

Configures the port.

4. `(config-if)# no shutdown`

`(config-if)# exit`

Exits the port from the shutdown state.

Related information:

To stop operation of the port, you can use the operation command `inactivate`. If the `inactivate` operation command is used to set the port to an inactive state and then the Switch is restarted, the port enters an active state. However, if the port was shut down, its status remains disabled even after the switch is restarted. To change the status from disabled to active, you must release the port from the shutdown status by setting the `no shutdown` configuration command to the port.

13.2.6 Setting the link-down detection timer

If the wait time before a link-down is detected after the detection of a link fault is too short, depending on the remote device, the link might be unstable. You can avoid this problem by setting a link-down detection timer.

Points to note

Make sure that you set as small a link-down detection timer value as possible without risking the link becoming unstable. If the link is stable even when a link-down detection timer is not set, you do not need to set one.

The following shows a configuration example for a FastEthernet port.

Command examples

1. `(config)# interface fastethernet 0/10`

Specifies the setting for port 0/10.

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.

13.2.7 Flow control settings

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

Determine flow control settings that do not conflict with the settings on the remote device.

The following shows a configuration example for a Fastethernet port.

Command examples

1.

```
(config)# interface fastethernet 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
```

Notes

For 100BASE-FX, no flow control operation based on negotiation is performed because auto-negotiation is not used. Set **full** for **duplex** so that only full duplex setting is used.

13.2.8 Automatic MDIX functionality settings

Fastethernet and Gigabitethernet (RJ45) ports on the Switch support automatic MDIX. Therefore, these ports enable communication by automatically switching the MDI setting according to the cable type (straight or crossover) during auto-negotiation. If this functionality is disabled, MDI-X (for hub use) is always selected.

(1) Setting fixed MDI

Points to note

To configure MDI-X to always be used instead of automatic MDIX, disable automatic MDIX for the port.

The following shows a configuration example for a Fastethernet port.

Command examples

1. `(config)# interface fastethernet 0/24`
Specifies the setting for port 0/24.
2. `(config-if)# no mdix auto`
`(config-if)# exit`

Disables the automatic MDIX functionality so that MDI-X is always selected.

13.2.9 Using jumbo frames

The maximum transmission unit (MTU) in the Ethernet interface standard is 1500 octets. On the Switch, the MTU can be extended by using jumbo frames to increase the amount of data that is transmitted at one time, which improves throughput.

For a port to send or receive jumbo frames, an MTU must be set. When an MTU is set, the Switch can send or receive frames whose maximum size is the specified MTU plus the size of one VLAN tag.

Determine the port MTU value appropriate for the network and remote device.

(1) Setting MTU for a port

Points to note

If you set the MTU of port 0/10 to 8192 octets, jumbo frames without VLAN tags up to 8206 octets and jumbo frames with VLAN tags up to 8210 octets can be sent and received.

The following shows a configuration example for a Fastethernet port.

Command examples

1. `(config)# interface fastethernet 0/10`
`(config-if)# shutdown`
`(config-if)# mtu 8192`
Sets the MTU of port 0/10 to 8192 octets.
2. `(config-if)# no shutdown`
`(config-if)# exit`

Notes

Even if the MTU for each port is set by using a configuration command, the MTU is fixed at 1,500 octets when a 10BASE-T or 100BASE-TX half-duplex connection is used. This 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

If you set 4096 octets as the MTU for the all ports on a Switch, jumbo frames without VLAN tags up to 4110 octets and jumbo frames with VLAN tags up to 4114 octets can be sent and received.

Command examples

1. `(config)# system mtu 4096`

Sets 4096 octets as the MTU for the all ports on the Switch.

Notes

Even if the MTU for all ports is set by using a configuration command, the MTU is fixed at 1,500 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.

13.3 Operations common to all Ethernet interfaces

13.3.1 List of operation commands

The following table describes the operation commands common to Ethernet.

Table 13-4 List of operation commands

Command name	Description
show interfaces	Displays Ethernet information.
show port	Displays Ethernet information in list format.
clear counters	Clears the Ethernet statistics counters.
inactivate	Changes the status of an Ethernet port from <i>active</i> to <i>inactive</i> .
activate	Changes the status of an Ethernet port from <i>inactive</i> to <i>active</i> .

13.3.2 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 13-5 Example of the results of executing the command that displays the status of all Ethernet ports on the Switch

```
> show port
```

```
Date 2008/11/13 11:40:21 UTC
Port Counts: 26
Port  Name           Status Speed           Duplex    FCtl FrLen  ChGr/Status
0/1  fastether0/1        up    100BASE-TX      full(auto) off   1518  8/up
0/2  fastether0/2        up    100BASE-TX      full(auto) off   1518  8/up
0/3  fastether0/3        up    100BASE-TX      full(auto) off   1518  8/up
0/4  fastether0/4        up    100BASE-TX      full(auto) off   1518  8/up
0/5  fastether0/5        down  -               -         -      8/up
0/6  fastether0/6        down  -               -         -      8/up
:
:
```

13.4 Description of Fastethernet [AX1250S] [AX1240S]

A Fastethernet port uses a 10BASE-T or 100BASE-TX twisted pair cable (UTP). This section describes a 10BASE-T or 100BASE-TX interface.

13.4.1 Functionality

(1) Connection interface: 10BASE-T or 100BASE-TX

(a) Automatic 10BASE-T/100BASE-TX recognition (auto-negotiation)

10BASE-T and 100BASE-TX support connection methods that use automatic recognition (auto-negotiation) and fixed settings.

- Automatic recognition: 10BASE-T and 100BASE-TX
- 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) Connection specifications of 10BASE-T and 100BASE-TX

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.

Table 13-5 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	N	N	N	100BASE-TX full duplex	N

Settings on the remote device		Settings on the Switch				
Method	Interface	Fixed settings				Auto-negotiation
		10BASE-T half duplex	10BASE-T full duplex	100BASE-TX half duplex	100BASE-TX full duplex	
	full duplex					
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
	10/100BASE-TX full duplex and half duplex	10BASE-T half duplex	N	100BASE-TX half duplex	N	100BASE-TX full duplex

Legend N: A connection is not possible

(2) Auto-negotiation

Two connected devices use auto-negotiation to determine the connection conditions (transmission speed, duplex mode (full or half), and whether to use flow control).

Reference note: For details on the connection specifications for the Switch, see *Table 13-5 Connection specifications for transmission speed and duplex mode (full or half)*.

(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. Flow control can be configured separately for sending and receiving packets. This functionality operates even if only one of them is configured. For details about how the operation mode is determined from the settings on the Switch and remote device, see *Table 13-6 Flow control for sending on the switch*, *Table 13-7 Flow control for receiving on the switch*, and *Table 13-8 Flow control operation determined by the auto-negotiation result*.

Table 13-6 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.
desired	desired	Sending on the remote device is regulated.

Legend:

on: Enabled.

off: Disabled. If auto-negotiation is selected and either **on** or **off** is set when **desired** is set on the remote device, the flow control operation mode is determined by the negotiation result. For details, see *Table 13-8 Flow control operation determined by the auto-negotiation result*. For any setting other than auto-negotiation, **flowcontrol** is fixed to **on**.

desired: Enabled. If auto-negotiation is selected, the flow control operation mode is determined from the negotiation result. For details, see *Table 13-8 Flow control operation determined by the auto-negotiation result*.

Table 13-7 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.
desired	desired	Sending on the Switch is regulated.

Legend:

on: Enabled.

off: Disabled. If auto-negotiation is selected and either **on** or **off** is set when **desired** is set on the remote device, the flow control operation mode is determined by the negotiation result. For details, see *Table 13-8 Flow control operation determined by the auto-negotiation result*. For any setting other than auto-negotiation, **flowcontrol** is fixed to **on**.

desired: Enabled. If auto-negotiation is selected, the flow control operation mode is determined from the negotiation result. For details, see *Table 13-8 Flow control operation determined by the auto-negotiation result*.

Table 13-8 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	Pause packet	Is sending regulated on the Switch?	Is sending regulated on the remote device?
on	any	Enabled	any	Enabled	Yes	Yes
		any	Enabled	Enabled	Yes	Yes
		Disabled	Disabled	Disabled	No	No
any	on	Enabled	any	Enabled	Yes	Yes
		any	Enabled	Enabled	Yes	Yes
		Disabled	Disabled	Disabled	No	No
desired	any	Enabled	any	Enabled	Yes	Yes
		any	Enabled	Enabled	Yes	Yes
		Disabled	Disabled	Disabled	No	No
any	desired	Enabled	any	Enabled	Yes	Yes
		any	Enabled	Enabled	Yes	Yes
		Disabled	Disabled	Disabled	No	No
off	off	Enabled	any	Disabled	No	No
		any	Enabled	Disabled	No	No
		Disabled	Disabled	Disabled	No	No

#

any indicates that any setting is allowed for the Switch (**on**, **off**, or **desired**) or the remote device (**Enabled** or **Disabled**).

(4) Automatic MDIX functionality

The automatic MDIX functionality automatically switches between MDI and MDI-X. The functionality enables communication via either a crossover cable or a straight cable, and is available only when auto-negotiation is used. If the connection mode (full duplex or half duplex) is fixed, MDI-X is always selected. The following table shows the MDI and MDI-X pin mappings.

Table 13-9 MDI and MDI-X pin mappings

RJ45 Pin No.	MDI		MDI-X	
	100BASE-TX	10BASE-T	100BASE-TX	10BASE-T
1	TD+	TD+	RD+	RD+
2	TD-	TD-	RD-	RD-
3	RD+	RD+	TD+	TD+
4	Unused	Unused	Unused	Unused
5	Unused	Unused	Unused	Unused
6	RD-	RD-	TD-	TD-
7	Unused	Unused	Unused	Unused
8	Unused	Unused	Unused	Unused

#

For the 10BASE-T and 100BASE-TX cables, separate signal lines are used for sending (TD) and reception (RD).

(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 *13.1.3 Control on the MAC and LLC sublayers*. For details about the format of tagged frames, see the format of tagged frames in *17.1.5 VLAN tags*. Note that switches support only 100BASE-TX (full duplex) as the physical interface. The following table describes the jumbo frame support status.

Table 13-10 Jumbo frame support status

Item	Frame format		Description
	Ethernet V2 [#]	IEEE 802.3 [#]	
Frame size (octets)	No tags: 1519 to 9234 With tags: 1523 to 9238	N	Total field size of DA (in the MAC header) to DATA FCS is 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

#

See the format of frames in *13.1.3 Control on the MAC and LLC sublayers*.

(6) Notes when 10BASE-T or 100BASE-TX is connected

- Make sure that the transmission speed and the duplex mode (full or half) settings on the local and remote devices are the same.
If these settings on the devices are different, communication might stop. If communication stops, execute the `inactivate` operation command, and then execute the `activate` operation command for the relevant ports.
- When using 100BASE-TX, use a twisted pair cable (UTP) of category 5 or higher as the connection cable.
- A full-duplex interface is implemented by not using collision detection and loopback functions. Therefore, to use 10BASE-T or 100BASE-TX under a full-duplex setting, make sure that you set the connecting interface of the remote device to full-duplex.

13.5 Configuration of Fastethernet [AX1250S] [AX1240S]

13.5.1 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 fastethernet 0/10
(config-if)# shutdown
(config-if)# speed 10
(config-if)# duplex half
```

Configures the switch so that the connection with the remote device is a 10BASE-T, half-duplex connection.

2.

```
(config-if)# no shutdown
(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 fastethernet 0/10
(config-if)# shutdown
(config-if)# speed auto 100
```

Configure the Switch to only use 100BASE-TX even if it establishes a connection with the remove 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.

13.5.2 Flow control settings

For details, see *13.2.7 Flow control settings*.

13.5.3 Automatic MDIX functionality settings

For details about automatic MDIX settings, see *13.2.8 Automatic MDIX functionality settings*.

13.5.4 Using jumbo frames

For details about jumbo frame settings, see *13.2.9 Using jumbo frames*.

13.6 Description of Gigabitethernet (RJ45)

A Gigabitethernet (RJ45) port uses a 10BASE-T, 100BASE-TX, or 1000BASE-T twisted pair cable (UTP). This section describes the 10BASE-T, 100BASE-TX, and 1000BASE-T interface.

13.6.1 Functionality

(1) Connection interface: 10BASE-T, 100BASE-TX, and 1000BASE-T

(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 configuration settings of the Switch and the connection specifications for transmission speed and duplex mode (full or half) on 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, auto-negotiation mode.

Table 13-11 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	N	N	100BASE-TX half duplex	N	100BASE-TX

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	
	half duplex					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
	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

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	
	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
	10/100/1000 BASE-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

Two connected devices use auto-negotiation 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 13-11 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 operation, see (6) *Down-shift functionality in 13.6.1 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. The flow control settings for sending and reception are configured separately. Whether to enable or disable flow control depends on these settings and the auto-negotiation result. When specifying the flow control settings, make sure that the sending and receiving settings on the Switch and the remote device do not conflict. For example, if you set **on** for the pause-packet send setting on the Switch, pause packet reception on the remote device must be enabled. For details about how the operation mode is determined from the settings on the Switch and remote device, see *Table 13-12 Flow control for sending on the switch*, *Table 13-13 Flow control for receiving on the switch*, and *Table 13-14 Flow control operation determined by the auto-negotiation result*.

Table 13-12 Flow control for sending on the switch

Pause-packet send setting on the Switch	Pause-packet receive setting on the remote device	Flow control operation
on	Enabled	Sending on the remote device is regulated.
off	Disabled	Sending on the remote device is not regulated.
desired	desired	Sending on the remote device is regulated.

Legend:

on: Enabled.

off: Disabled. If either **on** or **off** is set when **desired** is set on the remote device, the flow control operation mode is determined by the negotiation result. For details, see *Table 13-14 Flow control operation determined by the auto-negotiation result*.

desired: Enabled. If auto-negotiation is selected, the flow control operation mode is determined from the negotiation result. For details, see *Table 13-14 Flow control operation determined by the auto-negotiation result*.

Table 13-13 Flow control for receiving on the switch

Pause-packet receive setting on the Switch	Pause-packet send setting on the remote device	Flow control operation
on	Enabled	Sending on the Switch is regulated.
off	Disabled	Sending on the Switch is not regulated.
desired	desired	Sending on the Switch is regulated.

Legend:

on: Enabled.

off: Disabled. If either **on** or **off** is set when **desired** is set on the remote device, the flow control operation mode is determined by the negotiation result. For details, see *Table 13-14 Flow control operation determined by the auto-negotiation result*.

desired: Enabled. If auto-negotiation is selected, the flow control operation mode is determined from the negotiation result. For details, see *Table 13-14 Flow control operation determined by the auto-negotiation result*.

Table 13-14 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	off	off	No	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	Yes	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
		Enabled	Enabled	on	on	Yes	Yes
			Disabled	off	on	Yes	No
			desired	on	on	Yes	Yes
off	desired	Enabled	Enabled	on	on	Yes	Yes
			Disabled	off	on	Yes	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	Yes	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
		Enabled	Enabled	on	on	Yes	Yes
			Disabled	off	off	No	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?
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	Yes	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
	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	Yes	Yes
			Disabled	off	off	No	No

Switch		Remote device		Result of auto-negotiation on the Switch		Flow control operation	
Send pause packet	Receive pause packet	Send pause packet	Receive pause packet	Send pause packet	Receive pause packet	Is sending regulated on the Switch ?	Is sending regulated on the remote device?
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes

(4) Automatic MDIX functionality

The automatic MDIX functionality automatically switches between MDI and MDI-X. The functionality enables communication via either a crossover cable or a straight cable, and is available only when auto-negotiation is used. If the connection mode (full duplex or half duplex) is fixed, MDI-X is always selected. The following table shows the MDI and MDI-X pin mappings.

Table 13-15 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 *13.1.3 Control on the MAC and LLC sublayers*. For details about the format of tagged frames, see the format of tagged frames in *17.1.5 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 13-16 Jumbo frame support status

Item	Frame format		Description
	Ethernet V2 [#]	IEEE 802.3 [#]	
Frame size (octets)	No tags: 1519 to 9234 With tags: 1523 to 9238	N	Total field size of DA (in the MAC header) to DATA FCS is 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

[#]

See the format of frames in *13.1.3 Control on the MAC and LLC sublayers*.

(6) Down-shift functionality

Down-shift works when auto-negotiation is set. If a link cannot be established by using auto-negotiation, down-shift disables the highest speed advertized during auto-negotiation, and then tries establishing a link by using the next highest speed. (No operation can disable the down-shift functionality.)

(a) Applied line

This functionality is supported on 1000BASE-T.

(b) Order of changing line speed

After auto-negotiation is completed, if a link cannot be established, the line speed is lowered as follows: phase 1 -> phase 2 ... If a link cannot be established even at the lowest line speed, the operation returns to phase 1 and the down-shift operation continues.

Table 13-17 Order of changing line speed

#	Down-shift functionality	Phase	Configuration (speed parameter setting) ^{#1}				Remarks
			auto	auto 10 100 1000	auto 10 100	auto 1000, 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	--	--	

--: A down-shift operation is not performed. The usual auto-negotiation is performed.

#1: The number indicates the line speed.

(7) Notes on a 10BASE-T, 100BASE-TX, or 1000BASE-T connection

- If a switch and the remote device to be connected do not have the same transmission speed and duplex mode (full or half), the devices cannot be connected.
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.
- When using 100BASE-TX, use a twisted pair cable (UTP) of category 5 or higher as the connection cable. When using 1000BASE-T, use a twisted pair cable (UTP) of enhanced category 5 or higher as the connection cable.
- A full-duplex interface is implemented by not using collision detection and loopback functions. Therefore, to use 10BASE-T or 100BASE-TX under a full-duplex setting, 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.

13.6.2 Automatic SFP recognition (selection of media type) [AX1250S] [AX1240S]

A Gigabitethernet port on the Switch is used as either an RJ45 (10BASE-T/100BASE-TX/1000BASE-T) port or an SFP (100BASE-FX/1000BASE-X) port exclusively. In the default configuration with which these Switches ship, automatic detection of a media type is set. If SFP is detected, SFP is used. (When link-up is detected on a 1000BASE-X port, the media type is switched to SFP.)

To use a fixed media type (fixed to SFP or RJ45), set it by using the `media-type` configuration command.

13.7 Configuration of Gigabitethernet (RJ45)

13.7.1 Configuring ports

(1) Setting the transmission speed and duplex mode

You can set the transmission speed and duplex mode used for communication between the Switch and a remote device. By default, the transmission speed and duplex mode are determined automatically by auto-negotiation. To change to the transmission speed and duplex mode that corresponds to the remote device, first specify `rj45` for the media type, and then change the setting. For details about media types, see *13.7.5 Setting the media type [AX1250S] [AX1240S]*.

(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 0/25
(config-if)# shutdown
(config-if)# media-type rj45
(config-if)# speed 100
(config-if)# duplex half
```

This example 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 0/25
(config-if)# shutdown
(config-if)# media-type rj45
(config-if)# speed auto 1000
```

This sequence ensures 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.

13.7.2 Flow control settings

For details, see *13.2.7 Flow control settings*.

13.7.3 Automatic MDIX functionality settings

For details about automatic MDIX settings, see *13.2.8 Automatic MDIX functionality settings*.

13.7.4 Using jumbo frames

For details about jumbo frame settings, see *13.2.9 Using jumbo frames*.

13.7.5 Setting the media type [AX1250S] [AX1240S]

You can use the `media-type` command to set which media is used on a 1 gigabit Ethernet port.

(1) Setting automatic media detection

Points to note

You can enable automatic media detection for a 1 gigabit Ethernet interface as follows.

Command examples

1. `(config)# interface range gigabitethernet 0/25-26`
`(config-if-range)# shutdown`
`(config-if-range)# media-type auto`
 This enables automatic media detection.
2. `(config-if-range)# no shutdown`
`(config-if-range)# exit`

(2) Setting the media to RJ45

Points to note

You must configure this setting if you choose to use a 10BASE-T, 100BASE-TX, or 1000BASE-T interface.

Command examples

1. `(config)# interface range gigabitethernet 0/25-26`

```
(config-if-range)# shutdown
```

```
(config-if-range)# media-type rj45
```

Disables automatic media detection, and sets that a 10BASE-T, 100BASE-TX, or 1000BASE-T interface is used.

2. `(config-if-range)# no shutdown`

```
(config-if-range)# exit
```

(3) Setting the media to SFP

Points to note

You must configure this setting if you choose to use SFP as the fixed media type.

Command examples

1. `(config)# interface range gigabitethernet 0/25-26`

```
(config-if-range)# shutdown
```

```
(config-if-range)# media-type sfp
```

- Disables automatic media detection, and sets the media type to SFP.

2. `(config-if-range)# no shutdown`

```
(config-if-range)# exit
```

(4) Notes when setting the media type [AX1250S] [AX1240S]

1. If the `media-type` setting is changed, the settings of the following configuration commands return to the default values:
 - `duplex`
 - `mdix auto`
 - `speed`
2. If `media-type auto` is set, the configuration commands below cannot be set. Use the default value.
 - `duplex`
 - `mdix auto`
 - `speed`

13.8 Description of Gigabitethernet (SFP)

A Gigabitethernet (SFP) port uses a 100BASE-FX or 1000BASE-X optical fiber cable. This section describes a 100BASE-FX or 1000BASE-X optical fiber interface.

13.8.1 Functionality

100BASE-FX or 1000BASE-X optical fiber interfaces are described below.

(1) Connection interface: 100BASE-FX [AX1250S]

The 100BASE-FX interface is supported. The transmission speed and duplex mode settings are fixed at 100 Mbit/s and full duplex. Auto-negotiation is not supported.

100BASE-FX:

This Ethernet interface uses a multiple-terminal mode optical fiber cable that ensures a connection over two kilometers.

(2 km max. in multiple-terminal mode)

Configure the following mode:

- Transmission speed: fixed to 100 Mbit/s, duplex: full duplex
- Media type: fixed to SFP

(a) 100BASE-FX connection specifications

The table below describes the configuration settings on the Switch and the connection specifications for transmission speed and duplex mode (full or half) on a remote device. For details about the physical specifications for the 100BASE-FX interface, see the *Hardware Instruction Manual*.

Table 13-18 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-FX full duplex
Fixed settings	100BASE-FX half duplex	N
	100BASE-FX full duplex	100BASE-FX full duplex
Auto-negotiation	100BASE-FX half duplex	N
	100BASE-FX full duplex	N

Legend N: A connection is not possible

(2) Connection interface: 1000BASE-X

The 1000BASE-SX, 1000BASE-SX2, 1000BASE-LX, 1000BASE-LH, and 1000BASE-BX interfaces are supported. The transmission speed and duplex mode settings are fixed at 1000 Mbit/s and full duplex.

1000BASE-SX:

This Ethernet interface is used for short-distance connections
(550m max. in multiple-terminal mode)

1000BASE-SX2:

This Ethernet interface uses a multiple-terminal mode optical fiber cable that ensures a connection over two kilometers.
(2 km max. in multiple-terminal mode)

1000BASE-LX:

This Ethernet interface is used for medium-distance connections
(5 km max. in single-terminal mode, 550 m max. in multiple-terminal mode)

1000BASE-LH:

This Ethernet interface is used for long-distance connections
(70 km max. in single-terminal mode)

1000BASE-BX:

This Ethernet interface is a low-cost interface that uses a single-core optical fiber in 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 switch.

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/1000BASE-BX10-U:

This Ethernet interface is used for medium-distance connections
(10km max. in single-terminal mode)

1000BASE-BX40-D/1000BASE-BX40-U:

This Ethernet interface is used for long-distance connections
(40 km max. in single-terminal 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)

(a) 1000BASE-X connection specifications

The table below describes the configuration settings on the Switch and the connection specifications for transmission speed and duplex mode (full or half) on a remote device. For details about the physical specifications for the 1000BASE-X interface, see the *Hardware Instruction Manual*.

Table 13-19 Connection specifications for transmission speed and duplex mode (full or half)

Settings on the remote device		Settings on the Switch	
Method	Interface	Fixed settings	Auto-negotiation
		1000BASE full duplex	1000BASE full duplex
Fixed settings	1000BASE half duplex	N	N
	1000BASE full duplex	1000BASE full duplex	N
Auto-negotiation	1000BASE half duplex	N	N
	1000BASE full duplex	N	1000BASE full duplex

Legend N: A connection is not possible

(3) 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 13-19 Connection specifications for transmission speed and duplex mode (full or half)*. Note that if the connection conditions are not determined by auto-negotiation, the Switch attempts to establish a connection until a link is established.

Auto-negotiation is not supported on 100BASE-FX.

(4) 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. The flow control settings for sending and reception are configured separately. Whether to enable or disable flow control depends on these settings and the auto-negotiation result. When specifying the flow control settings, make sure that the sending and receiving settings on the Switch and the remote device do not conflict. For example, if you set **on** for the pause-packet send setting on the Switch, pause packet reception on the remote device must be enabled. For details about how the operation mode is determined from the settings on the Switch and remote device, see *Table 13-20 Flow control for sending on the switch*, *Table 13-21 Flow control for receiving on the switch*, and *Table 13-22 Flow control operation determined by the auto-negotiation result*.

For 100BASE-FX, no flow control is performed during auto-negotiation because auto-negotiation is not supported.

Table 13-20 Flow control for sending on the switch

Pause-packet send setting on the Switch	Pause-packet receive setting on the remote device	Flow control operation
on	Enabled	Sending on the remote device is regulated.
off	Disabled	Sending on the remote device is not regulated.
desired	desired	Sending on the remote device is regulated.

Legend:

on: Enabled.

off: Disabled. If either **on** or **off** is set when **desired** is set on the remote device, the flow control operation mode is determined by the negotiation result. For details, see *Table 13-22 Flow control operation determined by the auto-negotiation result*.

desired: Enabled. If auto-negotiation is selected, the flow control operation mode is determined from the negotiation result. For details, see *Table 13-22 Flow control operation determined by the auto-negotiation result*.

Table 13-21 Flow control for receiving on the switch

Pause-packet receive setting on the Switch	Pause-packet send setting on the remote device	Flow control operation
on	Enabled	Sending on the Switch is regulated.
off	Disabled	Sending on the Switch is not regulated.
desired	desired	Sending on the Switch is regulated.

Legend:

on: Enabled.

off: Disabled. If either **on** or **off** is set when **desired** is set on the remote device, the flow control operation mode is determined by the negotiation result. For details, see *Table 13-22 Flow control operation determined by the auto-negotiation result*.

desired: Enabled. If auto-negotiation is selected, the flow control operation mode is determined from the negotiation result. For details, see *Table 13-22 Flow control operation determined by the auto-negotiation result*.

Table 13-22 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	off	off	No	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	Yes	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
		off	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	off	No	No
			desired	on	on	Yes	Yes
		Disabled	Enabled	on	on	Yes	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
		off	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	Yes	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
		desired	Enabled	on	on	Yes	Yes
			Disabled	off	off	No	No
			desired	on	on	Yes	Yes
	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	Yes	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
			desired	on	on	Yes	Yes

(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 *13.1.3 Control on the MAC and LLC sublayers*. For details about the format of tagged frames, see the format of tagged frames in *17.5 VLAN tags*. The following table describes the jumbo frame support status.

Table 13-23 Jumbo frame support status

Item	Frame format		Description
	Ethernet V2 [#]	IEEE 802.3 [#]	
Frame size (octets)	No tags: 1519 to 9234 With tags: 1523 to 9238	N	Total field size of DA (in the MAC header) to DATA FCS is 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

[#]

See the format of frames in *13.1.3 Control on the MAC and LLC sublayers*.

(6) Automatic SFP recognition (selection of media type) [AX1250S] [AX1240S]

See *13.6.2 Automatic SFP recognition (selection of media type) [AX1250S] [AX1240S]*.

See also *13.8.2 Notes on using SFP* below because some SFP transceivers have restrictions on the automatic media detection functionality.

13.8.2 Notes on using SFP

(1) Notes when inserting a 1000BASE-FX SFP transceiver [AX1250S]

Media type is not automatically detected on 100BASE-FX even if automatic media detection is enabled. For 100BASE-FX, use the following settings:

- Transmission speed: Fixed to 100 Mbit/s; duplex: Full duplex
- Media type: Fixed to SFP

(2) Notes after 100BASE-FX is used [AX1250S]

If you use 10BASE-T, 100BASE-TX, 1000BASE-T or 1000BASE-X after using 100BASE-FX, change the following settings in the order given before starting use:

1. Delete the speed setting (no speed).
2. Delete the full-duplex setting (no duplex).
3. Delete the media type setting (no media-type).

(3) 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.

(4) Automatic media detection operation and restrictions on 1000BASE-SX2 [AX1250S] [AX1240S]

In automatic media detection, priority is given to 1000BASE-X. When the 1000BASE-X link is enabled, even if 10BASE-T, 100BASE-TX, or 1000BASE-T (RJ45) is being used, 1000BASE-X is automatically detected.

However, for SFP for 1000BASE-SX2, if RJ45 is being used, 1000BASE-X is not automatically detected because the 1000BASE-X link is not enabled.

Therefore, for 1000BASE-SX2, use either of the following methods:

1. Use the fixed media setting.
2. Make sure an optical fiber cable and a UTP (RJ45) cable are not inserted at the same time.

(5) Notes when inserting a 1000BASE-BX[#] SFP transceiver [AX1250S] [AX1240S]

If a 1000BASE-BX SFP transceiver is inserted when automatic media detection functionality is enabled and the 10BASE-T, 100BASE-TX, or 1000BASE-T (RJ45) link is enabled, note that a link-down temporarily occurs in 10BASE-T, 100BASE-TX, or 1000BASE-T.

#

1000BASE-BX10-D, 1000BASE-BX10-U, 1000BASE-BX40-D, or
1000BASE-BX40-U

When operation on the RJ45 side has precedence, insert the 1000BASE-BX SFP transceiver by using either of the following methods:

1. Insert an SFP transceiver with the fixed media (RJ45) setting.
2. Insert the SFP transceiver before turning on the Switch.

13.9 Configuration of Gigabitethernet (SFP)

13.9.1 Setting 100BASE-FX ports [AX1250S]

For a port for which 100BASE-FX is used, specify the transmission speed, full duplex, and media type.

Points to note

Configure as follows: transmission speed of 100 Mbit/s, full duplex, and a media type of SFP

Command examples

1.

```
(config)# interface gigabitethernet 0/26
(config-if)# shutdown
(config-if)# media-type sfp
(config-if)# speed 100
(config-if)# duplex full
```

Sets the media type to `sfp` and configures a 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

When you use 100BASE-FX, make sure that you configure the above settings. (Flow control is disabled when `duplex` has not been set or has been set to `auto`.)

13.9.2 Setting a 1000BASE-X port

(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. To change to the transmission speed and duplex mode that corresponds to the remote device, first specify `sfp` for the media type, and then change the setting. For details about media types, see *13.7.5 Setting the media type [AX1250S] [AX1240S]. [AX1250S] [AX1240S]*

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)# media-type sfp
(config-if)# speed 1000
(config-if)# duplex full
```

Sets the media type to `sfp`, and 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.

13.9.3 Flow control settings

For details, see *13.2.7 Flow control settings*.

13.9.4 Using jumbo frames

For details about jumbo frame settings, see *13.2.9 Using jumbo frames*.

13.9.5 Setting the media type [AX1250S] [AX1240S]

For details, see *13.7.5 Setting the media type [AX1250S] [AX1240S]*.

13.10 Description of PoE [AX2200S] [AX1240S]

13.10.1 Overview of PoE

PoE (Power over Ethernet) supplies power to network devices by using an RJ45 cable, which is normally a cable used for data communication. It can supply a maximum of 30.0 W of power. An AX2200S series switch can supply a maximum of 60.0 W of power.

PoE is used for network devices installed at locations where external power is not readily available. In PoE, the power supplier is called *power sourcing equipment* (PSE), and the power receiver is called a *powered device* (PD).

The Switch, which is a PSE that complies with the IEEE 802.3af and IEEE802.3at standards, automatically performs three processes: detecting the PD (detection process), classifying the level of power required by the PD (power level classification process), and supplying power (power supply process).

(1) Detection process

The detection process detects whether the connected device is a PD. If the connected device is a PD that complies with the IEEE 802.3af or IEEE802.3at standards, the processing proceeds to the next power level classification process. Note, however, that the switch does not supply power to a network device that does not support PoE.

(2) Power level classification process

In the power level classification process, the power level of the PD is determined by the use of a special voltage defined in the IEEE802.3af and IEEE802.3at standards. The PD recognizes that it is in the power level classification process due to the special voltage supplied from the Switch. At this time, the Switch can determine which of the five power classes the PD belongs to by how the PD consumes the current (also defined in the IEEE802.3af and IEEE802.3at standards). Note that because power level classification is prescribed as optional in the IEEE 802.3af standard, not all PDs always support such power level classifications. A device that does not support this classification is classified as Class 0.

(3) Power supply process

Based on the PD's demand, the Switch can supply power up to the maximum output power shown in *Table 13-24 Power class and maximum output power of the Switch*.

Table 13-24 Power class and maximum output power of the Switch

Power class	Maximum output power
Class 0	15.4 W
Class 1	4.0 W
Class 2	7.0 W
Class 3	15.4 W
Class 4	30.0 W

13.10.2 Allocating the power supplied by PoE [AX2200S]

AX2200S series switches can supply 60.0 W of power, in addition to complying with the IEEE802.3af and IEEE802.3at standards. As shown in the figure below, AX2200S series switches can supply 60.0 W on ports 0/1 to 0/4 (system 1). They can also supply a

maximum of 30.0 W on ports 0/5 to 0/24 (system 2).

Figure 13-6 Overview of the power supply functionality on an AX2200S series switch

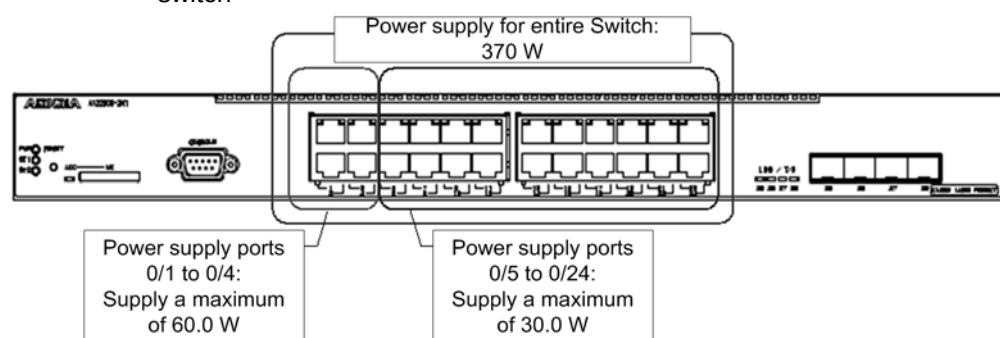


Table 13-25 Overview of the PoE functionality on an AX2200S switch

Functionality		Specifications		Remarks
Model		AX2230S-24P		
Maximum capacity of power supply	For entire Switch [W]		370.0	
	For each port [W]	System 1: 0/1 to 0/4	60.0	Manually set by the configuration.
		System 2: 0/5 to 0/24	30.0	
	For each class [W]	Class 0	15.4	
		Class 1	4.0	
		Class 2	7.0	
		Class 3	15.4	
		Class 4	30.0	
Pre.STD		Not supported		
Priority control		Operates within system 1.		
		Operates within system 2.		

(1) Power control for entirely Switch

An AX2200S series switch controls the maximum amount of power that can be supplied by the entire Switch by means of two power supply systems: system 1 (for ports 0/1 to 0/4) and system 2 (for ports 0/5 to 0/24).

Table 13-26 Power control for each system shows the maximum power control for each system.

For system 1, you can use the configuration command below to set the maximum amount of power that can be supplied. To apply this configuration command, you need to restart the Switch.

```
power inline system-allocation limit <Threshold>
```


Table 13-26 Power control for each system

Syst em	Applica ble port	Maximum power control operations	Remarks
1	0/1 to 0/4	- For system 1, the maximum amount of power to be supplied set by the configuration is allocated. - After the setting is changed, the Switch must be restarted. - Priority control is performed among system 1 ports.	System 1 default 61.6 [W] (= 15.4 [W] × 4 ports)
2	0/5 to 0/24	- For system 2, the value obtained by subtracting the maximum amount of power supply allocated for system 1 from the maximum amount of power supply for the entire Switch is allocated. - The maximum amount of power supply to allocate for system 2 depends on the configuration of system 1. The value for system 2 cannot be set by the configuration. - Priority control is performed among system 2 ports.	System 2 default 308.4 [W] (= 370.0 [W] - 61.6 [W])

(2) Allocating power supplied by PoE

The following two types of setting methods can be used for allocating power for system 1 and system 2, and either of the setting methods can be selected for each port separately:

- Class-based setting
- Manual setting

(a) Class-based setting

When the class-based setting is specified using the `power inline allocation auto` configuration command to set the amount of power to allocate to the target port, the allocation of the power supplied is calculated based on the class. The class-based allocation of power supply is handled according to *Table 13-24 Power class and maximum output power of the Switch*.

(b) Manual setting

When the manual setting is specified using the `power inline allocation limit` configuration command to set the amount of power to allocate to the target port, the amount of power to be allocated is manually calculated.

Normally, operation is performed using the class-based setting. However, if the actual power consumption is considerably smaller than the power allocated based on the class, operation can be economized by manually setting the allocation.

For example, when you connect the PD that is classified in Class 4 (30.0 W) according to the class-based setting, if the actual power consumption of the PD is 18.0 W, you can manually set the power to 20.0 W, which allows you to increase the power that can be allocated to other ports.

If you connect a PD to system 1 that requires more than 30.0 W, you need to manually allocate the maximum supply power.

13.10.3 Allocating power supplied by PoE [AX1240S]

(1) Capacity limits

The following table describes the amount of power that the Switch can supply by using PoE, and the maximum number of PDs that can connect concurrently to (can receive power from) the switch.

Table 13-27 Maximum number of PDs that can connect concurrently to (can receive power from) the switch

Item		Specifications
Model		AX1240S-24P2C
Total amount of power that the Switch's PoE can supply		370.0 W
Number of PoE ports to which PDs can be connected ^{#1}	Class 0 (15.4 W)	24 ports ^{#2}
	Class 1 (4.0 W)	24 ports
	Class 2 (7.0 W)	24 ports
	Class 3 (15.4 W)	24 ports
	Class 4 (30.0 W)	12 ports ^{#3}

#1

If the calculated power to be supplied to PDs exceeds the maximum power value due to some cause such as the addition of PDs, power supply is blocked from ports that have lower priority. (If the priority of the ports is the same, power supply is blocked from the larger port numbers.)

#2

PDs that cannot be negotiated with are treated as Class 0.

#3

The maximum number of PDs that consume 30.0 W and can connect concurrently to switch is 12. (30.0 W x 12 = 360.0 W)

(2) Allocating power to be supplied by PoE

Power to be supplied to a PD can be selected on a port-by-port basis by specifying class-based or manual.

(a) Class-based setting

When the class-based setting is specified using the `power inline allocation auto` configuration command to set the amount of power to allocate to the target port, the allocation of the power supplied is calculated based on the class. Class-based power allocation is handled according to *Table 13-24 Power class and maximum output power of the Switch*.

(b) Manual setting

When the manual setting is specified using the [power inline allocation limit](#) configuration command to set the amount of power to allocate to the target port, the amount of power to be allocated is manually calculated.

Normally, operation is performed using the class-based setting. However, if the actual power consumption is considerably smaller than the power allocated based on the class, operation can be economized by manually setting the allocation.

For example, when you connect a PD that is classified in Class 4 (30.0 W) according to the class-based setting, if the actual power consumption of the PD is 18.0 W, you can manually set the power to 20.0 W, which allows you to increase the supply power allocated to other ports.

If you connect a PD that is Class 0 but needs 30.0 W of power supply, you need to manually allocate the maximum amount of power.

(c) Total amount of power allocated to a port

Set the power to be supplied by PoE (total amount of power to be allocated to a port) to 370.0 W or lower. Also make sure that the amount of power supplied to PDs connected to PoE ports satisfies the following expression:

Total amount of power available for distribution to all ports (W) $\geq$

Number of class 0 ports $\times$ output power (15.4) +

Number of class 1 ports $\times$ output power (4.0) +

Number of class 2 ports $\times$ output power (7.0) +

Number of class 3 ports $\times$ output power (15.4) +

Number of class 4 ports $\times$ output power (30.0) +

Total amount of power for the ports for which manual power allocation is set

13.10.4 Setting behavior of when the maximum power supply is exceeded

You can use the configuration to set the priority of ports that determines whether a port is to be enabled or disabled when the maximum amount of power to be supplied is exceeded for each of system 1 and system 2 (for AX2200S series switches) or when the maximum supply power for the entire Switch is exceeded (for AX1240S series switches).

There are two types of operations when power consumption becomes too large as follows:

- Port priority set by the configuration
- Priority given to the powered ports

(1) Port priority set by the configuration

Power supply priority can be set for each port. This function helps to specify ports for which to ensure power supply as well as ports for which to stop power supply, when power supply becomes insufficient. If no priority is specified by the configuration, the priority is set as [high](#) by default. If more than one port has the same setting, the port with the lower port number is given priority.

For an AX2200S series switch, the priority set for each port is used, and power supply to the ports that have a higher priority within system 1 or system 2 take precedence.

For an AX1240S series switch, the priority set for each port is used, and power supply to the ports that have a higher priority within the entire switch take precedence.

Critical

This level is set for the most important ports, whose power supply is always guaranteed. Set this value for a port for which power must always be supplied.

High

Power is supplied to ports whose priority is set to **high**. Set this level to ports that are frequently used. Ports with no priority specified are assumed to be high-priority ports.

If the amount of power that can be supplied is no longer sufficient, the supply of power to high-priority ports stops later than it does for low-priority ports. Of the high-priority ports, the higher the port number, the earlier the supply of power stops.

Low

Power is supplied to ports whose priority is set to **low**. Set this level to ports that are infrequently used. If the amount of power that can be supplied is no longer sufficient, the supply of power to low-priority ports stops earlier than it does for high-priority ports. Of the low-priority ports, the higher the port number, the earlier the supply of power stops.

Never

The power supply unit stops and the PoE functionality is disabled. Set this level for ports for which the PoE functionality is not used. For the never-priority ports, power is never supplied even when plenty of power is available.

(2) Priority given to the powered ports

This function secures power supply to the ports that have already been connected, without depending on the priority set for each port.

For an AX2200S series switch, powered ports take precedence over other ports in the same system (system 1 or system 2).

For an AX1240S series switch, powered ports take precedence over other ports on the entire switch.

The **power inline priority-control disable** configuration command is used to give priority to the powered ports.

When priority is given to the powered ports, power is first supplied to a power-receiving device connected earlier. When the total power consumption is over 370.0 W, even if a power-receiving device is connected to a port with priority set as **critical**, power will not be supplied.

Therefore, the priority setting configured by the **power inline** configuration command is disabled, and those ports are simply recognized as ports for which power is to be supplied. If the **power inline never** configuration command is set, power is not supplied.

Even when priority is given to the powered ports, a trap for notifying a warning for power supply is issued.

The setting by the **power inline priority-control disable** configuration command is enabled after the Switch is restarted.

(3) Relationship between the configuration and the powered port

The following table describes the relationship between the priority setting by the configuration and the priority of powered port

Table 13-28 Relationship between the configuration and the powered port

Priority of powered port (power inline priority-control disable)	Priority setting by the configuration (power inline)	Behavior of the port
Priority is not given to powered ports (power inline priority-control disable has not been set.)	critical	Ports to supply power: priority critical
	high	Ports to supply power: priority high
	low	Ports to supply power: priority low
	never	Ports not to supply power: priority never
Priority is given to powered ports. (power inline priority-control disable has been set.)	critical	Ports to supply power: priorities critical , high , and low are ignored.
	high	
	low	
	never	Ports not to supply power: priority never

(4) Stopping PoE power supply

If the total power supply to PDs exceeds 370.0 W, power supply is stopped according to the priority set to the ports. The Switch stops power supply to PDs with lower priority when the following condition is met (the resulting value exceeds 370.0 W):

Value for judging the status of power supply (370.0 W) <

Number of class 0 ports × output power (15.4) +

Number of class 1 ports × output power (4.0) +

Number of class 2 ports × output power (7.0) +

Number of class 3 ports × output power (15.4) +

Number of class 4 ports × output power (30.0) +

Total amount of power for the ports for which manual power allocation is set

If the priority of the ports is the same, power supply is stopped from the ports with larger port numbers. (Priority is given to the ports with smaller port numbers for power supply.)

If the priority setting for powered ports has been set, power supply is stopped from the ports with lower port priority. (Priority is given to the powered ports for power supply.)

(5) Notifying the warning for power supply

Because the Switch's maximum capacity of power supply is 370.0 W, priority control is conducted when the total power consumption of all ports exceeds 370.0 W. The threshold of the trap to issue a power supply warning notification is 340.0 W (about 90 %).

13.10.5 Resuming and stopping power supply, and the port status

(1) Resuming and stopping power supply by using an operation command

You can use the `activate power inline` operation command to resume power supply to the Switch ports for which power supply has been stopped.

However, the configuration of ports, execution of operation commands, and behavior of power saving schedule affect power control.

The following table describes configuration commands and scheduled power saving operation, and the effect on power supply control.

Table 13-29 Configuration commands and scheduled power saving operation, and the effect on power supply control

Specifi ed for	Configuration commands	Effect on power supply control			Remarks
		Scheduled power saving operation			
		Disabled	Enabled (Normal time range)	Enabled (Scheduled time range)	
Switch	Not supported	--	--	--	
Port	shutdown	Y	Y	N	
	no shutdown	Y	Y	N	
	power inline never	Y	Y	Y	Forcible stop of power supply
	schedule-power-control shutdown interface	N	N	Y	
	no schedule-power-control shutdown interface	N	N	Y	

Legend:

Y: Affected (Power supply to the relevant ports is resumed or stopped.)

N: Not affected.

--: Not affected because the command is not supported.

The following table describes operation commands and the effect on power supply control. Whether the scheduled power supply operation is enabled is not affected.

Table 13-30 Operation commands and the effect on power supply control

Target	Port setting	Operation commands	Effect on power supply control	Remarks
Switch	None	Not supported	--	
Port	no shutdown Other than power inline never	inactivate interface	N	
		activate interface	N	
		inactivate power inline	Y	Link-down due to power supply stoppage
		activate power inline	Y	Link-up due to resumption of power supply
	All other cases	inactivate interface	N	Execution of operation commands has no affect, and power supply control is performed according to the configuration. (See <i>Table 13-29</i> .)
		activate interface	N	
		inactivate power inline	N	
		activate power inline	N	

Legend:

Y: Affected.

N: Not affected.

--: Not affected because the command is not supported.

(2) Trigger of transition of the port status

Transitions of the status of the ports displayed by the **show power inline** operation command are triggered by the setting of configuration, execution of operation commands, or a change in the status of the power supply.

- **off**: Power is not being supplied.
- **on**: Power is being supplied.
- **denied**: Power is not being supplied because there is not enough power.
- **faulty**: Power cannot be supplied to the connected device.
- **inact**: The supply of power has been stopped by an operation command.

The following table describes the port status and the triggers of status transition.

Table 13-31 Port status and the triggers of status transition

Port status	Trigger of status transition	Port status after transition
off (when no PD is connected)	A PD is connected (power supply is started).	on
	The <code>inactivate power inline</code> operation command is executed.	inact
off (when <code>shutdown</code> is set)	The <code>no shutdown</code> configuration command is set.	off (when no PD is connected)
		on (when a PD is connected)
on	A PD is disconnected (power supply is stopped).	off
	The <code>shutdown</code> configuration command is set.	
	The <code>inactivate power inline</code> operation command is executed.	inact
	Power shortage of the entire Switch is detected (power supply is stopped).	denied
	A power overload is detected.	faulty
	Abnormality on temperature of the PoE controller is detected.	
	Other abnormality is detected.	
denied	The <code>shutdown</code> configuration command is set.	off
	A PD is disconnected.	
	Power shortage of the entire Switch has been resolved (power supply is started).	on
	The <code>inactivate power inline</code> operation command is executed.	inact
faulty	The <code>shutdown</code> configuration command is set.	off
	The <code>activate power inline</code> operation command is executed.	off (when no PD is connected)
		on (when a PD is connected)
	The <code>inactivate power inline</code> operation command is executed.	inact
	A PD is disconnected.	faulty
	A PD is connected.	

Port status	Trigger of status transition	Port status after transition
inact	The <code>shutdown</code> configuration command is set.	off
	The <code>activate power inline</code> operation command is executed.	off (when no PD is connected)
		on (when a PD is connected)
	A PD is disconnected.	inact
	A PD is connected.	

(a) Cause and handling of the faulty port status

When `faulty` is displayed as the port status, power supply to the relevant port is stopped. As shown in *Table 13-31 Port status and the triggers of status transition*, the main causes of `faulty` port status are as follows:

- An overload is detected.
- Abnormality of the temperature of the PoE controller is detected.
- Other PoE abnormality is detected.

To resume power supply to the relevant port, execute the `activate power inline` operation command.

(b) Cause and handling of the denied port status

When `denied` is displayed as the port status, which means power supply of the entire Switch is insufficient, power supply to the relevant port is being stopped.

Use the `show power inline` operation command to check the amount of power allocated to the entire Switch and the total amount of power supplied to the entire Switch, and use configuration to set the appropriate amount of power to be allocated or check the connection configuration of PDs.

When the shortage of power supply of the entire Switch is resolved, the port status `denied` is no longer displayed.

13.10.6 Notes on PoE usage

(1) Setting for manual power allocation

When specifying manual allocation settings, read the documentation for the power-receiving device. The customer performs the operation at the customer's own risk.

Set a value for the maximum power consumption of the power-receiving device that leaves a margin.

If a value smaller than the minimum power consumption required by the power-receiving device is set manually, a power overload is detected and power to the power-receiving device might stop. To restore power, execute the `activate power inline` operation command.

(2) Use on priority of powered port

If you set the `power inline priority-control disable` configuration command, the priority setting by the `power inline` configuration command is disabled, and the relevant ports are recognized merely as the ports for which power is to be supplied. If the `power inline never` configuration command is set, power is not supplied.

After the Switch restarts, it starts power supply from port 0/1 on in order. Therefore, if the

Switch is restarted when its total power consumption requirement exceeds 370.0 W, the ports for which power is supplied might be different from the ones before restarting the Switch.

(3) Connecting a device using Pre.STD

AX2200S series switches do not support connection to a device using Pre.STD.

For AX1240S series switches, use a straight cable to connect a PD that supports Pre.STD. A connection cannot be established by using a crossover cable.

(4) When a power saving scheduled is also used

If `schedule-power-control shutdown interface` is set to a PoE port, the console might appear not to respond for ten seconds or so at the timing of switching to the scheduled time range.

(5) Notes when the port status transition to denied [AX2200S]

If the port status transitions to `denied`, the Switch stops power supply to the relevant port. To restore power, execute the `activate power inline` operation command.

13.11 Configuration of PoE [AX2200S] [AX1240S]

13.11.1 List of configuration commands

The following table lists and describes the commands used to configure PoE.

Table 13-32 List of configuration commands

Command name	Description
power inline	Sets the port priority.
power inline priority-control disable	Assigns priority to a powered port.
power inline allocation	Sets power allocation for each port either based on its class or manually.
power inline system-allocation [AX2200S]	Sets the maximum amount of power that can be supplied for system 1 manually.

13.11.2 Setting the maximum amount of power that can be supplied for system 1 [AX2200S]

An AX2200S series switch has two systems, system 1 and system 2, and you can set the maximum amount of power that can be supplied for the whole of system 1 in the configuration.

The amount of power allocated to the whole of system 2 is obtained by subtracting the value allocated to system 1 from the value 370.0 W (for the entire Switch).

Points to note

You can allocate the maximum power supply of 240.0 W in order to supply 60.0 W for system 1 as follows.

Command examples

1. `(config)# power inline system-allocation limit 240000`

Please execute the reload command after save,
because this command becomes effective after reboot.

Sets 240.0 W as the maximum amount of power that can be supplied to the whole of system 1. A message appears that asks you to save the settings and restart the device.

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 command mode to administrator mode, and saves the settings.

3. `@# reload`

`Restart OK? (y/n): y`

After the configuration setting is saved, @ is displayed in front of the prompt. Use the `reload` operation command to restart the Switch.

Notes

When this command is set or deleted, the new setting is applied after the Switch is restarted.

13.11.3 Setting port priority

The Switch uses PoE with three priority levels. If the amount of available power is insufficient, a port with a lower priority level loses power earlier. If you do not want the Switch to supply power to specific ports, you can stop the supply of power to those ports.

Points to note

If a device that you want to connect is a PoE-powered device and you do not want to supply PoE power from the Switch, or if a remote device to which you want to connect is also a PoE-power sourcing equipment, set the **Never** priority level for the port.

In the example below, port **0/10** will be configured so that power is never supplied to it.

Notes

If PoE ports of the Switch are used to connect to a PSE, make sure that you set *never* as the power supply priority level for these ports. If you do not stop the supply of power to a PSE, an overload might be detected, resulting in the output of a message. If the power supplied from the remote PSE can be stopped, we recommend also stopping the power supplied from the remote PSE.

Command examples

1.

```
(config)# interface fastethernet 0/10
(config-if)# power inline never
```

Configures a specific port so that PoE does not supply power to it.
2.

```
(config-if)# exit
```

13.11.4 Setting so that priority is given to powered ports

When port priority is disabled and priority is given to the powered ports, power is first supplied to the PDs connected earlier. When the total power consumption is over 370.0 W, even if a power-receiving device is connected to a port with priority set as **critical**, power will not be supplied.

Points to note

You can disable the port priority setting configured by the **power inline** configuration command and give priority to powered ports as follows.

Command examples

1.

```
(config)# power inline priority-control disable
```

Please execute the reload command after save, because this command becomes effective after reboot.

Disables the port priority setting, and gives priority to powered ports. A message appears that asks you to save the settings and restart the device.
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 command mode to administrator mode, and saves the settings.

3. `@# reload`

`Restart OK? (y/n): y`

After the configuration setting is saved, `@` is displayed in front of the prompt. Use the `reload` operation command to restart the Switch.

Notes

When this command is set or deleted, the new setting is applied after the Switch is restarted.

13.11.5 Allocating power that can be supplied to each port

Power to be supplied to each port can be set either based on its class or manually. The initial setting is based on its class.

Points to note

If you connect a class 4 PD and its power consumption is lower than the maximum power consumption of 30.0 W, set the power to be supplied, adding a margin to the maximum power consumption of the PD.

In this example, you set an arbitrary value for the power supplied to port 0/20.

Command examples

1. `(config)# interface fastethernet 0/20`

`(config-if)# power inline allocation limit 20000`

Sets 20000 mW (20 W) for the power to be supplied to port 0/20.

2. `(config-if)# exit`

13.12 Operation of PoE [AX2200S] [AX1240S]

The following table describes the list of operation commands for PoE.

Table 13-33 List of operation commands

Command name	Description
show power inline	Displays PoE information.
activate power inline	Manually resumes the supply of power.
inactivate power inline	Manually stops the supply of power.

13.12.1 Checking the PoE power supply status

You can check the PoE power supply status by using the `show power inline` operation command. When the power is supplied, `on` is displayed in `Status`, the priority for power supply is displayed in `Priority`, the power class that complies with IEEE802.3af and IEEE802.3at is displayed in `Class`, and the current, voltage, and power consumption are displayed in `Cur`, `Vol`, and `Power` respectively.

The following figure shows an example of the results of executing the `show power inline` operation command.

Figure 13-7 Example of displaying the status of PoE power supply [AX2200S]

```
> show power inline
Please wait a little.

Date 2012/07/03 20:46:06 UTC
System Wattage      : 370.0
Priority Control     : enable

                        < 0/1-4> <0/5-24>
Threshold(W)        : 240.0    130.0
Total Allocate(W)    : 240.0    60.8
Total Power(W)       : 210.3    2.0

Port Counts          : 24
Port Status Priority Class Alloc(mW) Power(mW) Vol(V) Cur(mA) Description
0/1 on low manual 60000 54400 53.6 1014
0/2 on high manual 60000 48600 53.7 900
0/3 on critical manual 60000 51200 53.9 949
0/4 on high manual 60000 56100 53.9 1047
0/5 on critical manual 30000 700 53.9 14
0/6 on low 0 15400 700 53.9 14
0/7 off high - 0 0 0.0 0
0/8 off high - 0 0 0.0 0
0/9 off high - 0 0 0.0 0
0/10 off high - 0 0 0.0 0
0/11 off high - 0 0 0.0 0
0/12 off high - 0 0 0.0 0
0/13 off high - 0 0 0.0 0
0/14 off high - 0 0 0.0 0
0/15 off high - 0 0 0.0 0
0/16 off high - 0 0 0.0 0
0/17 off high - 0 0 0.0 0
0/18 off high - 0 0 0.0 0
0/19 off high - 0 0 0.0 0
0/20 off high - 0 0 0.0 0
```

```

0/21 off    high    -           0           0    0.0      0
0/22 off    high    -           0           0    0.0      0
0/23 off    high    -           0           0    0.0      0
0/24 on     high    0          15400        600   53.8     13

```

>

Figure 13-8 Example of displaying the status of PoE power supply [AX1240S]

```

> show power inline
Please wait a little.

```

Date 2012/07/03 20:46:06 UTC

System Wattage:

Threshold(W) : 370.0

Total Allocate(W) : 146.6

Total Power(W) : 87.1

Priority Control : enable

Port Counts : 24

Port	Status	Priority	Class	Alloc(mW)	Power(mW)	Vol(V)	Cur(mA)	Description
0/1	on	high	0	15400	5400	51.3	107	IPphone(1001)
0/2	on	high	0	15400	5200	51.1	102	IPphone(1002)
0/3	on	high	0	15400	5100	50.9	101	IPphone(1003)
0/4	inact	high	-	0	0	0.0	0	IPphone(1004)
0/5	on	critical	4	30000	25900	50.9	510	PRINTER
0/6	off	high	-	0	0	0.0	0	
0/7	off	never	-	0	0	0.0	0	
0/8	on	high	3	15400	12400	50.9	244	
0/9	on	low	1	4000	2100	51.0	43	
0/10	off	high	-	0	0	0.0	0	
0/11	on	critical	manual	30000	18000	51.1	353	wirelessAP
0/12	off	high	-	0	0	0.0	0	
0/13	off	high	-	0	0	0.0	0	
0/14	on	high	2	7000	5900	51.0	117	
0/15	off	low	-	0	0	0.0	0	
0/16	off	high	-	0	0	0.0	0	
0/17	off	high	-	0	0	0.0	0	
0/18	off	never	-	0	0	0.0	0	
0/19	off	high	-	0	0	0.0	0	
0/20	on	high	2	7000	3800	51.1	76	
0/21	off	high	-	0	0	0.0	0	
0/22	off	high	-	0	0	0.0	0	
0/23	on	high	2	7000	3300	50.9	66	
0/24	off	high	-	0	0	0.0	0	

>

14. Link Aggregation

This chapter describes link aggregation and its use.

14.1	Description of the basic link aggregation functionality
14.2	Configuration of the basic link aggregation functionality
14.3	Description of the link aggregation extended functionality
14.4	Configuration of the link aggregation extended functionality
14.5	Operation for link aggregation

14.1 Description of the basic link aggregation functionality

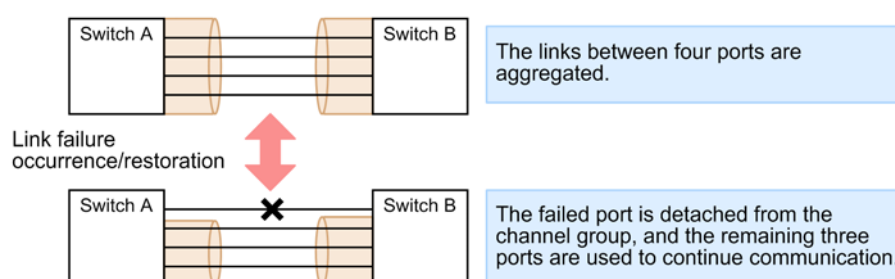
14.1.1 Overview

Link aggregation is functionality that connects devices by establishing multiple links between the Ethernet ports of each device, and that treats these links as one virtual link. The virtual link is called a *channel group*. Link aggregation can expand bandwidth and ensure redundancy between connected devices.

14.1.2 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 14-1 Example of a link aggregation configuration



14.1.3 Supported specifications

(1) Link aggregation modes

The link aggregation of the Switch supports LACP and static modes.

- LACP link aggregation

LACP link aggregation uses the LACP (Link Aggregation Control Protocol) compliant with IEEE 802.3ad. LACP link aggregation starts operation of a channel group when LACP negotiation is successful. LACP is used to verify consistency and link normality between devices.

- Static link aggregation

Static link aggregation is link aggregation manually set by using configuration commands. LACP is not used. Operation of a channel group starts when the ports in the channel group are placed in the link-up status.

The following table shows the supported specifications for link aggregation.

Table 14-1 Supported specifications for link aggregation

Item	Supported specifications	Remarks
Number of channel groups per device	8	--
Maximum number of ports per group	8	--
Link aggregation modes	LACP Static	--

Item	Supported specifications	Remarks
Transmission speed between ports	Only the same speed is used.	A slow line [#] is detached.
Duplex mode	Only full-duplex mode is supported.	--

Legend:

--: Not applicable

#

A line that is slower than the maximum speed of link-up lines.

14.1.4 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 changes.

14.1.5 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 shows the information used for port allocation.

Table 14-2 Port allocation for sending frames

Forward	Frame type	Information used for port allocation
Layer 2 forwarding	Frame for which the MAC address has not been learned yet (Broadcasts and multicasts are included.)	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

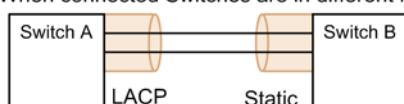
14.1.6 Notes on using link aggregation

(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.

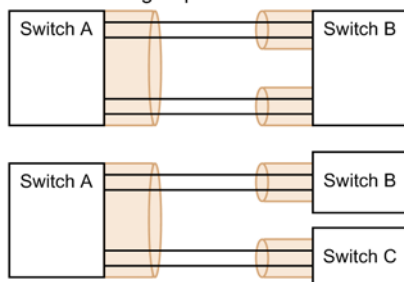
Figure 14-2 Examples of configurations in which link aggregation is not possible

- When connected Switches are in different modes



In this configuration, LACP negotiation does not succeed, preventing communication.

- When channel groups of the connected Switches are in a point-to-multipoint relationship



In this configuration, communication does not work correctly, resulting in a loop. For example, frames sent from Switch A might return to it via Switch B.

(2) About 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. After doing that, make sure that the connections between switches are not in a configuration such as those in (1) *Configurations in which link aggregation is not possible*, and then return the ports to the link-up status.

(3) If CPU load is excessive

If CPU load is excessive when LACP link aggregation mode is used, the LACPDUs (link aggregation control protocol data units) that the Switch sends or receives might be discarded, or the sending or reception might be delayed. If this situation occurs, a timeout message might be output or communication might temporarily stop. If timeouts or temporary communication interruptions frequently occur, the CPU might be overloaded. Set a longer interval for sending LACPDUs, or use static link aggregation.

14.2 Configuration of the basic link aggregation functionality

14.2.1 List of configuration commands

The following table describes the commands used to configure the basic link aggregation functionality.

Table 14-3 List of configuration commands

Command name	Description
channel-group lacp system-priority	Sets the LACP system priority for each channel group.
channel-group mode	Adds a port to a channel group.
channel-group periodic-timer	Sets the LACPDU sending interval.
description	Sets supplementary information about a channel group.
interface port-channel	Sets up a port channel interface. The parameters of a channel group are also set in port channel interface mode.
lacp port-priority	Set the LACP port priority.
lacp system-priority	Sets the default for the LACP system priority.
shutdown	Shuts down a port in a channel group to stop communication.

14.2.2 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 fastethernet 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.

14.2.3 Configuration of 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 set either `active` or `passive` mode in Ethernet interface configuration mode.

Command examples

1. `(config)# interface range fastethernet 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 LACPDUs in active mode, independently of the remote device. If `passive` mode is specified, the LACP starts sending LACPDUs only when LACPDUs are received from the remote device.

(2) Setting the system priority

The LACP system priority can be set. 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 fastethernet 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 LACPDUs to the Switch. The Switch receives LACPDUs at the set interval.

For the LACPDU sending interval, set **long** (30 seconds) or **short** (one 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** (one 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.

14.2.4 Configuration of 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 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 table below describes the commands related to port channel interface.

Table 14-4 Related commands for a port channel interface

Functionality	Command
VLAN	switchport mode
	switchport access
	switchport protocol
	switchport trunk
	switchport mac
Spanning Tree Protocol	spanning-tree portfast
	spanning-tree bpdupfilter
	spanning-tree bpduguard
	spanning-tree guard
	spanning-tree link-type
	spanning-tree port-priority
	spanning-tree cost
	spanning-tree vlan port-priority
	spanning-tree vlan cost
	spanning-tree single port-priority
	spanning-tree single cost
	spanning-tree mst port-priority
	spanning-tree mst cost
DHCP snooping	ip arp inspection limit rate
	ip arp inspection trust
	ip dhcp snooping limit rate
	ip dhcp snooping trust
	ip verify source
IEEE802.1X	dot1x port-control
	dot1x multiple-authentication

Functionality	Command
	dot1x reauthentication
	dot1x timeout reauth-period
	dot1x timeout tx-period
	dot1x timeout supp-timeout
	dot1x timeout server-timeout
	dot1x timeout keep-unauth
	dot1x timeout quiet-period
	dot1x max-req
	dot1x ignore-eapol-start
	dot1x supplicant-detection
	dot1x force-authorized
	dot1x force-authorized vlan
Uplink redundancy	switchport backup interface
	switchport backup flush request transmit
L2 Loop Detection	loop-detection
CFM	ethernet cfm enable
	ethernet cfm mep
	ethernet cfm mip

(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 Protocol, and other functionality used for channel group operations. In this example, you set up a trunk port.

Command examples

- ```
(config)# interface range fastethernet 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.

## 14 Link Aggregation

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 fastethernet 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.

### 14.2.5 Deleting a channel group

Before you remove ports from a channel group or delete an entire channel group, you must set `shutdown` in Ethernet interface configuration mode for the ports that will be removed. If you do not set `shutdown`, a communication loop might occur.

#### (1) Removing ports from a channel group

##### Points to note

You can 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 14-4 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 fastethernet 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

You can delete an entire channel group. Because the ports in the deleted channel group can operate independently, **shutdown** is set beforehand to prevent a communication loop.

An entire channel group is deleted by deleting the **interface port-channel** command. After this deletion, the **channel-group mode** configuration command is automatically deleted from each port registered in the channel group. Be careful when using the ports for another purpose because the related commands that were set for the ports by using the **interface port-channel** command before the port group was deleted remain after the removal. (For details about the related commands, see *Table 14-4 Related commands for a port channel interface.*)

### Command examples

1. `(config)# interface range fastethernet 0/1-2`  
`(config-if-range)# shutdown`  
`(config-if-range)# exit`

Sets **shutdown** for all ports in the channel group to place these ports in the link-down status so that the entire channel group can be deleted safely.

2. `(config)# no interface port-channel 3`

Deletes channel group 3. The **channel-group mode** configuration commands set for ports 0/1 and 0/2 are also deleted automatically.

## 14.3 Description of the link aggregation extended functionality

### 14.3.1 Standby link functionality

#### (1) Description

The standby link functionality replaces a faulty port with a standby port in the same channel group to maintain the number of active ports in the channel group. This functionality can prevent a reduction of available bandwidth if a fault occurs.

This functionality is available only when static link aggregation is used.

#### (2) How a standby link is selected

The maximum number of active ports in a channel group is set in configuration mode. The rest of the ports in the channel group are standby ports.

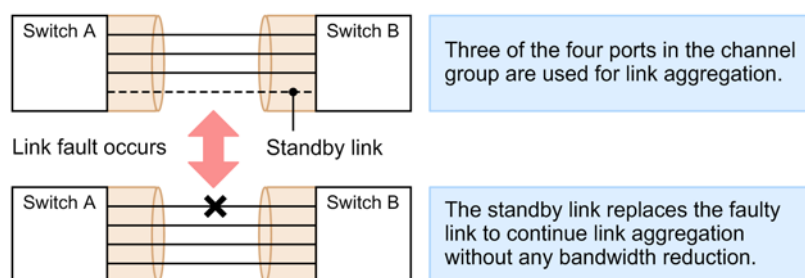
Standby ports are selected based on the port priority set in configuration mode and the port number. The following table describes the selection principle.

**Table 14-5** Standby port selection principle

| Precedence | 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 3.

**Figure 14-3** Example of standby link operation



#### (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 (standby ports) 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 in this mode, standby ports do not send data, but can receive data. A device that does not support the standby link functionality does not detect the link-down status on the partner device, and can continue sending to the partner device. In link-not-down mode, connecting to the device is possible.

In link-down mode, if there is only one active port in a channel group and a fault occurs on that port, the channel group is temporarily shut down when the faulty port is replaced with a standby port. In link-not-down mode, the standby port replaces the faulty port without the channel group shutting down.

The status in which only one port is active in a channel group arises in either of the following cases:

- The maximum number of active ports is set to 1 by using the `max-active-port` configuration command.
- Only one port has the maximum speed, and the other ports have lower speed.

#### **(4) Notes on using link-down mode**

If Fastethernet ports and Gigabitethernet ports are mixed in the same channel group, and Gigabitethernet ports are used as operating ports, use the `lacp port-priority` configuration command to set the higher priority to the Gigabitethernet ports. (A smaller port priority value indicates a higher priority.)

## 14.4 Configuration of the link aggregation extended functionality

### 14.4.1 List of configuration commands

The following table describes the commands used to configure the link aggregation extended functionality.

**Table 14-6** List of configuration commands

| Command name                          | Description                                                                                                            |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| channel-group lacp<br>system-priority | Sets the system priority for a channel group.                                                                          |
| channel-group max-active-port         | Enables the standby link functionality, and sets how many ports in the channel group can be used for link aggregation. |
| lacp port-priority                    | Sets the port priority. The port priority is used to select standby links.                                             |
| lacp system-priority                  | Sets the default value for the system priority.                                                                        |

### 14.4.2 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`  
Changes the mode to port channel interface configuration mode for channel group 3.
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 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 fastethernet 0/1`  
`(config-if)# channel-group 5 mode on`  
`(config-if)# lacp port-priority 300`  
`(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.

## 14.5 Operation for link aggregation

### 14.5.1 List of operation commands

The following table describes the operation commands for link aggregation.

**Table 14-7** List of operation commands

| Command name                        | Description                                                                      |
|-------------------------------------|----------------------------------------------------------------------------------|
| show channel-group                  | Displays link aggregation information.                                           |
| show channel-group statistics       | Displays the statistics for data packets sent and received for link aggregation. |
| show channel-group statistics lacp  | Displays the statistics for sent and received LACPDUs.                           |
| clear channel-group statistics lacp | Clears the statistics for sent and received LACPDUs.                             |

### 14.5.2 Displaying link aggregation information

#### (1) Checking the connection status for link aggregation

When the `show channel-group` operation command is executed, information about link aggregation for a channel group is displayed. In the command execution result, **CH Status** indicates the connection status of the channel group. You can use the execution result to check whether the settings are correct.

The following figure shows an example of executing the `show channel-group` operation command.

**Figure 14-4** Example of executing the show channel-group command

```
> show channel-group 8

Date 2008/11/13 10:54:25 UTC
ChGr: 8 Mode: LACP
 CH Status : Up Elapsed Time: 00:00:16
 Max Active Port: 8
 MAC address : 0012.e231.0101 VLAN ID: 100
 Actor System : Priority: 128 MAC: 00ed.f031.0001 Key: 8
 Partner System : Priority: 128 MAC: 0012.e214.ff99 Key: 8
 Port Information
 0/1 Up State: Distributing
 0/2 Up State: Distributing
 0/3 Up State: Distributing
 0/4 Up State: Distributing
 0/5 Down State: Detached
 0/6 Down State: Detached
 0/7 Down State: Detached
 0/8 Down State: Detached
 Uplink redundant
 Switchport backup pairs
 Primary Status Secondary Status Preemption Flush
 Delay Limit VLAN
 ChGr 8 Blocking Port 0/24 Forwarding 60 43 -
>
```

#### (2) Checking the operating status of each port

When the `show channel-group detail` operation command is executed, detailed status



information for 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 14-5** Example of executing the show channel-group detail command

```
> show channel-group 8 detail

Date 2008/11/13 10:55:01 UTC
ChGr: 8 Mode: LACP
 CH Status : Up Elapsed Time: 00:00:52
 Max Active Port: 8
 MAC address : 0012.e231.0101 VLAN ID: 100
 Actor System : Priority: 128 MAC: 00ed.f031.0001 Key: 8
 Partner System : Priority: 128 MAC: 0012.e214.ff99 Key: 8
 Port Information
 Port: 0/1 Up
 State: Distributing Speed: 100M Duplex: Full
 Actor Port : Priority: 128
 Partner System: Priority: 128 MAC: 0012.e214.ff99 Key: 8
 Partner Port : Priority: 128 Number: 22
 Port: 0/2 Up
 State: Distributing Speed: 100M Duplex: Full
 Actor Port : Priority: 128
 Partner System: Priority: 128 MAC: 0012.e214.ff99 Key: 8
 Partner Port : Priority: 128 Number: 21
 Port: 0/3 Up
 State: Distributing Speed: 100M Duplex: Full
 Actor Port : Priority: 128
 Partner System: Priority: 128 MAC: 0012.e214.ff99 Key: 8
 Partner Port : Priority: 128 Number: 24
 Port: 0/4 Up
 State: Distributing Speed: 100M Duplex: Full
 Actor Port : Priority: 128
 Partner System: Priority: 128 MAC: 0012.e214.ff99 Key: 8
 Partner Port : Priority: 128 Number: 23
 Port: 0/5 Down
 State: Detached Speed: - Duplex: -
 Actor Port : Priority: 128
 Port: 0/6 Down
 State: Detached Speed: - Duplex: -
 Actor Port : Priority: 128
 Port: 0/7 Down
 State: Detached Speed: - Duplex: -
 Actor Port : Priority: 128
 Port: 0/8 Down
 State: Detached Speed: - Duplex: -
 Actor Port : Priority: 128
 Uplink redundant
 Switchport backup pairs
 Primary Status Secondary Status Preemption Delay Limit Flush
 ChGr 8 Blocking Port 0/24 Forwarding 60 5 -
>
```



## **15. Layer 2 Switching Overview**

This chapter provides an overview of the Layer 2 switch functionality used to forward data over Layer 2 of the OSI model for the Switch.

---

15.1 Overview

---

15.2 Supported functions

---

15.3 Compatibility between Layer 2 switch functionality and other functionality

---

---

## 15.1 Overview

---

### 15.1.1 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.

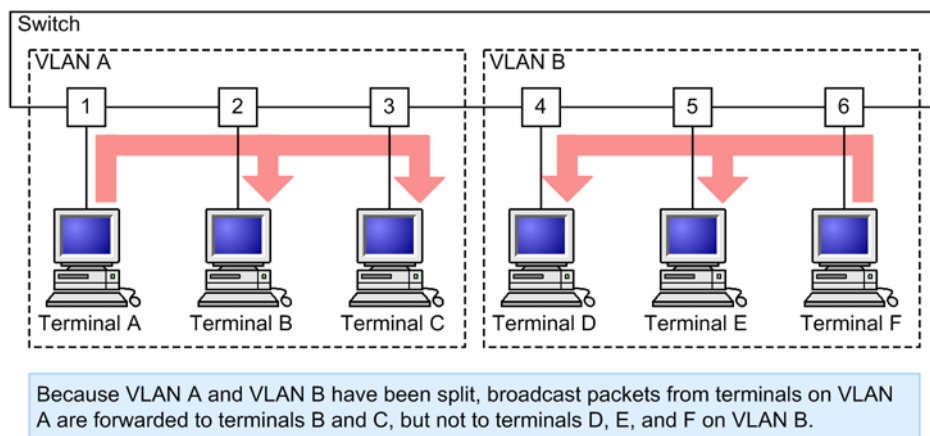
Layer 2 switches forward frames according to the entries in the MAC address table. When an entry matches the destination MAC address of a frame, the frame is forwarded to the port in the entry (however, if the port in the entry is the port on which the frame was received, the frame is not forwarded). 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*.

### 15.1.2 VLAN

VLAN functionality divides a switch into virtual groups. A switch can be internally grouped into multiple VLANs to partition broadcast domains. This allows enhanced broadcast frame control and security.

The figure below provides a VLAN overview. Because the broadcast domain is divided between VLAN A and VLAN B, no frames will arrive.

**Figure 15-1** VLAN overview



## 15.2 Supported functions

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 15-1** Supported Layer 2 switch functionality

| Supported functions                     |                                | Overview of authentication VLAN functionality                                                                            |
|-----------------------------------------|--------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| 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 anything not yet configured belongs                                                                    |
|                                         | Native VLANs                   | Another name for the port VLAN that handles untagged frames on trunk ports, protocol ports, and MAC ports                |
|                                         | L2 protocol frame transparency | The forwarding of frames with the Layer 2 protocol. Spanning Tree Protocols (BPDUs) and IEEE 802.1X (EAP) are forwarded. |
| Spanning Tree Protocol                  | 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 and 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                                                                |

## 15.3 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 lists the restrictions regarding combinations of functionality.

Note that only functionality with compatibility restrictions is shown in the table.

**Table 15-2** Restrictions on VLANs

| Functionality used          |                                                     | Functionality                   | Available             |
|-----------------------------|-----------------------------------------------------|---------------------------------|-----------------------|
| VLAN type                   | Port VLAN                                           | Layer 2 authentication          | Partial <sup>#1</sup> |
|                             |                                                     | Port mirroring (mirrored ports) | No                    |
|                             | Protocol VLAN                                       | Default VLAN                    | No                    |
|                             |                                                     | PVST+                           |                       |
|                             |                                                     | Layer 2 authentication          | Partial <sup>#1</sup> |
|                             |                                                     | Port mirroring (mirrored ports) | No                    |
|                             | MAC VLAN                                            | Default VLAN                    | No                    |
|                             |                                                     | PVST+                           |                       |
|                             |                                                     | Layer 2 authentication          | Partial <sup>#1</sup> |
|                             |                                                     | Port mirroring (mirrored ports) | No                    |
| Default VLAN                |                                                     | Protocol VLAN                   | No                    |
|                             |                                                     | MAC VLAN                        |                       |
|                             |                                                     | IGMP snooping                   |                       |
|                             |                                                     | MLD snooping                    |                       |
|                             |                                                     | Layer 2 authentication          | Partial <sup>#1</sup> |
|                             |                                                     | Port mirroring (mirrored ports) | No                    |
| Extended VLAN functionality | L2 protocol frame transparency functionality (BPDU) | PVST+                           | No                    |
|                             |                                                     | Single Spanning Tree            |                       |
|                             |                                                     | Multiple Spanning Tree          |                       |
|                             | L2 protocol frame transparency functionality (EAP)  | Layer 2 authentication          | Partial <sup>#1</sup> |

| Functionality used |                                         | Functionality          | Available             |
|--------------------|-----------------------------------------|------------------------|-----------------------|
|                    | Inter-port relay blocking functionality | Spanning Tree Protocol | Partial <sup>#2</sup> |
|                    |                                         | DHCP snooping          |                       |
|                    |                                         | IGMP snooping          |                       |
|                    |                                         | MLD snooping           |                       |
|                    |                                         | GSRP aware             |                       |
|                    |                                         | CFM                    |                       |

#1

See 5 Overview of Layer 2 Authentication in the Configuration Guide Vol. 2.

#2

See 18.3.2 Notes on using the inter-port relay blocking functionality.

**Table 15-3** Restrictions on Spanning Tree Protocols

| Functionality used     |  | Functionality                                       | Available             |
|------------------------|--|-----------------------------------------------------|-----------------------|
| PVST+                  |  | Protocol VLAN                                       | No                    |
|                        |  | MAC VLAN                                            |                       |
|                        |  | L2 protocol frame transparency functionality (BPDU) |                       |
|                        |  | Multiple Spanning Tree                              |                       |
|                        |  | Ring Protocol                                       |                       |
|                        |  | Layer 2 Authentication                              | Partial <sup>#1</sup> |
|                        |  | Uplink redundancy                                   | Partial <sup>#2</sup> |
| Single Spanning Tree   |  | L2 protocol frame transparency functionality (BPDU) | No                    |
|                        |  | Multiple Spanning Tree                              |                       |
|                        |  | Ring Protocol                                       |                       |
|                        |  | Layer 2 Authentication                              | Partial <sup>#1</sup> |
|                        |  | Uplink redundancy                                   | Partial <sup>#2</sup> |
| Multiple Spanning Tree |  | L2 protocol frame transparency functionality (BPDU) | No                    |

| Functionality used | Functionality          | Available             |
|--------------------|------------------------|-----------------------|
|                    | Single Spanning Tree   |                       |
|                    | PVST+                  |                       |
|                    | Loop guard             |                       |
|                    | Ring Protocol          |                       |
|                    | Layer 2 Authentication | Partial <sup>#1</sup> |
|                    | Uplink redundancy      | Partial <sup>#2</sup> |

#1

See 5 Overview of Layer 2 Authentication in the Configuration Guide Vol. 2.

#2

Spanning Tree Protocols are forcibly disabled for ports that have been set to the primary port or secondary port of uplink redundancy.

**Table 15-4** Restrictions on the Ring Protocol

| Functionality used | Functionality                                 | Available             |
|--------------------|-----------------------------------------------|-----------------------|
| Ring Protocol      | PVST+                                         | No                    |
|                    | Single Spanning Tree                          |                       |
|                    | Multiple Spanning Tree                        |                       |
|                    | DHCP snooping (Terminal filter functionality) | Partial <sup>#1</sup> |
|                    | Layer 2 Authentication                        | Partial <sup>#2</sup> |
|                    | Uplink redundancy                             | Partial <sup>#3</sup> |

#1

Do not use ring ports for ports on which terminal filtering is enabled by using DHCP snooping.

#2

Do not use ring ports for ports on which authentication is performed.

#3

Do not use ring ports for the primary and secondary ports providing uplink redundancy.

**Table 15-5** Restrictions on IGMP or MLD snooping

| Functionality used | Functionality          | Available                               |
|--------------------|------------------------|-----------------------------------------|
| IGMP Snooping      | Default VLAN           | No                                      |
|                    | Layer 2 Authentication | Can only be partially used <sup>#</sup> |



| Functionality used | Functionality | Available |
|--------------------|---------------|-----------|
| MLD Snooping       | Default VLAN  | No        |

#

*See 5 Overview of Layer 2 Authentication in the Configuration Guide Vol. 2*

.

---

## 16. MAC Address Learning

This chapter describes the MAC address learning functionality and its use.

---

|      |                                     |
|------|-------------------------------------|
| 16.1 | Description of MAC address learning |
|------|-------------------------------------|

|      |                                    |
|------|------------------------------------|
| 16.2 | MAC address learning configuration |
|------|------------------------------------|

|      |                                |
|------|--------------------------------|
| 16.3 | MAC address learning operation |
|------|--------------------------------|

---

## 16.1 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.

### 16.1.1 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. The registered MAC addresses are kept until they are deleted by aging processing. Learning is performed per VLAN, and the MAC address table is managed using pairs of MAC addresses and VLANs. If the MAC address is the same but the VLANs are different, they are registered as separate entries.

### 16.1.2 Aging and MAC address learning

A learned entry is deleted when no frames are received from the source MAC address within the given aging time. This prevents entries from unnecessarily accumulating. When a frame is received within the aging time, the aging timer is updated and the entry is kept. The range within which the aging time can be set is as follows:

- Aging time range: 0 or 10 to 1000000 (seconds)  
0 indicates eternity, with no aging performed.
- Default value: 300 (seconds)

At a maximum, twice the maximum aging time might be necessary for a learned entry to be deleted.

Note that if a port goes down, all entries learned for the port are deleted. Entries learned for channel groups are deleted when their channel group goes down.

### 16.1.3 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 16-1** 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.                                                                                                                                      |
| 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. |

### 16.1.4 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 16-2** Parameters specified for static entries

| # | Specified parameter                   | Description                                    |
|---|---------------------------------------|------------------------------------------------|
| 1 | MAC address                           | Specifies a unicast MAC address.               |
| 2 | VLAN                                  | Specifies the VLAN for registering this entry. |
| 3 | Specification of the destination port | Specifies one port or channel group.           |

### 16.1.5 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 16-3** When the MAC address table is cleared

| Trigger                                                    | Description                                                                                                                                                                                                                                                              |
|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port down <sup>#1</sup>                                    | Learned entries are deleted from the corresponding port.                                                                                                                                                                                                                 |
| Channel group down <sup>#2</sup>                           | Learned entries are deleted from the corresponding channel group.                                                                                                                                                                                                        |
| Execution of the clear mac-address-table operation command | The MAC address table is cleared according to the parameters.                                                                                                                                                                                                            |
| Spanning Tree topology changed                             | "Configure the Spanning Tree Protocol on the Switch."<br>The MAC address table is cleared when a topology change is detected.                                                                                                                                            |
|                                                            | "The Switch runs as a transit node in a ring network configuration using a Spanning Tree Protocol and the Ring Protocol."<br>The MAC address table is cleared when a flush control frame sent during a topology change for a switch using the Ring Protocol is received. |
| GSRP master/backup switched                                | "The Switch runs GSRP-aware."<br>The MAC address table is cleared when the GSRP Flush request frame sent when the GSRP switch becomes the master is received.                                                                                                            |
|                                                            | "The Switch runs as a transit node in a ring network configuration using GSRP and the Ring Protocol."<br>The MAC address table is cleared when the flush control frame sent when a switch using the Ring Protocol becomes the master is received.                        |

| Trigger                                                                         | Description                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Route switched by the Ring Protocol                                             | "The Switch runs as a transit node."<br>The MAC address table is cleared when the flush control frame sent from the master node when the path is switched is received.<br>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.                                                                           |
| Primary port and secondary port switched due to uplink/redundancy functionality | The MAC address table is cleared when the flush control frame sent on switching from the primary port to the secondary port or on switching back from the secondary port to the primary port is received.                                                                               |

#1

Downed ports such as those that are down due to a line failure, execution of the `inactivate` operation command, or the settings in the `shutdown` configuration command.

#2

Downed channel groups such as those that are down due to the LACP, a line failure, or the settings in the `shutdown` configuration command.

### 16.1.6 Notes

#### (1) Restrictions regarding move detection for MAC address learning

In a model that accommodates 48 or more Ethernet interface ports, when a terminal such as a PC moves between ports, the MAC address learned on the previous port might be kept in the MAC address table.

In such cases, because attempts are made to send frames to the previous port, communication might not be performed correctly.

If this problem occurs, either wait for the previous port to be deleted by learned entry aging, or use the `clear mac-address-table` operation command to delete the learned entry for the previous port.

#### (2) Restrictions regarding unicast transmission

With models that accommodate 48 or more of Ethernet interface ports, if terminals connected to ports 1 to 24, 49, or 50 are communicating using unicasts and one of those terminals receives unicast communication from a terminal connected to ports 25 to 48, the frames in the communication might be flooded to part of the VLAN.

The flooding disappears when either a multicast or broadcast is sent from the destination terminal, or when bidirectional communication is performed.

#### (3) Aging time when the Layer 2 authentication functionality is used

The aging time for learned entries can be set by the configuration. When the Layer 2 authentication functionality is used, however, the following aging time is applied.

**Table 16-4** Aging time when the Layer 2 authentication functionality is used

| Setting of Layer 2 authentication | Setting of the aging time for the MAC address table | Aging operation |            |
|-----------------------------------|-----------------------------------------------------|-----------------|------------|
|                                   |                                                     | Operation       | Aging time |
|                                   |                                                     |                 |            |

| Setting of Layer 2 authentication                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Setting of the aging time for the MAC address table | Aging operation |                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|-----------------|----------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                     | Operation       | Aging time     |
| One of the following authentication methods is enabled:<br>1. IEEE802.1X <ul style="list-style-type: none"> <li>■ Authentication mode Port-based authentication (static) or Port-based authentication (dynamic)</li> <li>■ Functionality to monitor non-communication is enabled.</li> </ul> 2. Web Authentication <ul style="list-style-type: none"> <li>■ Authentication mode Fixed VLAN mode or Dynamic VLAN mode</li> <li>■ Functionality to monitor non-communication is enabled.</li> </ul> 3. MAC-based Authentication <ul style="list-style-type: none"> <li>■ Authentication mode Fixed VLAN mode or Dynamic VLAN mode</li> <li>■ Functionality to monitor non-communication is enabled.</li> </ul> | The aging time is set to 0 seconds.                 | N               | n/a            |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | The aging time is set from 10 to 300 seconds.       | Y               | 300 seconds    |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | The aging time is set from 301 to 1000000 seconds.  | Y               | Specified time |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Not set                                             | Y               | 300 seconds    |
| All other cases                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | The aging time is set to 0 seconds.                 | N               | n/a            |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | The aging time is set from 10 to 300 seconds.       | Y               | Specified time |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | The aging time is set from 301 to 1000000 seconds.  | Y               | Specified time |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Not set                                             | Y               | 300 seconds    |

Legend:

Y: Aging is performed.

N: Aging is not performed.

n/a: Not applicable.

## 16.2 MAC address learning configuration

### 16.2.1 List of configuration commands

The following table describes the commands used to configure MAC address learning.

**Table 16-5** List of configuration commands

| Command name                 | Description                                   |
|------------------------------|-----------------------------------------------|
| mac-address-table aging-time | Sets the aging time for MAC address learning. |
| mac-address-table static     | Sets a static entry.                          |

### 16.2.2 Setting the aging time

Points to note

You can change the aging time for MAC address learning. The setting is configured for each switch. If you do not set the aging time, the aging time is set to 300 seconds.

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 also used, the aging time of 10 to 300 seconds set by this command is set to 300 seconds. For details, see (3) *Aging time when the Layer 2 authentication functionality is used* in 16.1.6 Notes.

### 16.2.3 Configuring static entries

Because address learning is not performed for a specified MAC address, static entries can be registered to avoid flooding due to MAC address aging. When static entries are set, frames are always forwarded according to the registered entries. This functionality is useful for high-traffic terminals whose ports do not move, such as servers connected directly to the Switch.

A MAC address, VLAN, and output destination are specified for a static entry. A port or channel group is specified as the destination.

#### (1) Static entries specifying a port as the output destination

Points to note

The following shows an example in which a port is specified as the output destination.

Command examples

1. `(config)# mac-address-table static 0012.e200.1122 vlan 10 interface fastethernet 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 sender MAC address 0012.e200.1122 received by a means other than port 0/1 are discarded.
2. You cannot specify a VLAN that matches the VLAN that is automatically assigned to the port by Layer 2 authentication.



**(2) Static entries specifying a link aggregation as the output destination**

## Points to note

The following shows an example in which a link aggregation is specified 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.

## 16.3 MAC address learning operation

### 16.3.1 List of operation commands

The following table describes the operation commands for MAC address learning.

**Table 16-6** List of operation commands

| Command name            | Description                                                                                                                                                                                         |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show mac-address-table  | Displays information about the MAC address table.<br>When the <code>learning-counter</code> parameter is specified, the learning address count for MAC address learning is displayed for each port. |
| clear mac-address-table | Clears the MAC address table.                                                                                                                                                                       |

### 16.3.2 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 Layer 2 authentication, IGMP snooping, and MLD snooping.

**Figure 16-1** Result of executing the show mac-address-table command

```
> show mac-address-table

Date 2009/03/16 23:24:47 UTC
Aging time : 300
MAC address VLAN Type Port-list
0000.0088.7701 2 Dynamic 0/49-50
000b.972f.e22b 2 Dot1x 0/35
0000.ef01.34f4 1000 Static 0/30
0000.ef01.3d17 1000 Static 0/30
000b.9727.ee41 1024 WebAuth 0/28
0010.c6ce.e1c6 1024 MacAuth 0/29
0012.e284.c703 1024 Dynamic 0/49-50
001b.7887.a492 1024 Dynamic 0/49-50
0100.5e00.00fc 1024 Snoop 0/49-50

>
```

### 16.3.3 Checking the MAC address learning count

The `show mac-address-table` operation command (and `learning-counter` parameter) can be used to display the number of dynamic entries registered by MAC address learning for each port, and to check the number of terminals connected per port.

When link aggregation is used, the same value is displayed for all ports in the same channel group. The displayed value is the number of learned addresses in the channel group.

**Figure 16-2** Result of executing the show mac-address-table command (with the learning-counter parameter specified)

```
> show mac-address-table learning-counter
```

```
Date 2008/11/17 15:02:38 UTC
Port Count
0/1 7
0/2 0
0/3 0
0/4 124
0/5 0
0/6 2
0/7 0
0/8 0
0/9 0
0/10 0
>
```



---

## 17. VLANs

VLAN functionality divides a switch internally into virtual groups. This chapter describes VLANs and their use.

|      |                                               |
|------|-----------------------------------------------|
| 17.1 | Description of the basic VLAN functionality   |
| 17.2 | Configuration of the basic VLAN functionality |
| 17.3 | Description of port VLANs                     |
| 17.4 | Configuring port VLANs                        |
| 17.5 | Description of protocol VLANs                 |
| 17.6 | Configuration of protocol VLANs               |
| 17.7 | Description of MAC VLANs                      |
| 17.8 | Configuration of MAC VLANs                    |
| 17.9 | VLAN operation                                |

## 17.1 Description of the basic VLAN functionality

This section provides an overview of VLANs.

### 17.1.1 VLAN type

The following table describes the types of VLAN supported by the Switch.

**Table 17-1** 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. |

### 17.1.2 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 17-2** Port type

| Port type     | Overview                                                                                                                                                                                                                                                                                  | VLANs used                             |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| Access port   | Handles an untagged frame as a port VLAN.<br>With this port, all untagged frames are handled as a single port VLAN.                                                                                                                                                                       | Port VLAN<br>MAC VLAN                  |
| Protocol port | Handles an untagged frame as a protocol VLAN.<br>With this port, the VLAN is determined by the frame protocol.<br>Tagged frames received on this port are discarded.                                                                                                                      | Protocol VLAN<br>Port VLAN             |
| MAC port      | Handles an untagged frame as a MAC VLAN.<br>With this port, the VLAN is determined by the source MAC address in the frame.<br>Handling of a tagged frame received on this port depends on the configuration setting. For details, see <i>17.7.4 Optional functionality of MAC ports</i> . | MAC VLAN<br>Port VLAN                  |
| Trunk port    | Handles all VLAN types as tagged frames.<br>With this port, the VLAN is determined by the VLAN tag.<br>An untagged frame received on this port is handled on a native VLAN.                                                                                                               | Port VLAN<br>Protocol VLAN<br>MAC VLAN |

The table below describes the types of VLANs that can be used for each port type. Trunk ports that handle all VLAN tags can use the same port on all VLANs.

**Table 17-3** 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        |

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

## (2) Native VLAN for ports

Ports other than access ports (protocol ports, MAC ports, and trunk ports) might receive frames that do not match the port setup, 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. This VLAN is called the *native VLAN* on each port.

On ports other than access 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 that cannot be specified by configuration.

### 17.1.3 Default VLAN

#### (1) Overview

The Switch allows Layer 2 forwarding immediately after startup, even when the configuration has not been set up yet. In this case, all ports are access ports belonging to VLAN ID 1, which is known as the *default VLAN*. The default VLAN always exists, and its VLAN ID of 1 cannot be changed.

#### (2) Removing ports from the default VLAN

Access ports belong to VLAN 1 (the default VLAN) when their configuration has not been set up. However, depending on the configuration, they might be excluded from automatic ownership by the default VLAN. The following ports do not automatically belong to the default VLAN:

- Ports for which anything other than VLAN 1 is specified for the access port
- Mirror ports

Ports other than access ports (protocol ports, MAC ports, and trunk ports) cannot be automatically assigned to a VLAN.

### 17.1.4 VLAN priority

#### (1) VLAN judgment priority when frames are received

When a frame is received, its VLAN is determined. The following table shows the priority for determining the VLAN.

**Table 17-4** Priority

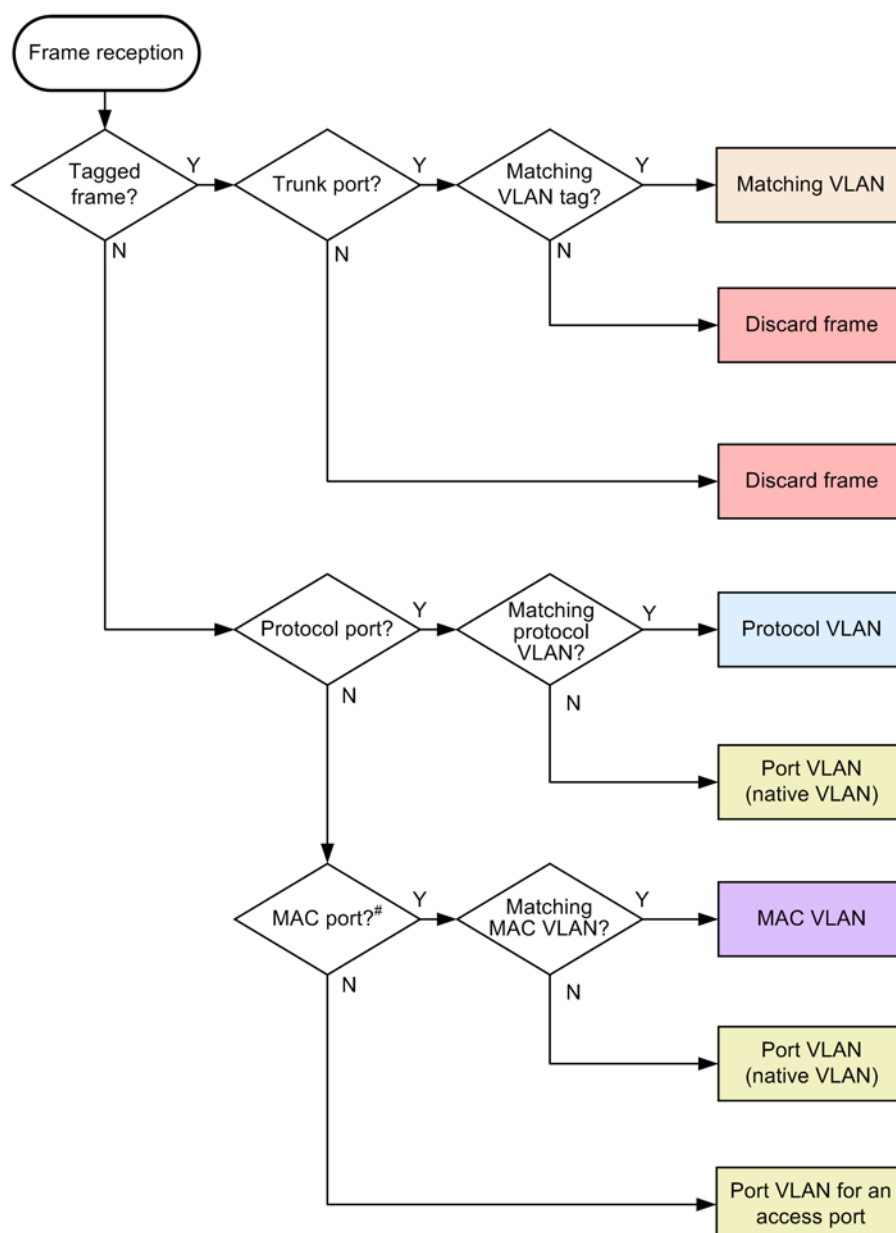
| Port type     | Priority                                                   |
|---------------|------------------------------------------------------------|
| Access port   | Port VLAN                                                  |
| Protocol port | Protocol VLAN > port VLAN (native VLAN)                    |
| MAC port      | VLAN Tag <sup>#</sup> > MAC VLAN > port VLAN (native VLAN) |
| Trunk port    | VLAN tag > port VLAN (native VLAN)                         |

#

Tagged frames can also be handled, depending on the configuration. For details, see *17.7.4 Optional functionality of MAC ports*.

The following figure shows the algorithm for determining the VLAN.



**Figure 17-1** Algorithm for determining the VLAN

#: Depending on the configuration settings, the tagged frame can also be used.

### 17.1.5 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 used on the trunk port or MAC port. VLAN tags must be recognized on the trunk ports and MAC ports on the Switch and the partner switch.

#### (2) Protocol specification

VLAN tags can embed an ID called a *tag* into an Ethernet frame. These tags are used to report VLAN information (a VLAN ID) to separate segments.

The figure below shows the tagged-frame format. There are two formats for Ethernet frames into which VLAN tag are inserted: Ethernet V2 and 802.3.

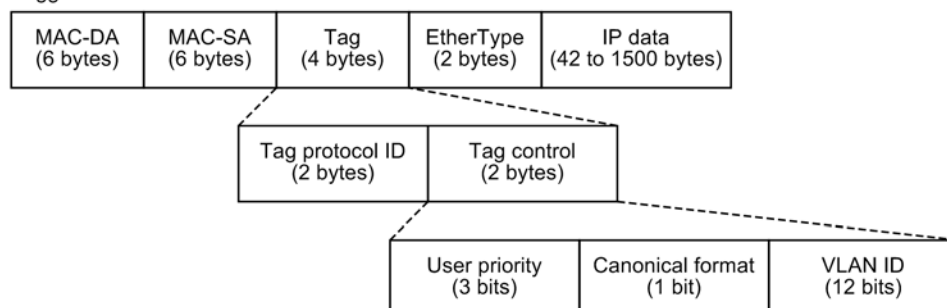
**Figure 17-2** Tagged-frame format

## ● Ethernet II frame

Normal frame

|                     |                     |                        |                               |
|---------------------|---------------------|------------------------|-------------------------------|
| MAC-DA<br>(6 bytes) | MAC-SA<br>(6 bytes) | EtherType<br>(2 bytes) | IP data<br>(46 to 1500 bytes) |
|---------------------|---------------------|------------------------|-------------------------------|

Tagged frame



## ● 802.3LLC/SNAP frame

Normal frame

|                     |                     |                     |                  |                   |                               |
|---------------------|---------------------|---------------------|------------------|-------------------|-------------------------------|
| MAC-DA<br>(6 bytes) | MAC-SA<br>(6 bytes) | Length<br>(2 bytes) | LLC<br>(3 bytes) | SNAP<br>(5 bytes) | IP data<br>(38 to 1492 bytes) |
|---------------------|---------------------|---------------------|------------------|-------------------|-------------------------------|

Tagged frame

|                     |                     |                  |                     |                  |                   |                               |
|---------------------|---------------------|------------------|---------------------|------------------|-------------------|-------------------------------|
| MAC-DA<br>(6 bytes) | MAC-SA<br>(6 bytes) | Tag<br>(4 bytes) | Length<br>(2 bytes) | LLC<br>(3 bytes) | SNAP<br>(5 bytes) | IP data<br>(34 to 1492 bytes) |
|---------------------|---------------------|------------------|---------------------|------------------|-------------------|-------------------------------|

The following table describes the fields for VLAN tags.

**Table 17-5** VLAN tag fields

| field                  | Description                                                                    | Conditions for the Switch                                                                |
|------------------------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| TPID (Tag Protocol ID) | An Ether Type value indicating that the IEEE 802.1Q VLAN tag continues         | The Switch does not support setting of TPIDs, so it operates with TPIDs fixed to 0x8100. |
| 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.                                                     |

The Switch uses the same user priority for frames forwarded that it uses for received frames. The default value of the user priority is as follows:

- When the received frame is a forwarded frame: The default value is 3.
- When the received frame is a frame originated by the Switch: The default value is 7.

Also, the user priority for sent frames can be changed by configuration. For details about how to change the user priority, see the following:

- Forwarded frames: 3.4 *Description of marking* in the *Configuration Guide Vol. 2*
- Frames originated by the Switch: 3.10 *Explanation of user priority for self-generated frames* in the *Configuration Guide Vol. 2*

## 17.1.6 Notes on VLAN usage

### (1) Notes on use with other functionality

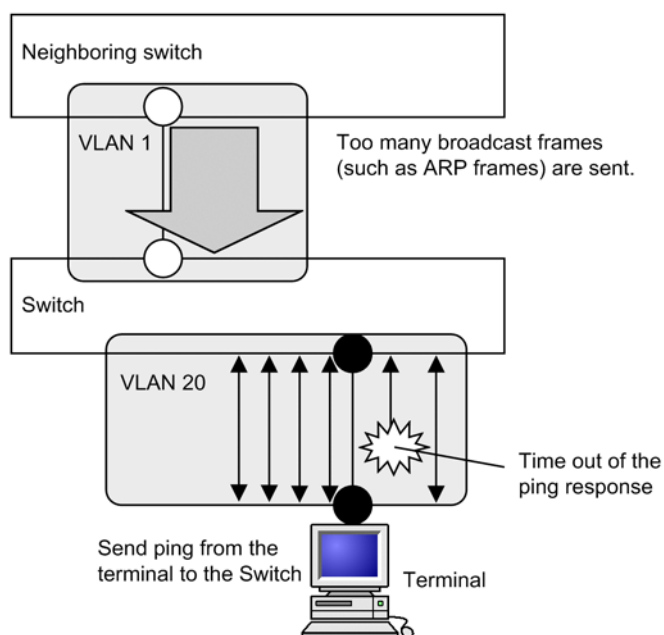
For details, see *15.3 Compatibility between Layer 2 switch functionality and other functionality*.

### (2) Using VLAN 1

If, on VLAN 1 on the Switch, reception of frames is overloaded by broadcast frames, response to a [ping](#) command on another VLAN might be affected.

The following figure shows an example when VLAN 1 is overloaded by broadcast frames.

**Figure 17-3** Example when VLAN 1 is overloaded by broadcast frames



- VLAN 1 on the Switch receives broadcast frames, such as ARP frames, from the partner switch. Another VLAN on the Switch (VLAN 20 in the above figure) receives a [ping](#) command from a remote terminal.
- If VLAN 1 is overloaded by broadcast frames, the Switch might fail to receive the [ping](#) command (ping response timeout) on another VLAN on the Switch. If this happens, use a VLAN other than VLAN 1.

## 17.2 Configuration of the basic VLAN functionality

### 17.2.1 List of configuration commands

The following table describes the commands used to configure basic VLAN functionality.

**Table 17-6** List of configuration commands

| Command name        | Description                                                                       |
|---------------------|-----------------------------------------------------------------------------------|
| name                | Sets a VLAN name.                                                                 |
| state               | Sets the VLAN status (started/stopped).                                           |
| switchport access   | Sets the access port VLAN.                                                        |
| switchport mac      | Sets MAC VLAN port information.                                                   |
| switchport mode     | Sets the type of a port (access, protocol, MAC, or trunk).                        |
| switchport protocol | Sets the VLAN for protocol ports.                                                 |
| switchport trunk    | Sets the VLAN for a trunk port.                                                   |
| vlan                | Creates a VLAN. Also, sets items pertaining to a VLAN in VLAN configuration mode. |

### 17.2.2 Configuring VLANs

#### Points to note

You can 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 switches to VLAN configuration mode. If a created VLAN is specified, only the mode is switched. The VLAN configuration mode allows VLAN parameters to be set.

Note that the following explains common settings that do not depend on the VLAN type. For details about port VLANs, protocol VLANs, and MAC VLANs, see the subsequent sections.

#### 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.

### 17.2.3 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 fastethernet 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 frame.

### 17.2.4 Setting 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 a VLAN when only the `switchport mode` configuration command has been set. The VLANs handled by this port are set using the `switchport trunk allowed vlan` configuration command.

VLANs can be added or removed by using the `switchport trunk vlan add` and `switchport trunk vlan remove` configuration commands. If the `switchport trunk allowed vlan` configuration command is executed again after having already been used to configure settings, the specified VLAN ID list is replaced.

#### Command examples

1. `(config)# vlan 10-20,100,200-300`  
`(config-vlan)# exit`  
`(config)# interface fastethernet 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 *17.4.3 Configuring native VLANs for trunk ports*.

## 17.3 Description of port VLANs

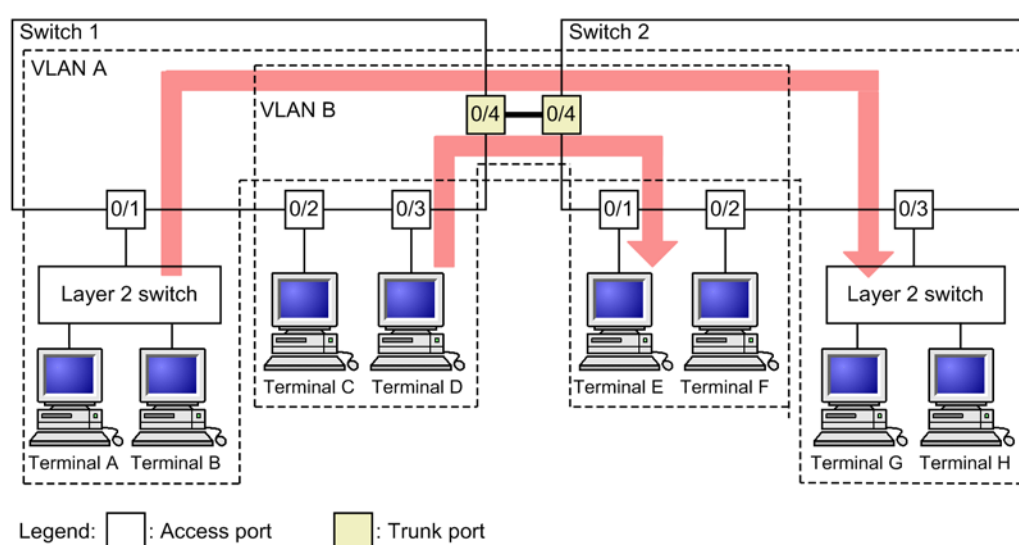
A port VLAN divides a VLAN into groups by port.

### 17.3.1 Access ports and trunk ports

A port VLAN allocates a single VLAN to a single port. The ports used for a port VLAN are set as access ports. A trunk port is used to connect multiple port VLANs to other LAN switches. Because a trunk port uses VLAN tags to identify VLANs, multiple VLANs can be set for a single port.

The figure below shows an example port VLAN configuration. Ports 0/1 to 0/3 set port VLANs as access ports. These two Switches are connected by a trunk port (port 0/4). VLAN tags are used in this case.

**Figure 17-4** Example port VLAN configuration



Multiple VLANs can be set for a trunk port. Trunk ports can distinguish VLANs by assigning VLAN tags, and then forwarding frames.

### 17.3.2 Native VLANs

Protocol ports, MAC ports, and trunk ports have a native VLAN to handle frames that do not match the configuration. The native VLAN for each port is VLAN 1 (the default VLAN) unless otherwise specified in the configuration. It can also be changed to another port VLAN.

For example, when VLAN B is set as the native VLAN for the trunk port in *Figure 17-4 Example port VLAN configuration*, VLAN B forwards untagged frames, even for the trunk port.

### 17.3.3 Notes on regarding port VLAN usage

#### (1) Note on tagged frames on access ports

Access ports handle untagged frames, discard any received tagged frames, and cannot perform transmission. Note that if the VLAN tag value matches the VLAN ID or is 0, the handling during reception is the same as for untagged frames. These frames are not sent.

## 17.4 Configuring port VLANs

### 17.4.1 List of configuration commands

The following table describes the commands used to configure port VLANs.

**Table 17-7** List of configuration commands

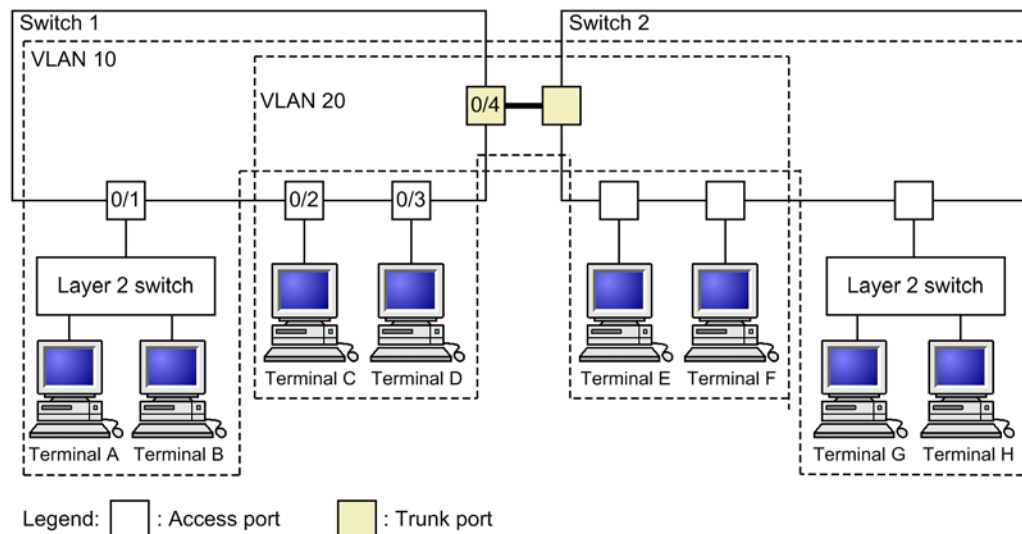
| Command name      | Description                                                                            |
|-------------------|----------------------------------------------------------------------------------------|
| switchport access | Sets the access port VLAN.                                                             |
| switchport mode   | Sets the port type (access or trunk).                                                  |
| switchport trunk  | Sets the VLAN for a trunk port.                                                        |
| vlan              | Creates a port VLAN. Also, sets items pertaining to a VLAN in VLAN configuration mode. |

### 17.4.2 Configuring a port VLAN

The following explains how to set a port VLAN. It provides example settings for Switch 1 shown in the figure below.

Port 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 17-5** Example port VLAN settings



#### (1) Creating a port VLAN

Points to note

You can 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, it is set as an access port.

Points to note

Set a port for the access port and the VLANs handled by the access port.

Command examples

1. `(config)# interface fastethernet 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 fastethernet 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

You can set the port that handles tagged frames as the trunk port, and set the VLANs for the trunk port.

Command examples

1. `(config)# interface fastethernet 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.

### 17.4.3 Configuring native VLANs for trunk ports

Points to note

You need to set a native VLAN for handling untagged frames on a trunk port. Only port VLANs can be set for a native VLAN.

When the VLAN ID of a native VLAN is specified by 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)# interface fastethernet 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.

3. 

```
(config-if)# switchport trunk allowed vlan 1,10,20
(config-if)# switchport trunk native vlan 10
(config-if)# exit
```

Sets VLAN 1, 10, and 20 for `allowed vlan` on trunk port 0/1. Sets the native VLAN to VLAN 10. VLAN 1 (default VLAN) and VLAN 20 handle tagged frames, and VLAN 10, which is a native VLAN, handles untagged frames.

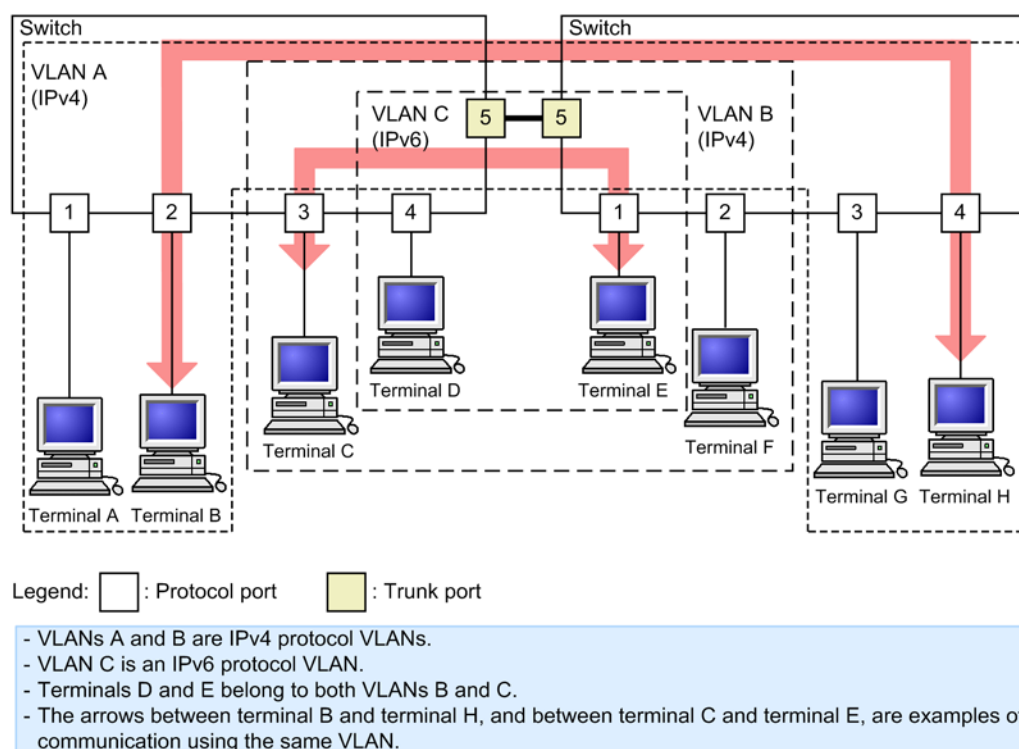
## 17.5 Description of protocol VLANs

### 17.5.1 Overview

A protocol VLAN divides VLANs by protocol. Different VLANs can be configured for each protocol, such as IPv4 and IPv6. Multiple protocols can be set for the same protocol VLAN.

The figure below shows an example protocol VLAN configuration. In the following example, VLANs A and B are configured with the IPv4 protocol, and VLAN C is configured with the IPv6 protocol.

**Figure 17-6** Example protocol VLAN configuration



### 17.5.2 Distinguishing protocols

The following table describes the three types of values that can be used to distinguish protocols.

**Table 17-8** 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 <b>AA AA 03</b> . |

Protocols are created by configuration and are associated with VLANs. Multiple protocols can be associated with a single protocol VLAN.

### 17.5.3 Protocol ports and trunk ports

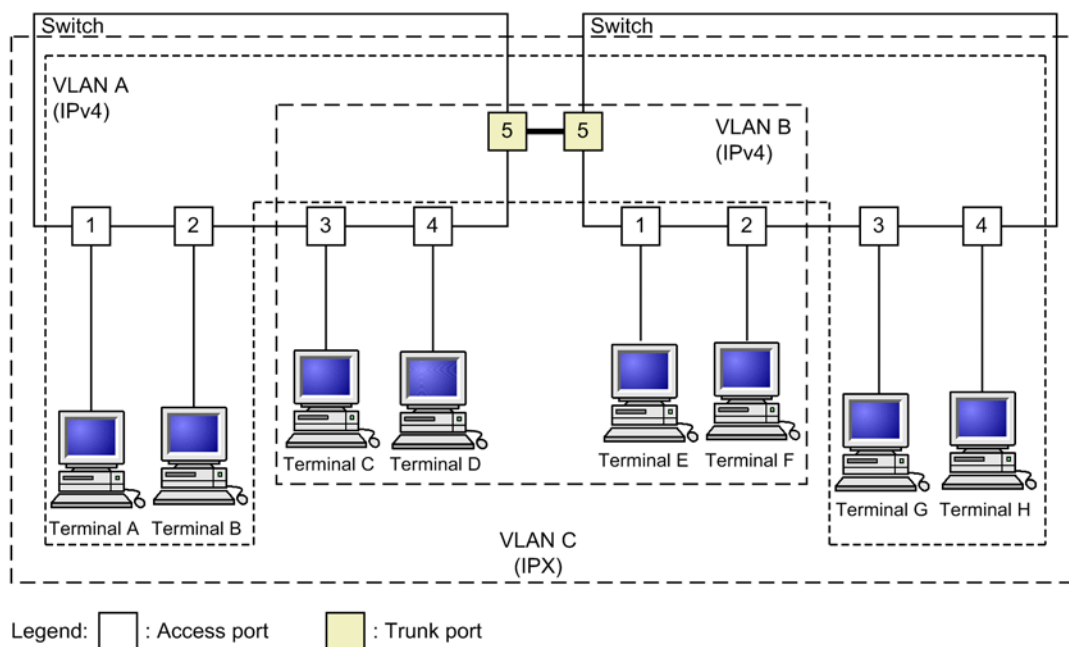
Protocol ports identify the protocol for untagged frames. Ports used as protocol VLANs set a protocol port. Different VLANs over multiple protocols can be assigned to a protocol port. Trunk ports are used to connect multiple protocol VLANs to another LAN switch. Note that because trunk ports distinguish VLANs by their VLAN tag, they do not distinguish according to protocol.

### 17.5.4 Native VLANs for protocol ports

When a frame with a protocol that does not match the configuration is received on a protocol port, it is handled by the native VLAN. The native VLAN is VLAN 1 (the default VLAN) unless otherwise specified in the configuration. It can also be changed to another port VLAN.

The figure below shows an example of a configuration in which the native VLAN is used for the protocol port. In this configuration, the IPX protocol is used for a single VLAN over the entire network, and other protocols such as IPv4 are split by VLAN for the port VLAN. VLAN A and VLAN B are set as the native VLAN for each port. Note that in this example configuration, both VLAN A and VLAN B can be set as IPv4 protocol VLANs.

**Figure 17-7** Example configuration using the native VLAN for the protocol port



- VLANs A and B are set as native VLANs on the port VLAN.
- VLAN C is an IPX protocol VLAN.
- All terminals belong to IPX protocol VLANs.
- Terminals A, B, G, and H belong to a different port VLAN than terminals C, D, E, and F.

## 17.6 Configuration of protocol VLANs

### 17.6.1 List of configuration commands

The following table describes the commands used to configure protocol VLANs.

**Table 17-9** List of configuration commands

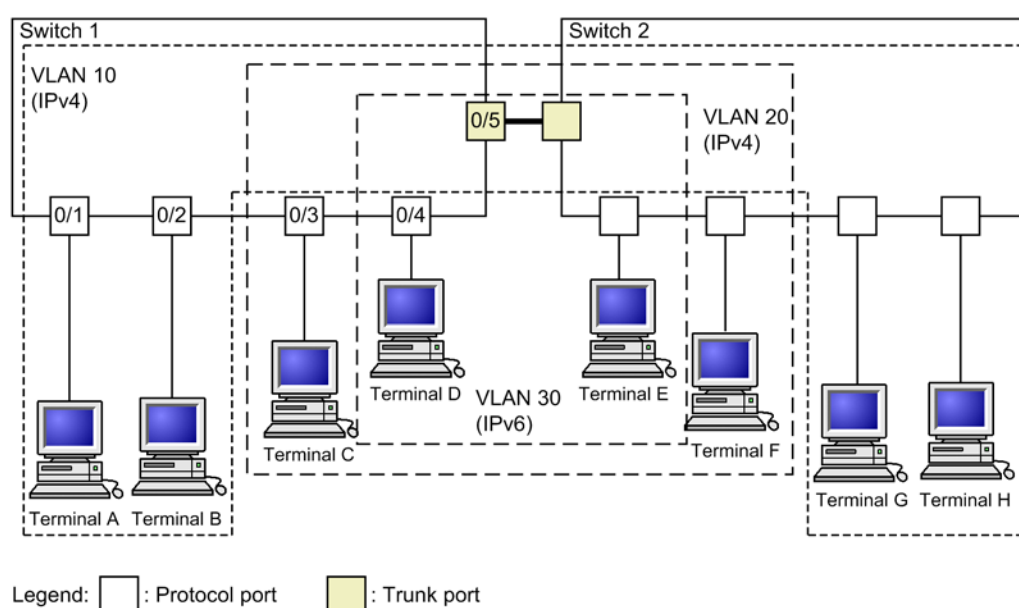
| Command name        | Description                                                                                |
|---------------------|--------------------------------------------------------------------------------------------|
| protocol            | Sets the protocol for identifying VLANs in protocol VLANs.                                 |
| switchport mode     | Sets the port type (protocol or trunk).                                                    |
| switchport protocol | Sets the VLAN for protocol ports.                                                          |
| switchport trunk    | Sets the VLAN for a trunk port.                                                            |
| vlan-protocol       | Sets the protocol name and protocol value for a protocol VLAN.                             |
| vlan protocol-based | Creates a protocol VLAN. Also, sets items pertaining to a VLAN in VLAN configuration mode. |

### 17.6.2 Creating protocol VLANs

The following explains how to set a protocol VLAN. It provides example settings for Switch 1 shown in the figure below.

Ports 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 17-8** Example settings for protocol VLANs



#### (1) Creating protocols to distinguish VLANs

Points to note

Use the `vlan-protocol` configuration command to set the distinguishing protocol

before creating a protocol VLAN. A protocol name and a protocol value are set for a protocol. Multiple protocol values can be associated with a single name.

Because the IPv4 protocol requires that both an IPv4 EtherType value and an 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 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 set to 05FF or smaller, it operates as 0000.

## (2) Creating protocol VLANs

#### Points to note

Creates 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`

Sets 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. The created IPv6 protocol is set 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 fastethernet 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 fastethernet 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 fastethernet 0/4
(config-if)# switchport protocol vlan add 30
(config-if)# exit
```

Adds VLAN 30 to port 0/4. Two types of protocol VLAN, IPv4 and IPv6 are set for port 0/4.

#### Notes

The `switchport protocol 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 protocol VLANs are already running, use the `switchport protocol vlan add` and `switchport protocol vlan remove` configuration commands.

### (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 fastethernet 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.

### 17.6.3 Configuring native VLAN for protocol ports

#### Points to note

You need to 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 set by the `switchport protocol native vlan` configuration command, it becomes the VLAN for handling untagged frames

that do not match the protocol set on the protocol port. The native VLAN is VLAN 1 (the default VLAN) unless explicitly set 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 fastethernet 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.



## 17.7 Description of MAC VLANs

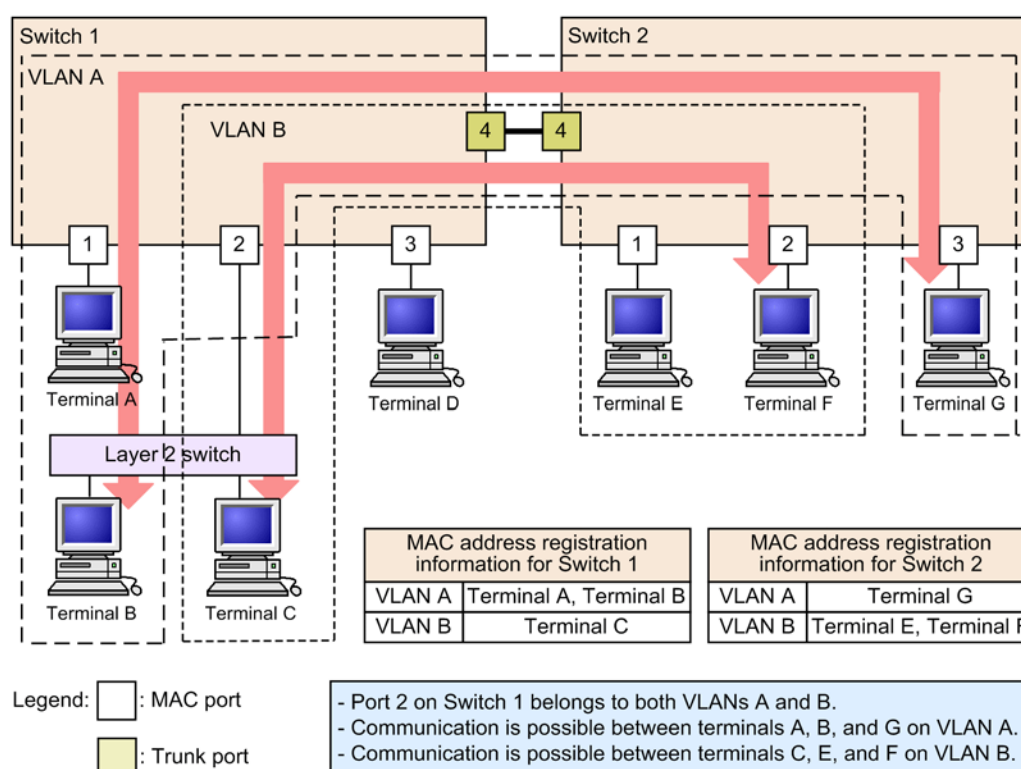
### 17.7.1 Overview

MAC VLANs divide VLAN groups by source MAC address. MAC addresses can be registered with VLANs by configuration, or dynamically through the Layer 2 authentication functionality.

MAC VLANs can be set to allow communication only with terminals permitted to connect by registering MAC addresses of permitted terminals during configuration, or by registering MAC addresses authenticated using the Layer 2 authentication functionality.

The figure below shows an example MAC VLAN configuration. When trunk ports are 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 addresses of the terminals connected to the MAC ports are set for each switch.

**Figure 17-9** Example MAC VLAN configuration

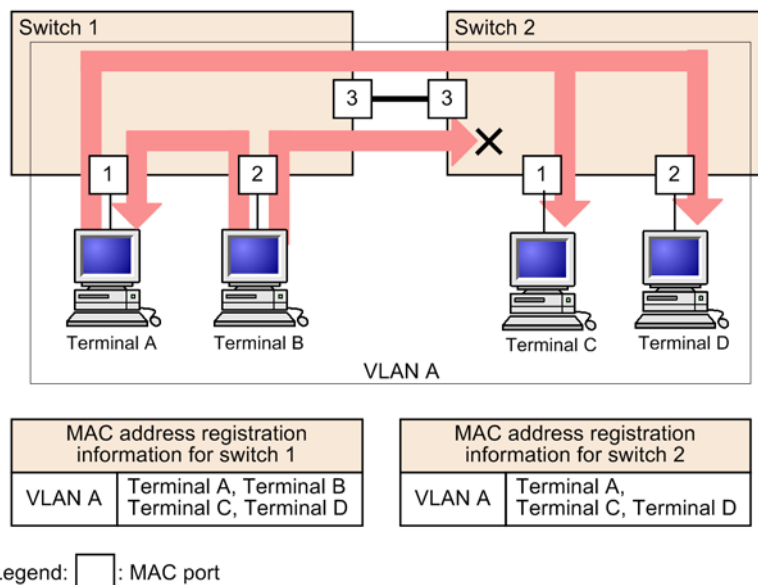


### 17.7.2 Connections between switches and MAC address settings

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 17-9 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 17-10** Switches connected by MAC ports

- Because terminal A is set on both Switch 1 and 2, it can communicate with terminal C and terminal D.
- Because there are no settings for terminal B on Switch 2, it cannot communicate with terminal C and terminal D. Communication is possible with terminal A.

### 17.7.3 Linkage with the Layer 2 authentication functionality

#### (1) Dynamically registering MAC addresses in a MAC VLAN

MAC VLANs can link with the Layer 2 authentication functionality to dynamically registered MAC addresses with a VLAN. The following are types of the Layer 2 authentication functionality that can be linked:

- IEEE 802.1X: port-based authentication (dynamic) and VLAN-based authentication (dynamic)
- Web authentication: dynamic VLAN mode and legacy mode
- MAC-based authentication: dynamic VLAN mode and legacy mode

When the same MAC address is set for the configuration and for Layer 2 authentication, the configuration MAC address is registered in the MAC VLAN.

If you want a device that supports untagged frames, such as a printer or server, to be accommodated in the specified VLAN on a MAC port without using Layer 2 authentication, use the `mac-address` configuration command to register the MAC address of the target device in a MAC VLAN.

If IEEE 802.1X port-based authentication (dynamic) or dynamic VLAN mode for Web authentication or MAC-based authentication is used, use the `mac-address-table static` configuration command to register the MAC address of the target device also in the MAC address table.

On a MAC port, tagged frames can be forwarded on a VLAN for which the `switchport mac dot1q vlan` configuration command has been set. For details about this functionality and the Layer 2 authentication functionality, see 17.7.4 *Optional functionality of MAC ports*.

For details about Layer 2 authentication, see 5 *Overview of Layer 2 Authentication* in the *Configuration Guide Vol. 2* and the description of each authentication method.

## (2) Automatic VLAN assignment for a MAC port

To set a VLAN for a MAC port, use the `switchport mac vlan` configuration command to configure the setting, or use automatic assignment by using the Layer 2 authentication functionality.

Automatic VLAN assignment operates with the following Layer 2 authentication methods:

- IEEE 802.1X:Port-based authentication (dynamic)
- Web authentication: dynamic VLAN mode
- MAC-based authentication: dynamic VLAN mode

If you used the `switchport mac vlan` configuration command to set a VLAN that had been automatically assigned to a port, cancel the automatically assigned VLAN. Authenticated terminals, however, follow the configuration that has been set, so authentication is not cancelled.

For details about automatic VLAN assignment of Layer2 authentication, see 5.4 *Functionality common to all Layer 2 authentication methods* in the *Configuration Guide Vol. 2*.

### 17.7.4 Optional functionality of MAC ports

Optionally, a MAC port can forward tagged frames with an arbitrary VLAN ID.

Use the `switchport mac dot1q vlan` configuration command to set this function. You can specify a port VLAN or MAC VLAN as a VLAN set by the `switchport mac dot1q vlan` configuration command.

You do not have to use a configuration command to register the MAC address of a device that supports tagged frames and is to be accommodated in the VLAN because the device is accommodated in the VLAN due to the VLAN tags in the frames.

#### (1) Behavior of received frames

A tagged frame that contains a VLAN ID set by the `switchport mac dot1q vlan` configuration command is forwarded to the relevant VLAN. If this command is used, the tagged frames that contain the VLAN IDs set in *Table 17-11 Configuration commands and VLAN types* are forwarded.

#### (2) Behavior of sent frames

Whether the frames have a VLAN tag differs depending on the forwarding destination of the tagged frames on the VLAN set by the `switchport mac dot1q vlan` configuration command.

**Table 17-10** Forwarding destination and handling of tagged frames

| Forwarding destination                            | Handling of tagged frames                             |
|---------------------------------------------------|-------------------------------------------------------|
| Access port                                       | After the tags are removed, untagged frames are sent. |
| Native VLANs for trunk ports                      | After the tags are removed, untagged frames are sent. |
| VLANs other than the Native VLANs for trunk ports | Tagged frames are sent.                               |
| Native VLANs for protocol ports                   | After the tags are removed, untagged frames are sent. |
| MAC VLANs for MAC ports                           | After the tags are removed, untagged frames are sent. |

| Forwarding destination                                   | Handling of tagged frames |
|----------------------------------------------------------|---------------------------|
| VLANs specified by <code>dot1q vlan</code> for MAC ports | Tagged frames are sent.   |

### (3) Notes on using the optional functionality

#### (a) Exclusive setting of VLANs

VLANs can be specified exclusively in the configuration commands below. A VLAN ID that has already been specified by one command cannot be specified by the other commands.

**Table 17-11** Configuration commands and VLAN types

| Configuration commands                  | VLAN types that can be set |
|-----------------------------------------|----------------------------|
| <code>switchport mac dot1q vlan</code>  | Port VLAN or MAC VLAN      |
| <code>switchport mac vlan</code>        | MAC VLAN                   |
| <code>switchport mac native vlan</code> | Port VLAN                  |

#### (b) Configuration command `switchport mac dot1q vlan`

This command is enabled when the `switchport mode mac-vlan` configuration command is set.

#### (c) Using with the Layer 2 authentication functionality

If the `switchport mac dot1q vlan` configuration command is set on a MAC port, untagged frames and tagged frames on the relevant VLAN and Layer 2 authentication operate as follows:

- Untagged frames and Layer 2 authentication

Untagged frames and Layer 2 authentication can be used in the same way as in *17.7.3 Linkage with the Layer 2 authentication functionality*.

- Tagged frames and Layer 2 authentication

If fixed VLAN mode of Web authentication or MAC-based authentication is set on the interface port in which the relevant VLAN is accommodated, the tagged frames that contain the VLAN IDs set in *Table 17-11 Configuration commands and VLAN types* are subject to authentication in fixed VLAN mode.

To prevent authentication in fixed VLAN mode, use the `mac-address-table static` configuration command to register the target MAC address and VLAN ID<sup>#</sup>.

<sup>#</sup>: Specify the VLAN ID that has been set by the `switchport mac dot1q vlan` configuration command.

## 17.8 Configuration of MAC VLANs

### 17.8.1 List of configuration commands

The following table describes the commands use to configure MAC VLANs.

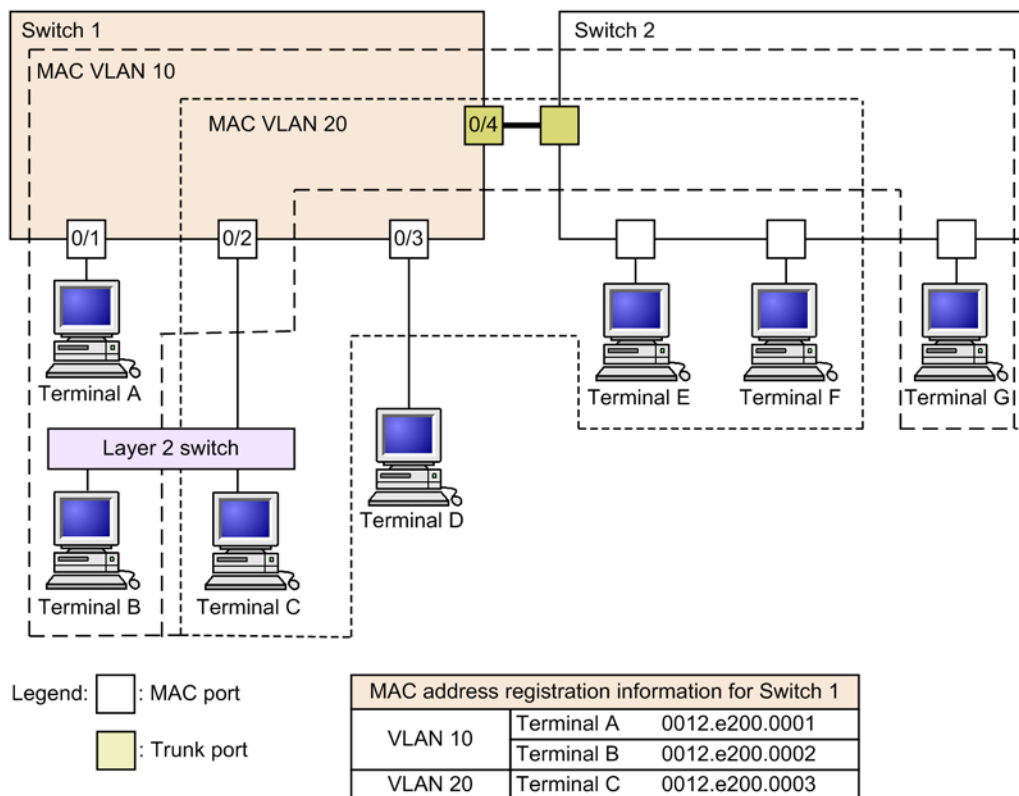
**Table 17-12** List of configuration commands

| Command name        | Description                                                                              |
|---------------------|------------------------------------------------------------------------------------------|
| mac-address         | Sets the MAC address, by configuration, for terminals belonging to VLANs for a MAC VLAN. |
| switchport mac-vlan | Sets the VLAN of a MAC port.                                                             |
| switchport mode     | Sets the port type (MAC or trunk).                                                       |
| switchport trunk    | Sets the VLAN for a trunk port.                                                          |
| vlan mac-based      | Creates a MAC VLAN. Also, sets items pertaining to a VLAN in VLAN configuration mode.    |

### 17.8.2 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 Layer 2 authentication, see *Configuration and Operation* for each authentication method in the *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 17-11** Example MAC VLAN settings

### (1) Creating MAC VLANs and registering MAC addresses

#### Points to note

You can create a MAC VLAN. When a VLAN is created, a VLAN ID and the **mac-based** parameter are specified.

As shown here, the MAC address belonging to the VLAN is also set. VLANs are registered for each terminal from A to C in the example configuration. Terminal D is not registered because communication with the MAC VLAN is not permitted for terminal D.

#### 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 fastethernet 0/1-2`

Switches ports 0/1 and 0/2 to Ethernet interface configuration mode. This setting is done because MAC VLAN 10 is set to ports 1/0 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. Then, sets VLAN 10.

3. `(config)# interface range fastethernet 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 for the MAC port. Then, sets VLAN 20. Because VLAN 10 has already been set to port 0/2, use the `switchport mac vlan add` configuration command to add VLAN 20. 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 fastethernet 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.

### 17.8.3 Configuring native VLANs for MAC ports

#### Points to note

Native VLANs are set 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 VLAN 10 and 20 as MAC VLANs. Then, creates VLAN 30 as a port VLAN.

2. `(config)# interface fastethernet 0/1`

```
(config-if)# switchport mode mac-vlan
```

Switches to the Ethernet interface configuration mode for port 0/1. Also, sets the port as a MAC port.

3. `(config-if)# switchport mac vlan 10.20`

Sets MAC VLANs 10 and 20 to port 1/0.

Port 0/1 allows only MAC VLANs 10 and 20 communications. 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 the native VLAN of port 0/1 as port VLAN 30. VLAN 30 handles untagged frames from MAC addresses not registered for port 0/1.

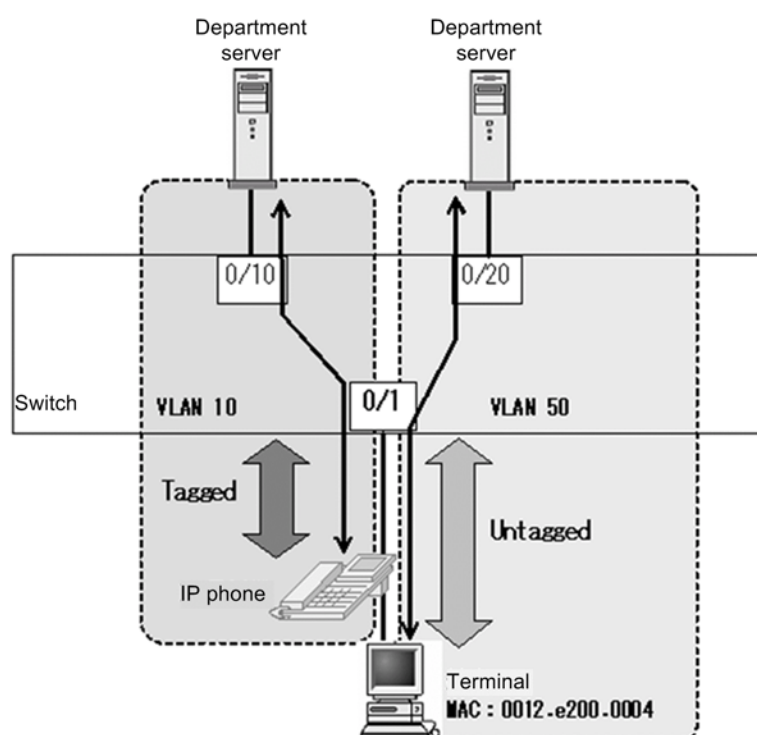
### 17.8.4 Setting forwarding of tagged frames on a MAC port

In the configuration shown in the figure below, if the Switch communicates with an IP telephone by receiving tagged frames on a port, and with a terminal under the IP telephone by receiving untagged frames on the same port, use the optional functionality for MAC ports.

In this optional functionality, if you use the `switchport mac dot1q vlan` configuration command and specify a VLAN ID to be used for forwarding of tagged frames, tagged frames and untagged frames can be forwarded on the same MAC port.

For details about the settings to authenticate IP telephones and terminals using Layer 2 authentication, see the *Configuration Guide Vol. 2*.



**Figure 17-12** Setting example of forwarding tagged frames on a MAC port**Points to note**

The example below shows how to configure a MAC port and to configure the same port to handle tagged and untagged frames. For a MAC VLAN, set the MAC address of the terminal.

- VLAN 10: The port VLAN handles tagged frames.
- VLAN 50: The MAC VLAN handles untagged frames.

**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 of the terminal belonging to VLAN 50 (0012.e200.0004).

3. `(config)# interface fastethernet 0/1`  
Switches to the Ethernet interface configuration mode for port 0/1.
4. `(config-if)# switchport mode mac-vlan`  
Specifies the port 0/1 for the MAC port.
5. `(config-if)# switchport mac dot1q vlan 10`

Configures VLAN 10 as the VLAN that handles a tagged frame 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. Note the following when using the `switchport mac dot1q vlan` configuration command:
  - Specifiable VLANs are port VLANs or MAC VLANs. VLANs that were specified by the `switchport mac vlan` or `switchport mac native vlan` configuration command cannot be specified.
  - This setting is enabled when the `switchport mode mac-vlan` configuration command is set.
2. Do not connect a device that sends BPDUs to a port for which forwarding of tagged frames has been set. (If you connect such a device to such a port, disable a Spanning Tree Protocol.)

## 17.9 VLAN operation

### 17.9.1 List of operation commands

The following table describes the VLAN operation commands.

**Table 17-13** List of operation commands

| Command name       | Description                                          |
|--------------------|------------------------------------------------------|
| show vlan          | Displays information about VLANs.                    |
| show vlan mac-vlan | Displays the MAC addresses registered for MAC VLANs. |

### 17.9.2 Checking VLAN status

#### (1) Checking the status of VLAN settings

You can check VLAN information with 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 17-13** Execution results of show vlan

```
> show vlan

Date 2009/10/28 16:32:45 UTC
VLAN counts: 5
VLAN ID: 7 Type: Port based Status: Up
 Learning: On
 BPDU Forwarding: EAPOL Forwarding:
 Router Interface Name: VLAN0007
 IP Address:
 Source MAC address: 0012.e294.aadc(System)
 Description: VLAN0007
 Spanning Tree: None(-)
 AXRP RING ID:200 AXRP VLAN group:1
 IGMP snooping: MLD snooping:
 Untagged(0) :
 Tagged(10) : 0/1,0/17-25
VLAN ID: 10 Type: Port based Status: Up
 Learning: On
 BPDU Forwarding: EAPOL Forwarding:
 Router Interface Name: VLAN0010
 IP Address:
 Source MAC address: 0012.e294.aadc(System)
 Description: VLAN0010
 Spanning Tree: None(-)
 AXRP RING ID:200 AXRP VLAN group:Control-VLAN
 IGMP snooping: MLD snooping:
 Untagged(0) :
 Tagged(9) : 0/17-25
VLAN ID: 30 Type: Protocol based Status: Down
 Protocol VLAN Information Name: "IPv4"
 EtherType: 0800,0806 LLC: Snap-EtherType:
 Learning: On
 BPDU Forwarding: EAPOL Forwarding:
 Router Interface Name: VLAN0030
 IP Address:
 Source MAC address: 0012.e294.aadc(System)
```

```

Description: PROT-VLAN0030
Spanning Tree: None(-)
AXRP RING ID: AXRP VLAN group:
IGMP snooping: MLD snooping:
Untagged(0) :
Tagged(0) :
VLAN ID: 51 Type: MAC based Status: Up
Learning: On
BPDU Forwarding: EAPOL Forwarding:
Router Interface Name: VLAN0051
IP Address:
Source MAC address: 0012.e294.aadc(System)
Description: VLAN0051
Spanning Tree: None(-)
AXRP RING ID: AXRP VLAN group:
IGMP snooping: MLD snooping:
Untagged(1) : 0/11
Tagged(0) :
VLAN ID: 4094 Type: Port based Status: Up
Learning: On
BPDU Forwarding: EAPOL Forwarding:
Router Interface Name: VLAN4094
IP Address: 192.168.0.150/24
Source MAC address: 0012.e294.aadc(System)
Description: VLAN4094
Spanning Tree: None(-)
AXRP RING ID:200 AXRP VLAN group:2
IGMP snooping: MLD snooping:
Untagged(1) : 0/14
Tagged(10) : 0/1,0/17-25

```

>

## (2) Checking the status of VLAN communication

You can check the status of VLAN communication with 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 17-14** Execution results of show vlan detail

```

> show vlan 10,4094 detail

Date 2009/10/28 16:32:49 UTC
VLAN counts: 2
VLAN ID: 10 Type: Port based Status: Up
Learning: On
BPDU Forwarding: EAPOL Forwarding:
Router Interface Name: VLAN0010
IP Address:
Source MAC address: 0012.e294.aadc(System)
Description: VLAN0010
Spanning Tree: None(-)
AXRP RING ID:200 AXRP VLAN group:Control-VLAN
IGMP snooping: MLD snooping:
Port Information
 0/17(ChGr:8) Down - Tagged
 0/18(ChGr:8) Down - Tagged
 0/19(ChGr:8) Down - Tagged
 0/20(ChGr:8) Down - Tagged
 0/21(ChGr:8) Down - Tagged
 0/22(ChGr:8) Down - Tagged

```

```

 0/23(ChGr:8) Down - Tagged
 0/24(ChGr:8) Up Forwarding Tagged
 0/25 Up Forwarding Tagged
VLAN ID: 4094 Type: Port based Status: Up
Learning: On
BPDU Forwarding: EAPOL Forwarding:
Router Interface Name: VLAN4094
IP Address: 192.168.0.150/24
Source MAC address: 0012.e294.aadc(System)
Description: VLAN4094
Spanning Tree: None(-)
AXRP RING ID:200 AXRP VLAN group:2
IGMP snooping: MLD snooping:
Port Information
 0/1 Up Forwarding Tagged
 0/14 Down - Untagged
 0/17(ChGr:8) Down - Tagged
 0/18(ChGr:8) Down - Tagged
 0/19(ChGr:8) Down - Tagged
 0/20(ChGr:8) Down - Tagged
 0/21(ChGr:8) Down - Tagged
 0/22(ChGr:8) Down - Tagged
 0/23(ChGr:8) Down - Tagged
 0/24(ChGr:8) Up Forwarding Tagged
 0/25 Up Forwarding Tagged

```

&gt;

### (3) Checking the VLAN ID list

You can use the `show vlan summary` operation command to check the set VLAN types, as well as their count and VLAN IDs.

**Figure 17-15** Execution results of show vlan summary

```

>show vlan summary

Date 2009/10/28 16:32:16 UTC
Total(5) : 7,10,30,51,4094
Port based(3) : 7,10,4094
Protocol based(1) : 30
MAC based(1) : 51

```

&gt;

### (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 statuses of VLAN settings, Layer 2 redundancy functionality, and IP address settings. Also, a VLAN, port, or channel group can be specified as a parameter to check a list of only the VLAN statuses specified for the parameter.

**Figure 17-16** Execution results of show vlan list

```

> show vlan list

Date 2009/10/28 16:31:47 UTC
VLAN counts: 5

```

| ID | Status | Fwd/Up | /Cfg | Name            | Type  | Protocol | Ext. | IP |
|----|--------|--------|------|-----------------|-------|----------|------|----|
| 7  | Up     | 3/     | 3/   | 10 VLAN0007     | Port  | AXRP (-) | -    | -  |
| 10 | Up     | 2/     | 2/   | 9 VLAN0010      | Port  | AXRP (C) | -    | -  |
| 30 | Down   | 0/     | 0/   | 0 PROT-VLAN0030 | Proto | -        | -    | -  |
| 51 | Up     | 1/     | 1/   | 1 VLAN0051      | MAC   | -        | -    | -  |

## 17 VLANs

```
4094 Up 3/ 3/ 11 VLAN4094 Port AXRP (-) - 4
 AXRP (C:Control-VLAN)
 S:IGMP/MLD snooping
 4:IPv4 address configured

>
```

### (5) Checking MAC addresses registered for MAC VLANs

You can use the `show vlan mac-vlan` operation command 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` are MAC addresses registered by Layer 2 authentication.

**Figure 17-17** Execution results of `show vlan mac-vlan`

```
> show vlan mac-vlan

Date 2008/11/17 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. Extended VLAN Functionality

This chapter describes the VLAN extended functionality and its use.

|      |                                                              |
|------|--------------------------------------------------------------|
| 18.1 | Description of L2 protocol frame transparency functionality  |
| 18.2 | Configuring the L2 protocol frame transparency functionality |
| 18.3 | Description of the inter-port relay blocking functionality   |
| 18.4 | Configuration of the inter-port relay blocking functionality |
| 18.5 | Operation for the VLAN extended functionality                |

## 18.1 Description of L2 protocol frame transparency functionality

### 18.1.1 Overview

L2 protocol frame transparency functionality forwards Layer 2 protocol frames. The frames that are forwarded include Spanning Tree BPDUs, and EAPOL for IEEE 802.1X. Usually, protocol frames for these layers are not forwarded.

The frames forwarded are handled as simple multicast frames on the Switch, and are not used as protocols by the Switch.

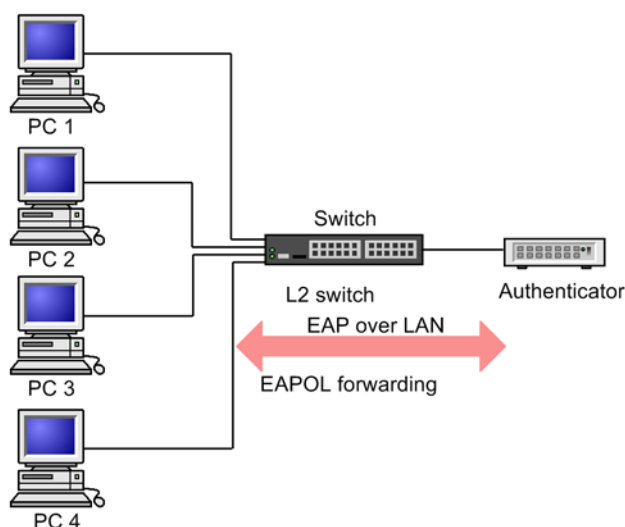
#### (1) BPDU forwarding functionality

The Switch can forward BPDUs when Spanning Tree Protocols are not used.

#### (2) EAPOL forwarding

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 18-1** Example application of EAPOL forwarding





## 18.2 Configuring the L2 protocol frame transparency functionality

### 18.2.1 List of configuration commands

The following table describes the commands used to configure the L2 protocol frame transparency functionality.

**Table 18-1** List of configuration commands

| Command name          | Description                            |
|-----------------------|----------------------------------------|
| l2protocol-tunnel eap | Forwards EAPOL frames for IEEE 802.1X. |
| l2protocol-tunnel stp | Forwards Spanning Tree BPDUs.          |

### 18.2.2 Configuring the L2 protocol frame transparency functionality

#### (1) Setting BPDU forwarding functionality

Points to note

The settings for this functionality take effect for each switch. When set, BPDUs are forwarded for all VLANs.

BPDU forwarding functionality needs to be set after stopping the Spanning Tree Protocol for the Switch.

Command examples

1. `(config)# spanning-tree disable`  
`(config)# l2protocol-tunnel stp`

Sets BPDU forwarding functionality. The Spanning Tree Protocol is stopped first, and then the BPDU forwarding functionality is set. The Switch forwards BPDUs without handling them as protocol frames.

#### (2) Setting EAPOL forwarding functionality

Points to note

The settings for this functionality take effect for each switch. When set, EAPOL frames are forwarded for all VLANs.

EAPOL forwarding and IEEE 802.1X cannot be used at the same time.

Command examples

1. `(config)# l2protocol-tunnel eap`

Sets EAPOL forwarding functionality. The Switch forwards EAPOL frames without handling them as protocol frames.

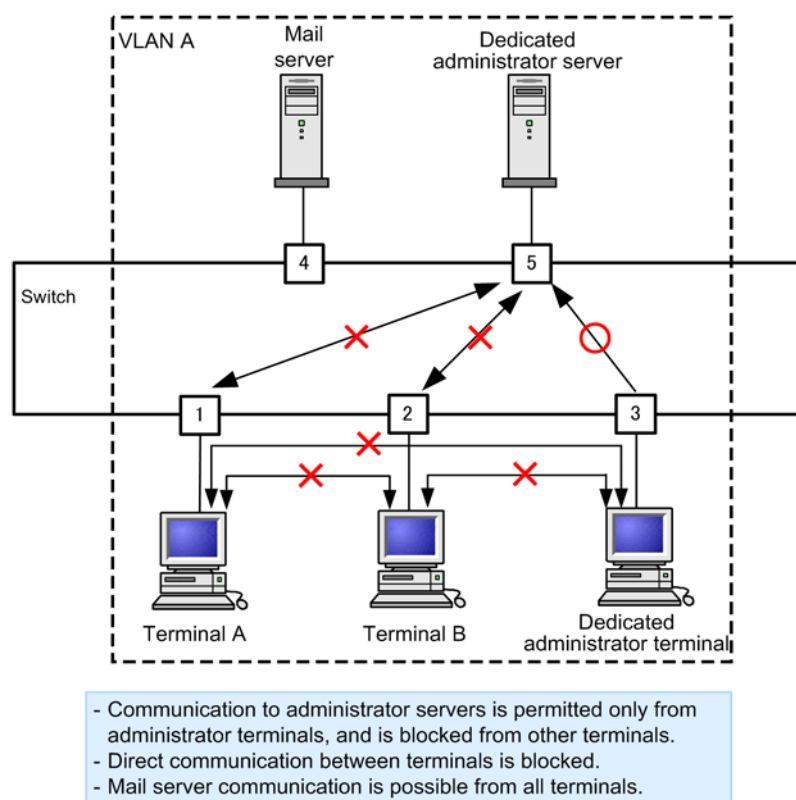
## 18.3 Description of the inter-port relay blocking functionality

### 18.3.1 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, the administrator server blocks access from normal terminals, allowing access only from the administrator terminal. Also, direct communication between terminals is blocked, to enhance the security of each terminal.

**Figure 18-2** Example application of the inter-port relay blocking functionality



### 18.3.2 Notes on using the inter-port relay blocking functionality

#### (1) Ports to be blocked

The inter-port relay blocking operates on ports that are not registered in channel groups.

#### (2) Notes on use with other functionality

The following table describes the operation when inter-port relay blocking is used concurrently with other functionality.

**Table 18-2** Concurrent use of inter-port relay blocking and other functionality

| Functionality          | Operation                                                                                                                                              |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Spanning Tree Protocol | When a Spanning Tree Protocol is run on a port that is blocking communication, communication might not be possible anymore, depending on the topology. |

| Functionality | Operation                                                                                                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DHCP snooping | Operating DHCP snooping on a port that is blocking communication disables the inter-port relay blocking for DHCP frames (and ARP frames when dynamic ARP inspection is valid), so that these frames are forwarded. |
| IGMP Snooping | Operating IGMP snooping on a port that is blocking communication disables the inter-port relay blocking for IGMP frames, so that these frames are forwarded.                                                       |
| MLD Snooping  | Operating MLD snooping on a port that is blocking communication disables inter-port relay blocking for MLD frames, so that these frames are forwarded.                                                             |
| GSRP aware    | Operating GSRP on a port that is blocking communication disables inter-port relay blocking for GSRP aware frames, so that these frames are forwarded.                                                              |
| CFM           | Operating CFM on a port that is blocking communication disables inter-port relay blocking for CFM frames, so that these frames are forwarded.                                                                      |

## 18.4 Configuration of the inter-port relay blocking functionality

### 18.4.1 List of configuration commands

The following table describes the command used to configure the inter-port relay blocking functionality.

**Table 18-3** List of configuration commands

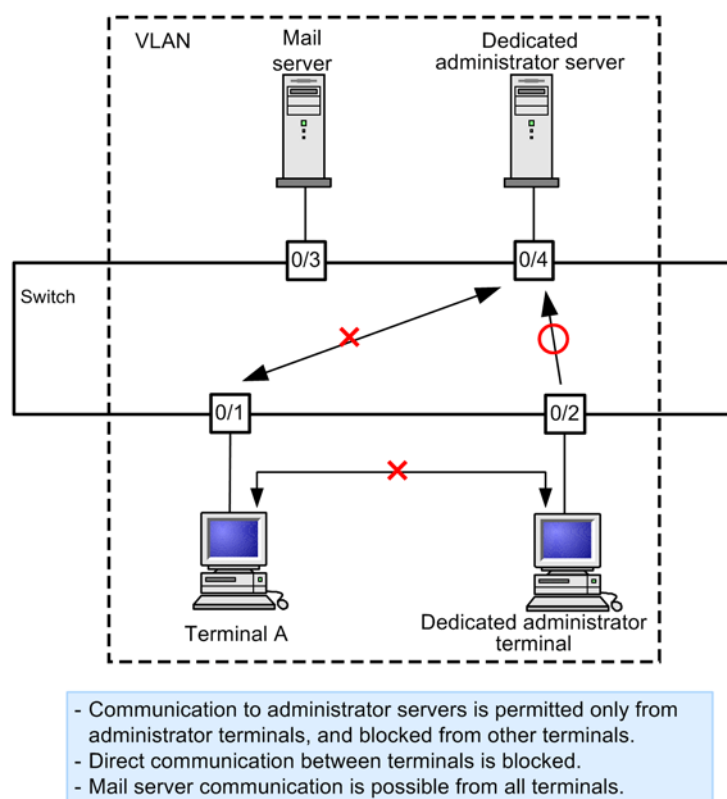
| Command name         | Description                              |
|----------------------|------------------------------------------|
| switchport isolation | Blocks forwarding to the specified port. |

### 18.4.2 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 18-3** Example settings for the inter-port relay blocking functionality



#### Points to note

The inter-port relay blocking functionality is set using the Ethernet interface configuration mode by specifying a port to which communication from other ports is not allowed. For each port to be blocked, communication needs to be blocked in both directions.

#### Command examples

- `(config)# interface fastethernet 0/1`

Switches to the Ethernet interface configuration mode for port 0/1.

2. 

```
(config-if)# switchport isolation interface fastethernet 0/2,0/4
(config-if)# exit
```

Blocks forwarding from ports 0/2 and 0/4 on port 0/1. This setting blocks one-way forwarding of transmissions to port 0/1.

3. 

```
(config)# interface fastethernet 0/2
(config-if)# switchport isolation interface fastethernet 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 fastethernet 0/4
(config-if)# switchport isolation interface fastethernet 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.

### 18.4.3 Changing blocked ports

Points to note

The `switchport isolation add` and `switchport isolation remove` configuration commands are used to change the ports blocked by the inter-port relay blocking functionality. When the `switchport isolation interface fastethernet <IF#>` or `switchport isolation interface gigabitethernet <IF#>` configuration command is used to batch specify ports already set, the specified settings are replaced.

Command examples

1. 

```
(config)# interface fastethernet 0/1
(config-if)# switchport isolation interface fastethernet 0/2-10
```

Switches to the Ethernet interface configuration mode for port 0/1, and blocks ports 0/2 to 0/10 from forwarding to port 0/1.

2. 

```
(config-if)# switchport isolation interface add fastethernet 0/11
(config-if)# switchport isolation interface remove fastethernet 0/5
```

Adds port 0/11 and removes the port 0/5 setting. Now ports 0/2 to 0/4 and ports 0/6 to 0/11 are blocked from communicating with port 0/1.

3. 

```
(config-if)# switchport isolation interface fastethernet 0/3-4
(config-if)# exit
```

Sets ports 0/3 to 0/4 as ports to be blocked. All previous settings are overwritten. Ports 0/3 to 0/4 are blocked from forwarding to port 0/1, but communication remains possible on other ports.

## 18.5 Operation for the VLAN extended functionality

### 18.5.1 List of operation commands

The following table describes the operation command for the VLAN extended functionality.

**Table 18-4** List of operation commands

| Command name | Description                                                            |
|--------------|------------------------------------------------------------------------|
| show vlan    | Checks the status of the settings for the VLAN extended functionality. |

### 18.5.2 Checking VLAN extended functionality

#### (1) Checking the status of VLAN communication

You can use the `show vlan detail` operation command to check the status of the settings for the VLAN extended functionality. The following table describes how to use the `show vlan detail` operation command to check the VLAN extended functionality.

**Table 18-5** Using the show vlan detail command to check VLAN extended functionality

| Functionality                                | How to check                                                                                       |
|----------------------------------------------|----------------------------------------------------------------------------------------------------|
| L2 protocol frame transparency functionality | Information is displayed in <a href="#">BPDU Forwarding</a> and <a href="#">EAPOL Forwarding</a> . |

**Figure 18-4** Execution results of show vlan detail

```
> show vlan 10,4094 detail

Date 2009/10/28 16:32:49 UTC
VLAN counts: 2
VLAN ID: 10 Type: Port based Status: Up
 Learning: On
 BPDU Forwarding: EAPOL Forwarding:
 Router Interface Name: VLAN0010
 IP Address:
 Source MAC address: 0012.e294.aadc(System)
 Description: VLAN0010
 Spanning Tree: None(-)
 AXRP RING ID:200 AXRP VLAN group:Control-VLAN
 IGMP snooping: MLD snooping:
 Port Information
 0/17(ChGr:8) Down - Tagged
 0/18(ChGr:8) Down - Tagged
 0/19(ChGr:8) Down - Tagged
 0/20(ChGr:8) Down - Tagged
 0/21(ChGr:8) Down - Tagged
 0/22(ChGr:8) Down - Tagged
 0/23(ChGr:8) Down - Tagged
 0/24(ChGr:8) Up Forwarding Tagged
 0/25 Up Forwarding Tagged
VLAN ID: 4094 Type: Port based Status: Up
 Learning: On
 BPDU Forwarding: EAPOL Forwarding:
 Router Interface Name: VLAN4094
 IP Address: 192.168.0.150/24
 Source MAC address: 0012.e294.aadc(System)
```

```
Description: VLAN4094
Spanning Tree: None(-)
AXRP RING ID:200 AXRP VLAN group:2
IGMP snooping: MLD snooping:
Port Information
 0/1 Up Forwarding Tagged
 0/14 Down - Untagged
 0/17(ChGr:8) Down - Tagged
 0/18(ChGr:8) Down - Tagged
 0/19(ChGr:8) Down - Tagged
 0/20(ChGr:8) Down - Tagged
 0/21(ChGr:8) Down - Tagged
 0/22(ChGr:8) Down - Tagged
 0/23(ChGr:8) Down - Tagged
 0/24(ChGr:8) Up Forwarding Tagged
 0/25 Up Forwarding Tagged
```

&gt;





---

# 19. Spanning Tree Protocol

This chapter describes the Spanning Tree functionality and its use.

|                                                               |
|---------------------------------------------------------------|
| 19.1 Overview of Spanning Tree Protocols                      |
| 19.2 Configuration of the Spanning Tree operating mode        |
| 19.3 Description of PVST+                                     |
| 19.4 PVST+ configuration                                      |
| 19.5 PVST+ operation                                          |
| 19.6 Description of Single Spanning Tree                      |
| 19.7 Configuration of Single Spanning Tree                    |
| 19.8 Operation for Single Spanning Tree                       |
| 19.9 Description of Multiple Spanning Tree                    |
| 19.10 Configuration of Multiple Spanning Tree                 |
| 19.11 Operation for Multiple Spanning Tree                    |
| 19.12 Description of common Spanning Tree functionality       |
| 19.13 Configuration of the common Spanning Tree functionality |
| 19.14 Operation for common Spanning Tree functionality        |

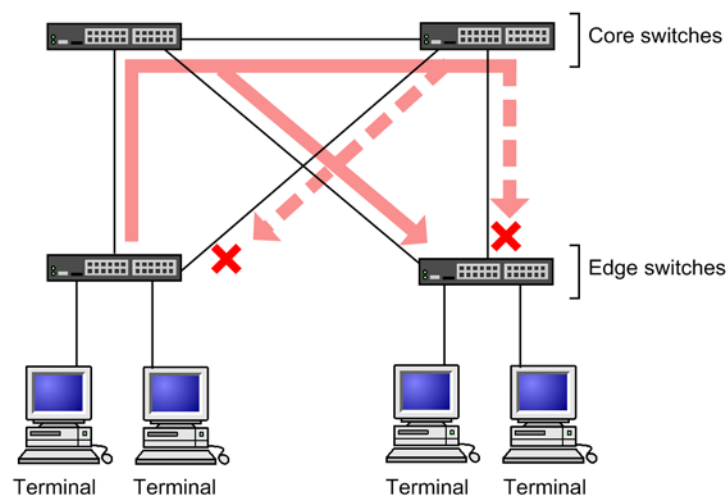
## 19.1 Overview of Spanning Tree Protocols

### 19.1.1 Overview

The Spanning Tree Protocol is a Layer 2 loop prevention protocol. The Spanning Tree Protocol can be used to make Layer 2 networks redundant, and prevent loops.

The following figure provides an overview of a network with a Spanning Tree Protocol applied.

**Figure 19-1** 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 to an alternate path when a fault occurs on the normal communication path.

A Layer 2 loop configuration is one in which a Layer 2 network is made redundant. Layer 2 loops cause broadcast storms and destabilize MAC address learning. Spanning Tree Protocols 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.

### 19.1.2 Types of Spanning Tree Protocols

The Switch supports three types of Spanning Tree Protocols: PVST+, Single Spanning Tree, and Multiple Spanning Tree. Each Spanning Tree Protocol is built differently. The following table provides an overview of the types of Spanning Tree Protocols.

**Table 19-1** Types of Spanning Tree Protocols

| Model 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 | At the switch level | 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. |

| Model name             | Build unit       | Overview                                                                                                                                                                                                          |
|------------------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Multiple Spanning Tree | Per-MST-instance | This kind of Spanning Tree Protocol is built by groups of multiple VLANs, called <i>MST instances</i> . If multiple VLANs belong to a single port, different tree build results are applied to each MST instance. |

The Switch allows the above Spanning Tree Protocols to be used as standalone or together. The following table describes which Spanning Tree combinations can be applied.

**Table 19-2** Spanning Tree combinations and applicability

| Tree building condition                       | Applicable topology calculation results                                                                                                                                                                 |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Standalone PVST+                              | A Spanning Tree Protocol for each VLAN is applied to VLANs for which PVST+ is running. The Spanning Tree Protocol is not applied to other VLANs.<br>PVST+ runs by default on port VLANs for the Switch. |
| Standalone Single Spanning Tree               | Single Spanning Tree is applied to all VLANs.<br>All PVST+ instances are stopped in this configuration.                                                                                                 |
| Combination of PVST+ and Single Spanning Tree | A Spanning Tree Protocol for each VLAN is applied to VLANs for which PVST+ is running. Single Spanning Tree is applied to other VLANs.                                                                  |
| Standalone Multiple Spanning Tree             | Multiple Spanning Tree is applied to all VLANs.                                                                                                                                                         |

Note: Multiple Spanning Tree cannot be used in combination with other trees.

### 19.1.3 Spanning Tree Protocols and rapid Spanning Tree Protocols

There are two types of PVST+ and Single Spanning Tree: IEEE 802.1D Spanning Tree Protocols and IEEE 802.1w rapid Spanning Tree Protocols. These are called *PVST+* and *Rapid PVST+*, and *STP* and *Rapid STP*.

When a communication path changes, the topology calculation for the Spanning Tree Protocol immediately puts the port in Blocking status (communication is not possible), switches to multiple statuses, and then puts it in Forwarding status (communication is possible). Because IEEE 802.1D Spanning Tree Protocols perform this status transition by a timer, a set time is required until communication is possible. IEEE 802.1w rapid Spanning Tree Protocols omit this timer-based waiting time for status transitions to perform high-speed status transitions, minimizing the time for which communication is stopped due to topology changes.

Note that because Multiple Spanning Tree is standardized under IEEE 802.1s, the status transition times is the same as for IEEE 802.1w. The following table describes the status transitions for each protocol, and their corresponding required times.

**Table 19-3** Status transitions for PVST+ and STP (Single Spanning Tree)

| Status  | Status overview                                                                                            | Transition to the next status |
|---------|------------------------------------------------------------------------------------------------------------|-------------------------------|
| Disable | Status in which a port cannot be used. This transitions to Blocking as soon as the port becomes available. | n/a                           |

| Status     | Status overview                                                                                                                                                                                                                    | Transition to the next status                 |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Blocking   | Status in which communication is not possible. In this status, MAC address learning is not performed. This is the status after link-up or of ports after topology stabilization and blocking.                                      | 20 seconds (variable) or until BPDU reception |
| Listening  | Status in which communication is not possible. In this status, MAC address learning is not performed. This is the duration until the topology stabilizes before the corresponding port is learned.                                 | 15 seconds (variable)                         |
| Learning   | Status in which communication is not possible. In this case, however, MAC address learning is performed. This is the duration for which MAC address learning is performed before the corresponding port transitions to Forwarding. | 15 seconds (variable)                         |
| Forwarding | Status in which communication is possible. In this case, the topology is stable.                                                                                                                                                   | n/a                                           |

Legend n/a: Not applicable

**Table 19-4** Status transitions for Rapid PVST+ and Rapid STP (Single Spanning Tree)

| Status     | Status overview                                                                                                                                                                                                                    | Transition to the next status    |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| Disable    | Status in which a port cannot be used. This transitions to Discarding as soon as the port becomes available.                                                                                                                       | n/a                              |
| Discarding | Status in which communication is not possible. In this status, MAC address learning is not performed. This is the duration until the topology stabilizes before the corresponding port is learned.                                 | Omitted or 15 seconds (variable) |
| Learning   | Status in which communication is not possible. In this case, however, MAC address learning is performed. This is the duration for which MAC address learning is performed before the corresponding port transitions to Forwarding. | Omitted or 15 seconds (variable) |
| Forwarding | Status in which communication is possible. In this case, the topology is stable.                                                                                                                                                   | n/a                              |

Legend n/a: Not applicable

With Rapid PVST+ and Rapid STP, the Discarding and Learning statuses are skipped by BPDU reception from the partner switch. This enables high-speed topology changes.

When using a rapid Spanning Tree Protocol, set it according to the conditions described below. If these conditions are not satisfied, discarding and learning might not be skipped, and high-speed status transitions might not be performed.

- The entire topology is built using the same protocol (Rapid PVST+ or Rapid STP). For details about reciprocal connections for Rapid PVST+ and Rapid STP, see *19.3.2 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.

### 19.1.4 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 19-5** 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 for forwarding frames from the root bridge.                |

#### (2) Port role

The table below describes port roles. Ports on designated bridges have three types of roles. For root bridges, all ports are designated ports.

**Table 19-6** Port role

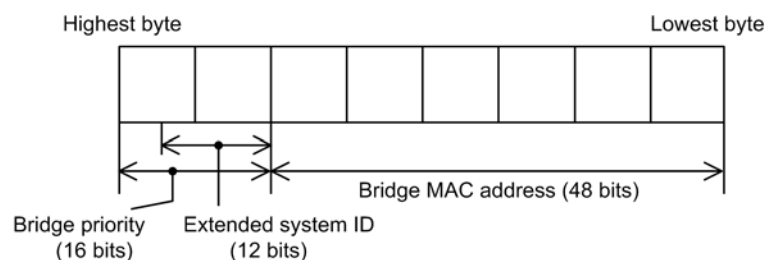
| Port role           | Overview                                                                                                                                                       |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 parameter that identifies a switch in a topology is called a *bridge ID*. The switch that has the lowest bridge ID has the highest priority, and is selected as the root bridge.

Bridge IDs consist of a bridge priority (16 bits) and the bridge MAC address (48 bits). The lowest 12 bits of a bridge priority is the extended system ID. For an extended system ID, 0 is set for Single Spanning Tree or Multiple Spanning Tree, and the VLAN ID is set for PVST+. The following figure shows a bridge ID.

**Figure 19-2** Bridge ID



#### (4) Path cost

A value corresponding to the communication speed of each port on a switch is called the *path cost*. The total value of the port costs for all intermediate ports from a designated bridge to the root bridge is called the *root path cost*. If there are multiple paths to the root bridge, the root path cost is that of the shortest path.

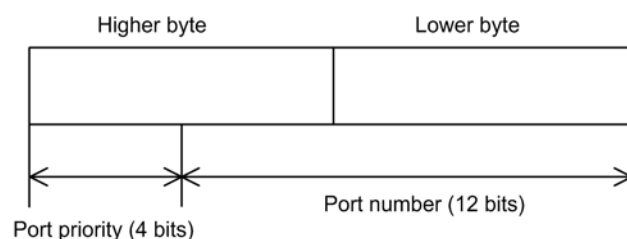
It is recommended that a lower path cost be specified for a port that has a faster packet transmission speed (that is, the faster the port, the lower the specified path cost). The default value of the path cost corresponds to the speed of the port, but can also be changed in the configuration.

### (5) Port identifier

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.

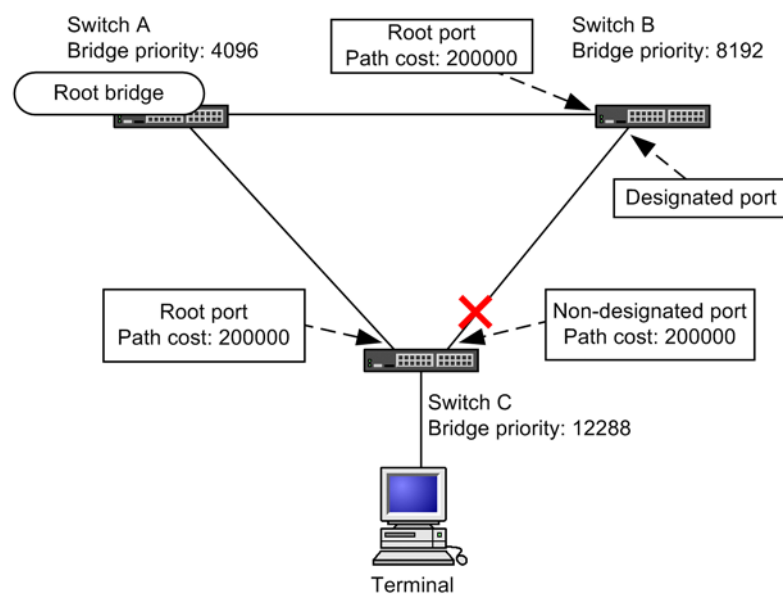
### Figure 19-3 Port ID



### 19.1.5 Designing Spanning Tree topologies

The topology of a Spanning Tree Protocol is based on the bridge ID and path cost. The figure below shows the basic procedures for designing a topology. In the example configuration in the figure, two core switches are used for redundancy, placed to handle terminals as edge switches.

### Figure 19-4 Designing Spanning Tree topologies



Legend: ✖: Blocking status

**(1) Selecting the root bridge by bridge IDs**

The switch with the lowest bridge ID is chosen as the root bridge. Normally, you set the bridge priority of the switch that you want to be the root bridge to the lowest value (highest priority). In the example in the figure, Switch A is the root bridge, and Switch B and Switch C are designated bridges.

Note that Switch B will become the alternate root bridge if a fault occurs on the root bridge. Switch C is set as the lowest priority.

For the design of a Spanning Tree topology, we recommend configurations that follow the example in the figure of setting the switch handling the network core as the root bridge and using alternate root bridges to make the core redundant.

**(2) Designing communication paths**

After a root bridge is determined, the communication paths from each designated bridge to the root bridge are determined.

**(a) Selecting the root port based on path cost**

For Switch B and Switch C, the path to the root bridge is determined by finding the lowest root path cost value. In the example in the figure, the path cost for all ports is 200000. Among the directly connected ports, the one with the lowest root path cost is chosen as the root port.

The root path cost of a path from a designated bridge to the root bridge is calculated by comparing the total path cost of the outgoing ports bound for the root bridge for each switch. For example, because the path cost of the path passing through Switch B for Switch C is 400000, it is not chosen for the root port.

The default cost for a path is the smallest value, which is based on the fastest port speed. In addition, the root port is determined by comparing root path costs. Therefore, you normally do not need to make changes to path costs to prioritize the use of paths with fast ports or the minimum of intermediate switches. To prioritize paths 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 Blocking status. This is how Spanning Tree Protocols use the Blocking status on a given side to prevent loops.

Designated ports and non-designated ports are chosen as follows:

- The port on the switch with the lowest root path cost between switches is the designated port, and ports on higher cost switches are non-designated ports.
- If root path costs are the same, the port on the switch that has the smaller bridge ID is the designated port, and ports on switches that have larger IDs are non-designated ports.

In the example in the figure, the root path costs are the same. According to the bridge priority, Switch B has the designated port and Switch C has the non-designated port, which is placed in Blocking status. To change the port of Switch B to Blocking status, set the path costs so that the root path cost of Switch B increases.

**19.1.6 STP compatibility mode****(1) Overview**

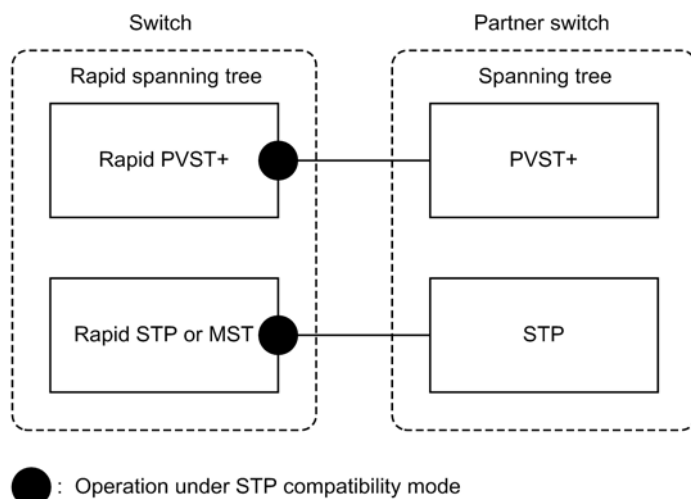
If the Switch uses a rapid Spanning Tree Protocol and the partner switch uses a Spanning Tree Protocol, the Switch's port connected to the partner switch runs in STP compatibility mode.

Under STP compatibility mode operation, high-speed transitions are not performed on the

corresponding port on the Switch because the port keeps pace with the remote port during this mode.

Combinations of Spanning Tree Protocols that can be used on the Switch and the partner switch are shown in the following figure.

**Figure 19-5** Relationship of the switch operations in STP compatibility mode



Under STP compatibility mode operation, high-speed transitions can no longer be performed on the corresponding port, requiring more time for communication to be restored.

The Switch supports automatic-restoration and forced restoration of a rapid Spanning Tree Protocol.

## (2) Restoration functionality

### (a) Automatic-restoration functionality

Automatic-restoration returns the Switch from STP compatibility mode operation to rapid Spanning Tree operation if the partner switch changes to a rapid Spanning Tree switch during operation in STP compatibility mode.

- The automatic STP compatibility mode recovery functionality operates if the link type of the corresponding port is point-to-point.
- If the corresponding port is a non-designated port<sup>#</sup> running in STP compatibility mode, an RST BPDU or MST BPDU can be sent from the corresponding port to disable STP compatibility mode.

<sup>#</sup>

For details about non-designated ports, see *Table 19-6 Port role* in 19.1.4 (2) *Port role*.

- If the link type of the corresponding port is shared, automatic-restoration mode does not run, because it cannot run correctly.

Depending on the timing of the restoration, the corresponding port and the partner switch continue running in STP compatibility mode.

### (b) Forced restoration functionality

The forced restoration functionality performs forced restoration for ports running in STP compatibility mode, allowing them to perform high-speed transitions normally.

This functionality executes the `clear spanning-tree detected-protocol` operation command to perform forced restoration from STP compatibility mode. The link type of the corresponding port can be either point-to-point or shared.



### 19.1.7 Notes common to Spanning Tree Protocols

#### (1) CPU overloading

If the CPU is overloaded, the BPDUs sent and received by the Switch are discarded, a timeout message might be output, the topology might change, and communication might be temporarily cut off.

#### (2) Specifying configuration commands that disable VLANs

When the `no spanning-tree disable` configuration command is used to enable the Spanning Tree functionality for the Switch, all VLANs temporarily go down.

## 19.2 Configuration of the Spanning Tree operating mode

The following explains settings for the Spanning Tree operating mode.

If the Switch is started without a configuration being set, it runs in the **pvst** operating mode.

### 19.2.1 List of configuration commands

The following table describes the commands used to configure the spanning-tree operating mode.

**Table 19-7** List of configuration commands

| Command name              | Description                                              |
|---------------------------|----------------------------------------------------------|
| spanning-tree disable     | Stops the Spanning Tree functionality.                   |
| spanning-tree mode        | Sets the operating mode for Spanning Tree functionality. |
| spanning-tree single mode | Selects STP and Rapid STP for Single Spanning Tree.      |
| spanning-tree vlan mode   | Selects PVST+ and Rapid PVST+ for each VLAN.             |

### 19.2.2 Configuring the operating mode

The operating mode of a switch can be set so that various Spanning Tree Protocols can be used. The table below describes the switch operating modes. If no operating mode is set, operation is performed in **pvst** mode.

Keep in mind that when **rapid-pvst** is specified for the operating mode, the Single Spanning Tree default is STP.

**Table 19-8** 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 is not run by default.                          |
| spanning-tree mode rapid-pvst | Allows Single Spanning Tree to be used with PVST+. Rapid PVST+ for rapid Spanning Tree Protocols is run by default. Single Spanning Tree is not run by default. |
| spanning-tree mode mst        | Runs Multiple Spanning Tree.                                                                                                                                    |

#### (1) Setting the pvst operation mode

Points to note

You can 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 is not run by default, but can be 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 is run using Rapid PVST+.
3. **(config)# spanning-tree single**  
Causes Single Spanning Tree to run. 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 operating mode of a switch 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 is not run by default, but can be run through settings. Keep in mind that when **rapid-pvst** is specified for the operating mode, the Single Spanning Tree default is STP.

Command examples

1. **(config)# spanning-tree mode rapid-pvst**  
Sets the Spanning Tree operating mode to **rapid-pvst**. Rapid PVST+ is automatically run for port VLANs.
2. **(config)# spanning-tree vlan 10 mode pvst**  
Changes the operating mode of VLAN 10 to PVST+. Other port VLANs are run using Rapid PVST+, and VLAN 10 is run using PVST+.
3. **(config)# spanning-tree single**  
Causes Single Spanning Tree to run. 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, the switch operating mode is set 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.

## 19 Spanning Tree Protocol

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.

## 19.3 Description of PVST+

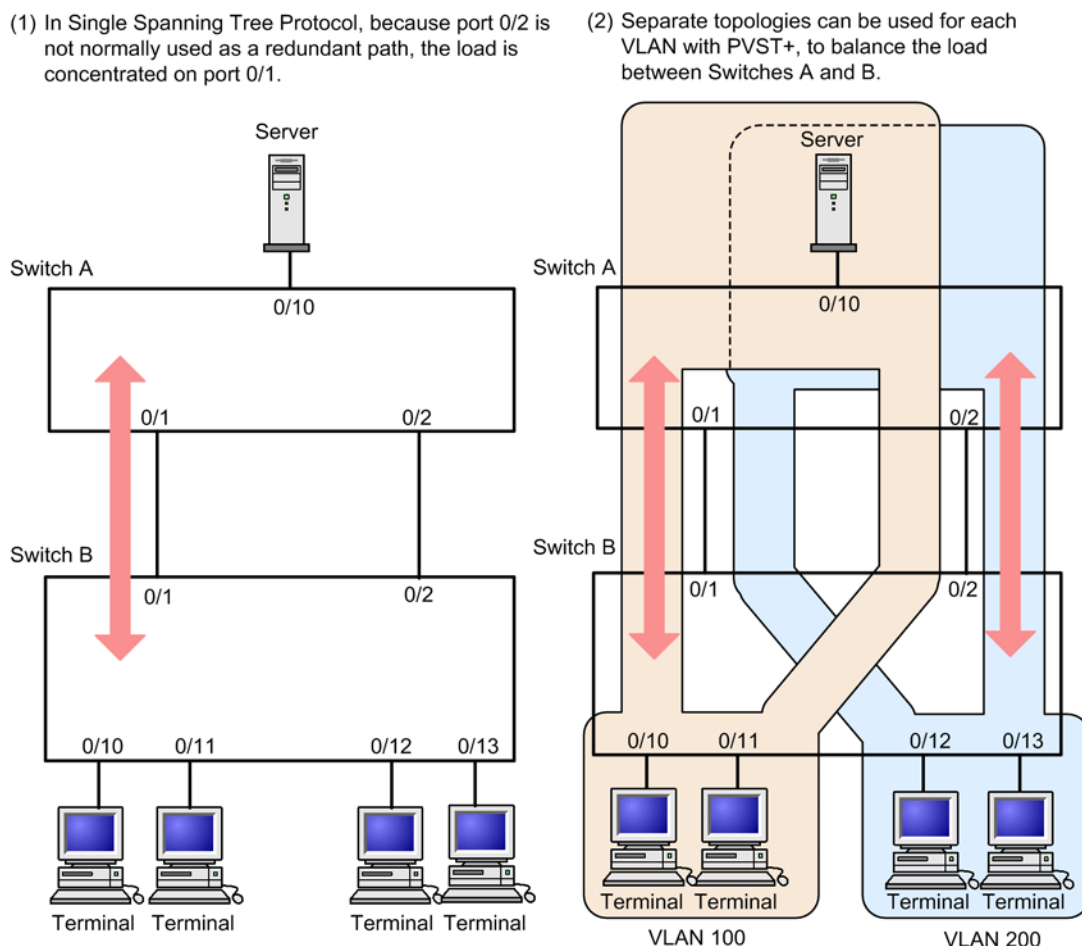
PVST+ builds a tree for each VLAN. These trees can be used for load balancing. In addition, access ports can be used to connect with switches running on Single Spanning Tree.

### 19.3.1 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 19-6** Using PVST+ to balance loads



### 19.3.2 PVST+ for access ports

#### (1) Description

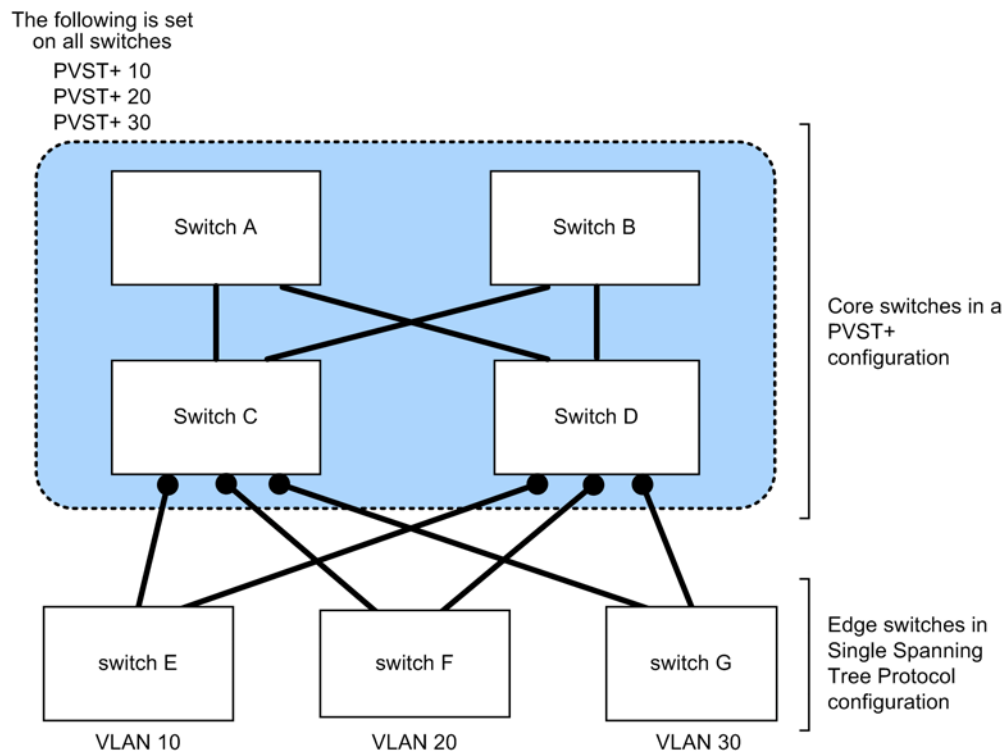
A network can be built using switches that use Single Spanning Tree or switches that support Single Spanning Tree functionality for one tree (abbreviated hereafter simply as *Single Spanning Tree*) and PVST+. Switches running with Single Spanning Tree are used as edge switches, and Switches are used as 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 is run on the edge switches, and PVST+ is run 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 19-7** Connecting to Single Spanning Tree



When a fault occurs on switch E, because the core switches use PVST+, topology change notifications are not sent to switches F and G.

Legend: ●: Access port

## (2) When PVST+ and Single Spanning Tree coexist on access ports

When PVST+ and Single Spanning Tree coexist, Single Spanning Tree is stopped (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 is stopped (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).

### 19.3.3 Notes on PVST+ usage

#### (1) Notes on use with other functionality

For details, see *15.3 Compatibility between Layer 2 switch functionality and other functionality*.

#### (2) VLAN 1 (default VLAN) PVST+ and Single Spanning Tree

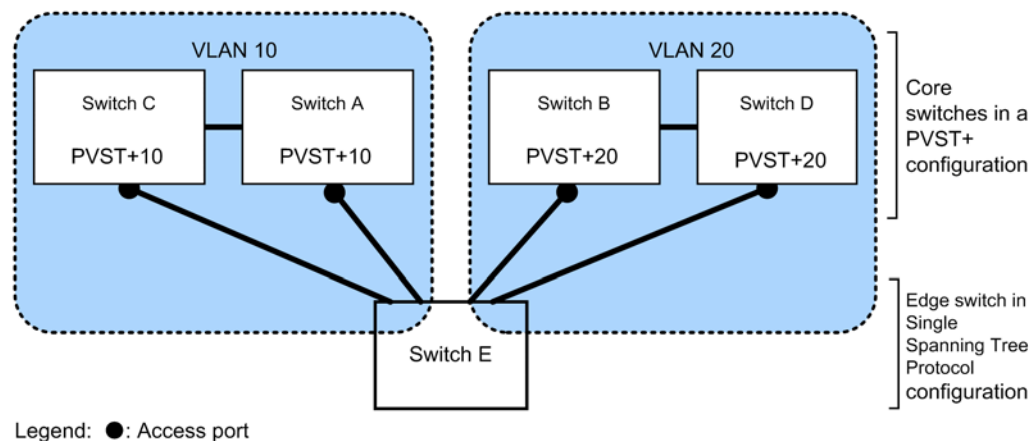
Single Spanning Tree and VLAN 1 PVST+ cannot be run at the same time. When Single Spanning Tree is run, the VLAN 1 PVST+ is stopped.

#### (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 19-8** Example of a prohibited configuration with Single Spanning Tree



Because switch E does not consist of one Spanning Tree, the topology is invalid.

## 19.4 PVST+ configuration

### 19.4.1 List of configuration commands

The following table describes the commands used to configure PVST+.

**Table 19-9** List of configuration commands

| Command name                          | Description                                                                       |
|---------------------------------------|-----------------------------------------------------------------------------------|
| spanning-tree cost                    | Sets the path cost for a port.                                                    |
| spanning-tree pathcost method         | Sets the margin of values used for path costs for a port.                         |
| spanning-tree port-priority           | Sets the port priority for each port.                                             |
| spanning-tree vlan                    | Sets PVST+ starting and stopping operation.                                       |
| spanning-tree vlan cost               | Sets the path cost value for a VLAN.                                              |
| spanning-tree vlan forward-time       | Sets the time required for port status transitions.                               |
| spanning-tree vlan hello-time         | Sets the sending interval for BPDUs.                                              |
| spanning-tree vlan max-age            | Sets the maximum enabled time for sent BPDUs.                                     |
| spanning-tree vlan pathcost method    | Sets the margin of values used for path costs for a VLAN.                         |
| spanning-tree vlan port-priority      | Sets the port priority for a VLAN.                                                |
| spanning-tree vlan priority           | Sets the bridge priority.                                                         |
| spanning-tree vlan transmission-limit | Sets the maximum number of BPDUs that can be sent per <b>hello-time</b> interval. |

### 19.4.2 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 be started or stopped per VLAN. The **no spanning-tree vlan** configuration command is used to stop operation.

To prevent PVST+ operation on a newly created VLAN, use the **no spanning-tree vlan** configuration command to set this before the VLAN is created.

#### Command examples

1. **(config)# no spanning-tree vlan 20**  
Stops VLAN 20 PVST+ operation.
2. **(config)# spanning-tree vlan 20**  
Runs the stopped VLAN 20 PVST+.



## Notes

- PVST+ runs automatically when nothing is displayed for the configuration. The `no spanning-tree vlan` 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.

### 19.4.3 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. This makes it more likely for a high-speed port to be selected 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 lists the default values for path costs.

**Table 19-10** Default path cost value

| Port speed | Default path cost value |                     |
|------------|-------------------------|---------------------|
|            | short (16-bit value)    | long (32-bit value) |
| 10 M bps   | 100                     | 2000000             |
| 100 M bps  | 19                      | 200000              |
| 1 G bps    | 4                       | 20000               |

### Command examples

1. 

```
(config)# interface fastethernet 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 fastethernet 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 partner connected switch does not support link aggregation.

#### Points to note

For port priorities, a lower value indicates a higher priority. When redundancy is used between two switches, the path whose switch is closer to the root bridge and whose port has a higher priority is used as the communication path. If this parameter is not set, the port with the lower port number is prioritized.

### Command examples

1. 

```
(config)# interface fastethernet 0/1
(config-if)# spanning-tree port-priority 64
(config-if)# exit
```
2. 

```
(config)# interface fastethernet 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.

## 19.4.4 Configuring PVST+ parameters

Each parameter must be set to satisfy the following relationship:  $2 \times (\text{forward-time} - 1) \geq$

$max-age \geq 2 \times (hello-time + 1)$ . When a parameter is changed, parameters must be adjusted on all switches comprising the Spanning Tree Protocol.

### (1) Setting BPDU sending intervals

A short BPDU sending interval makes topology changes easier to detect. A longer interval requires more time to detect a topology change, but can reduce BPDU traffic and the load on the Spanning Tree program for the Switch.

#### Points to note

When no value is set, BPDUs are sent at two-second intervals. Normally, this setting is not required.

#### Command examples

1. `(config)# spanning-tree vlan 10 hello-time 3`  
Sets the PVST+ BPDU sending interval to three seconds for VLAN 10.

#### Notes

A short BPDU sending interval makes topology changes easier to detect, but might increase load on the Spanning Tree program due to an increase in BPDU traffic. If setting this parameter shorter than the default value (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 PVST+, and is fixed at 3 for PVST+. Normally, this setting is not required.

#### Command examples

1. `(config)# spanning-tree vlan 10 transmission-limit 5`  
Sets the maximum number of BPDUs to be sent per *hello-time* to 5 for VLAN 10 Rapid PVST+.

### (3) Setting maximum enabled times for BPDUs

You can set the maximum enabled time for BPDUs sent from the root bridge. The BPDU counter is incremented whenever a switch is passed, and BPDUs exceeding the maximum enabled time are disabled and ignored.

#### Points to note

The maximum enabled time can be increased to have BPDUs reach many switches. If no value is set, 20 is used for the maximum enabled time.

#### Command examples

1. `(config)# spanning-tree vlan 10 max-age 25`  
Sets the maximum enabled time for BPDUs to 25 seconds on the PVST+ for VLAN 10.

#### (4) Setting status transition times

For timer-based operation in PVST+ mode or Rapid PVST+ mode, the port status transitions at a fixed time interval. For the PVST+ mode, it transitions from Blocking to Listening, Learning, and then Forwarding, and for the Rapid PVST+ mode, it transitions from Discarding to Learning and then Forwarding. The time required for these status transitions can be set. A small value can be set to transition more quickly to the Forwarding status.

##### Points to note

If no value is set, 15 seconds is used for the status transition time. When changing this parameter to a shorter time, make sure that the relationship between the BPDU maximum enabled time (*max-age*) and sending interval (*hello-time*) satisfies the following:  $2 \times (\text{forward-time} - 1) \geq \text{max-age} \geq 2 \times (\text{hello-time} + 1)$ .

##### Command examples

1. `(config)# spanning-tree vlan 10 forward-time 10`  
Sets the status transition time to 10 seconds for the VLAN 10 PVST+.

## 19.5 PVST+ operation

### 19.5.1 List of operation commands

The following table describes the operation commands for PVST+.

**Table 19-11** List of operation commands

| Command name                          | Description                                                         |
|---------------------------------------|---------------------------------------------------------------------|
| show spanning-tree                    | Displays Spanning Tree information.                                 |
| show spanning-tree statistics         | Displays statistics about Spanning Tree Protocols.                  |
| clear spanning-tree statistics        | Clears statistics about Spanning Tree Protocols.                    |
| clear spanning-tree detected-protocol | Forces recovery of STP compatible mode for Spanning Tree Protocols. |
| show spanning-tree port-count         | Displays the number of accommodated Spanning Tree Protocols.        |

### 19.5.2 Checking PVST+ statuses

PVST+ information is displayed in the execution results of the `show spanning-tree` operation command. The PVST+ or Rapid PVST+ operation mode can be checked in `Mode`. To check that the topology has been built properly, make sure that the contents of `Root Bridge ID` are correct, along with `Status` and `Role` in `Port Information`.

**Figure 19-9** Execution results of show spanning-tree

```
> show spanning-tree vlan 4094

Date 2008/11/14 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

>
```

## 19.6 Description of Single Spanning Tree

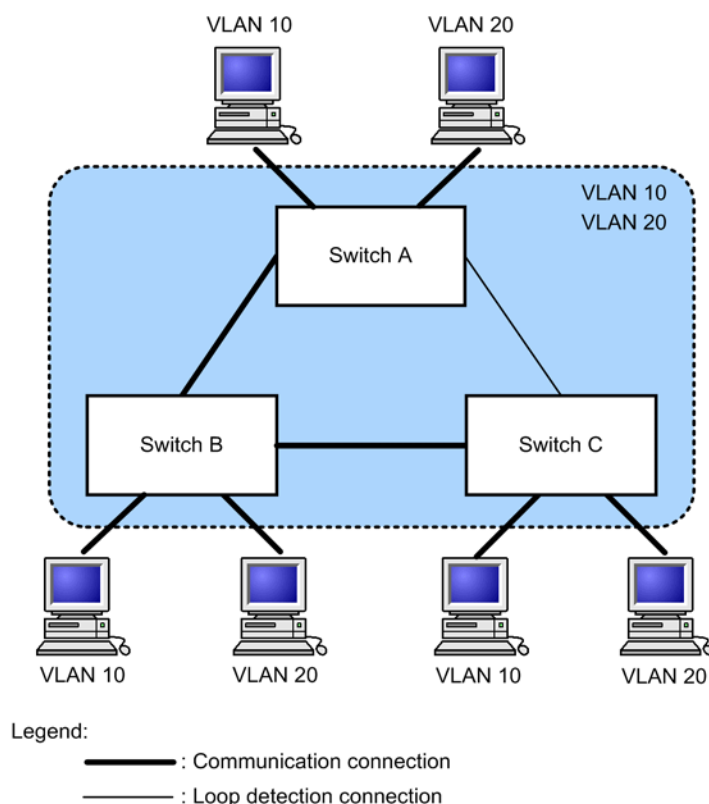
Single Spanning Tree creates topologies in which all switches are targets.

### 19.6.1 Overview

Single Spanning Tree and one Spanning Tree Protocol can be used to avoid loops on all VLANs, and can handle more VLANs than PVST+ controlling individual VLANs.

The figure below shows a network configuration based on Single Spanning Tree. In this figure, VLAN 10 and VLAN 20 are set for Switches A, B, and C, with PVST+ stopped on all VLANs to apply Single Spanning Tree. A single topology is used for all VLANs for communication.

**Figure 19-10** Network configuration based on Single Spanning Tree



### 19.6.2 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 lists the VLANs subject to Single Spanning Tree when Single Spanning Tree is used with a PVST+.

**Table 19-12** Single Spanning Tree target VLAN

| Item              | VLAN                                                                             |
|-------------------|----------------------------------------------------------------------------------|
| PVST+ target VLAN | VLANs running on a PVST+.<br>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+ is stopped (specified by the <code>no spanning-tree vlan</code> configuration command) |
|                                  | Default VLANs (port VLANs with a VLAN ID of 1)                                                               |
|                                  | Protocol VLANs                                                                                               |
|                                  | MAC VLANs                                                                                                    |

### 19.6.3 Notes on Single Spanning Tree usage

#### (1) Notes on use with other functionality

For details, see *15.3 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 be run at the same time. When Single Spanning Tree is run, the VLAN 1 PVST+ is stopped.

## 19.7 Configuration of Single Spanning Tree

### 19.7.1 List of configuration commands

The following table describes the commands used to configure Single Spanning Tree.

**Table 19-13** List of configuration commands

| Command name                            | Description                                                                                |
|-----------------------------------------|--------------------------------------------------------------------------------------------|
| spanning-tree cost                      | Sets the path cost for a port.                                                             |
| spanning-tree pathcost method           | Sets the margin of values used for path costs for a port.                                  |
| spanning-tree port-priority             | Sets the port priority for a port.                                                         |
| spanning-tree single                    | Starts or stops Single Spanning Tree.                                                      |
| spanning-tree single cost               | Sets the path cost value for Single Spanning Tree.                                         |
| spanning-tree single forward-time       | Sets the time required for port status transitions.                                        |
| spanning-tree single hello-time         | Sets the sending interval for BPDUs.                                                       |
| spanning-tree single max-age            | Sets the maximum enabled time for sent BPDUs.                                              |
| spanning-tree single pathcost method    | Sets the margin of values used for path costs for Single Spanning Tree.                    |
| spanning-tree single port-priority      | Sets the port priority for Single Spanning Tree.                                           |
| spanning-tree single priority           | Sets the bridge priority.                                                                  |
| spanning-tree single transmission-limit | Sets the maximum number of BPDUs that can be sent per <a href="#">hello-time</a> interval. |

### 19.7.2 Configuring Single Spanning Tree

#### Points to note

You can start and stop Single Spanning Tree. Single Spanning Tree does not run simply by setting the [pvst](#) or [rapid-pvst](#) operation mode, but start operation according to settings.

VLAN 1 (default VLAN) and Single Spanning Tree cannot be used at the same time. When Single Spanning Tree is set, the VLAN 1 PVST+ stops.

#### Command examples

1. [\(config\)# spanning-tree single](#)

Causes Single Spanning Tree to run. This setting stops the VLAN 1 PVST+, making VLAN 1 a Single Spanning Tree target.

2. [\(config\)# no spanning-tree single](#)

Stops Single Spanning Tree. When a VLAN 1 PVST+ is not set to be stopped, and 250 PVST+ instances are not already running, VLAN 1 PVST+ operation starts automatically.



### 19.7.3 Configuring topologies for Single Spanning Tree

#### (1) Setting bridge priority

The bridge priority is a parameter for determining the root bridge. When a topology is designed, the highest priority is set for the switch to be used for the root bridge, and the second highest priority is set for the switch to be used next for the root bridge if a fault occurs on the root bridge.

##### Points to note

For bridge priorities, a lower value indicates a higher priority, and the switch with the lowest set value is the root bridge. Because the root bridge is decided by a bridge ID consisting of the bridge priority and switch MAC address, if this parameter is not set, the switch with the lowest MAC address becomes the root bridge.

##### Command examples

1. `(config)# spanning-tree single priority 4096`  
Sets the bridge priority for Single Spanning Tree to 4096.

#### (2) Setting path costs

The path cost is a parameter for determining communication paths. When a Spanning Tree topology is designed, after the bridge priority is determined, the root port of each designated bridge (communication path from the designated bridge to the root bridge) is determined by using this parameter.

##### Points to note

Path cost values are set for each port of a designated bridge. Small values can be set to make root port selection more likely. If no value is set, different default values are used. This makes it more likely for a high-speed port to be selected 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 lists the default values for path costs.

**Table 19-14** Default path cost value

| Port speed | Default path cost value |                     |
|------------|-------------------------|---------------------|
|            | short (16-bit value)    | long (32-bit value) |
| 10 M bps   | 100                     | 2000000             |
| 100 M bps  | 19                      | 200000              |
| 1 G bps    | 4                       | 20000               |

##### Command examples

1. `(config)# interface fastethernet 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 fastethernet 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 to make connections between two switches redundant, but use this functionality when a Spanning Tree Protocol is needed for redundancy because the opposite connected switch does not support link aggregation.

#### Points to note

For port priorities, a lower value indicates a higher priority. When redundancy is used between two switches, the path whose switch is closer to the root bridge and whose port has a higher priority is used as the communication path. If this parameter is not set, the port with the lower port number is prioritized.

#### Command examples

1. 

```
(config)# interface fastethernet 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 fastethernet 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.

## 19.7.4 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 three 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.

## 19 Spanning Tree Protocol

### 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.

## 19.8 Operation for Single Spanning Tree

### 19.8.1 List of operation commands

The following table describes the operation commands for Single Spanning Tree.

**Table 19-15** List of operation commands

| Command name                          | Description                                                         |
|---------------------------------------|---------------------------------------------------------------------|
| show spanning-tree                    | Displays Spanning Tree information.                                 |
| show spanning-tree statistics         | Displays statistics about Spanning Tree Protocols.                  |
| clear spanning-tree statistics        | Clears statistics about Spanning Tree Protocols.                    |
| clear spanning-tree detected-protocol | Forces recovery of STP compatible mode for Spanning Tree Protocols. |
| show spanning-tree port-count         | Displays the number of accommodated Spanning Tree Protocols.        |

### 19.8.2 Checking the Single Spanning Tree status

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 19-11** Information about Single Spanning Tree

```
> show spanning-tree single

Date 2008/11/14 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
 0/21 Down Status:Disabled Role:- -
 0/22 Up Status:Learning Role:Designated -
 0/23 Down Status:Disabled Role:- -
 0/24 Up Status:Learning Role:Designated -
```

## 19 Spanning Tree Protocol

|        |      |                 |                 |           |
|--------|------|-----------------|-----------------|-----------|
| 0/25   | Down | Status:Disabled | Role:-          | LoopGuard |
| 0/26   | Down | Status:Disabled | Role:-          | LoopGuard |
| ChGr:1 | Up   | Status:Learning | Role:Designated | RootGuard |
| ChGr:8 | Down | Status:Disabled | Role:-          | RootGuard |

>

## 19.9 Description of Multiple Spanning Tree

### 19.9.1 Overview

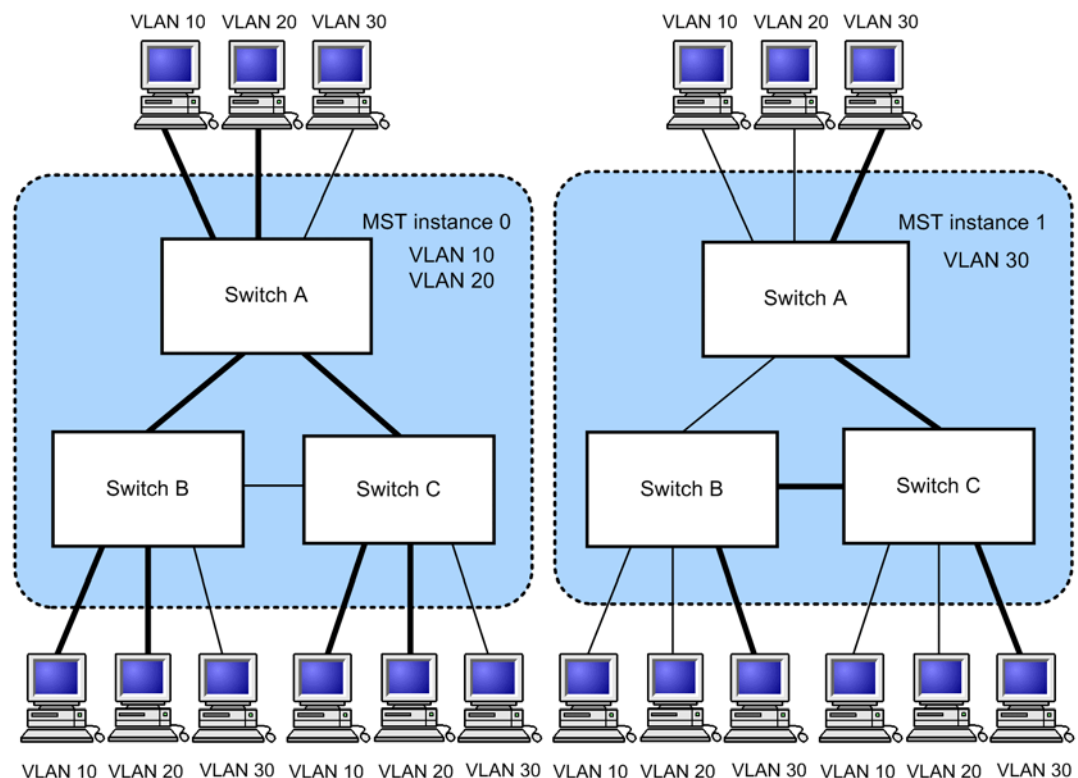
The following explains the features of Multiple Spanning Tree. MST instances can be used to perform load balancing. MST regions can be used to divide large network configurations into smaller configurations, to simplify network design. The following gives a functional overview of how Multiple Spanning 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 a Switch.

The following figure shows an example MST instance setup.

**Figure 19-12** Example MST instance setup



Two instances are defined on the network, with load balancing performed. VLANs 10 and 20 are made to belong to instance 0, and VLAN 30 is made to belong to instance 1.

Legend:

—: Communication connection

—: Loop detection connections and non-communication connections

#### (2) MST regions

Multiple Spanning Tree allows multiple switches to be grouped and handled as an MST region. To belong in the same MST region, the region name, revision number, MST

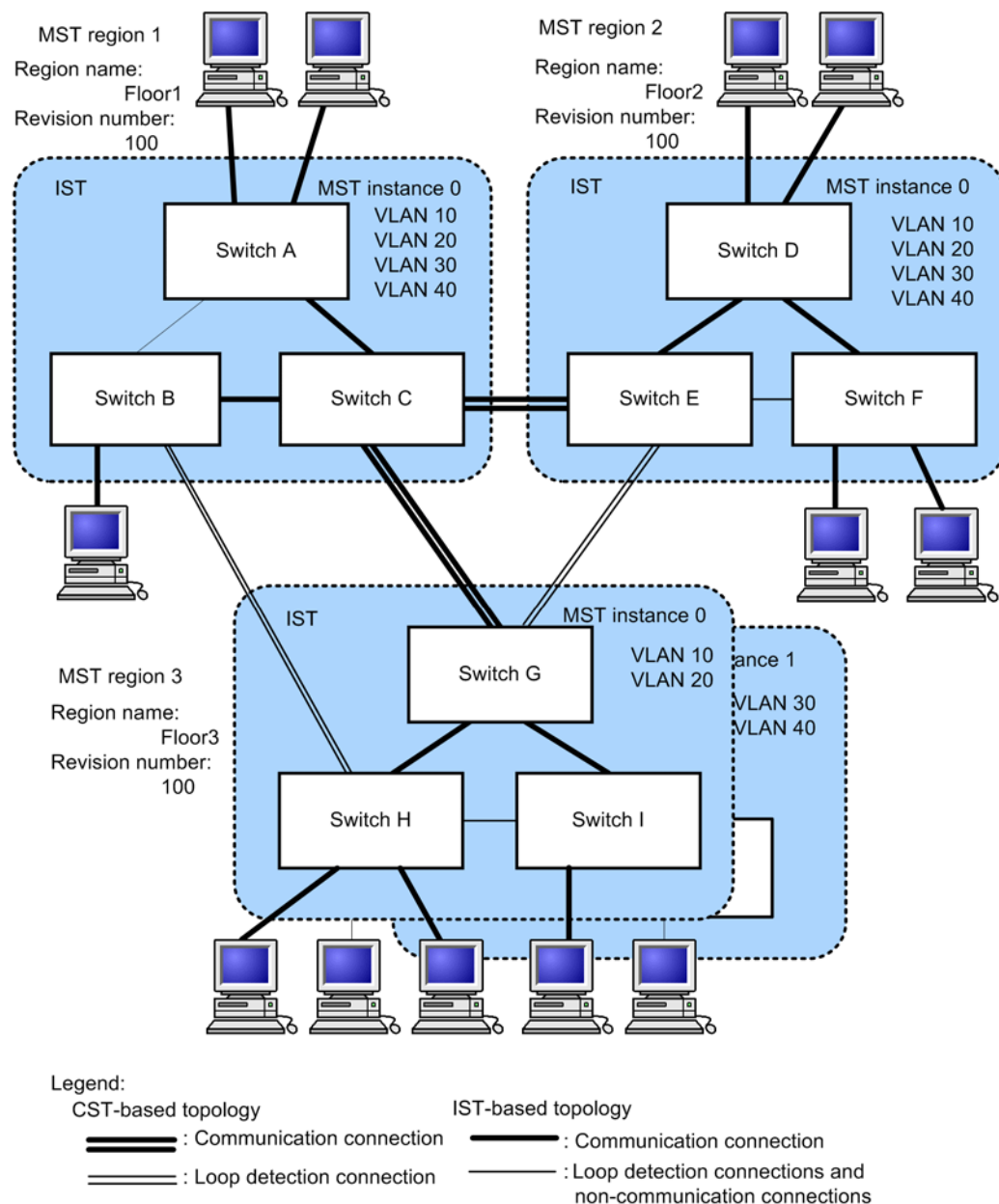
instance ID, and VLAN correspondence must be the same. These are set by configuration. Trees are built separately between MST regions and within MST regions, and the topology within an MST region can be built per MST instance.

The following explains Spanning Tree Protocols that run both between MST regions and within MST regions.

- CST  
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 provides an overview of Multiple Spanning Tree.

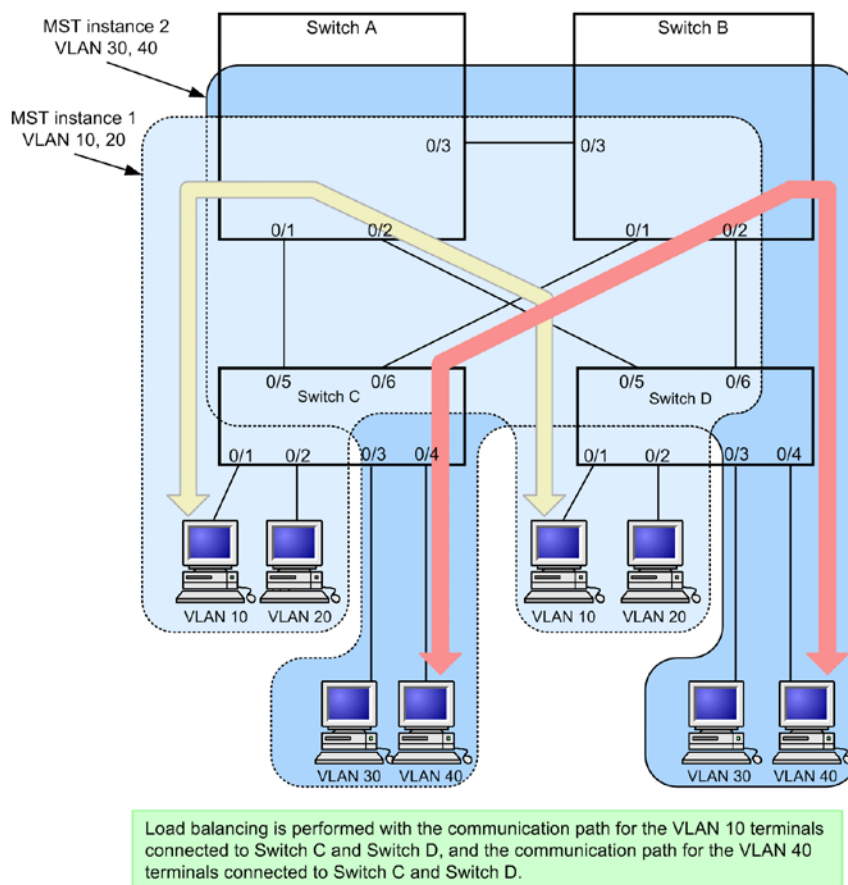


**Figure 19-13** Overview of Multiple Spanning Tree

## 19.9.2 Designing networks for Multiple Spanning Tree

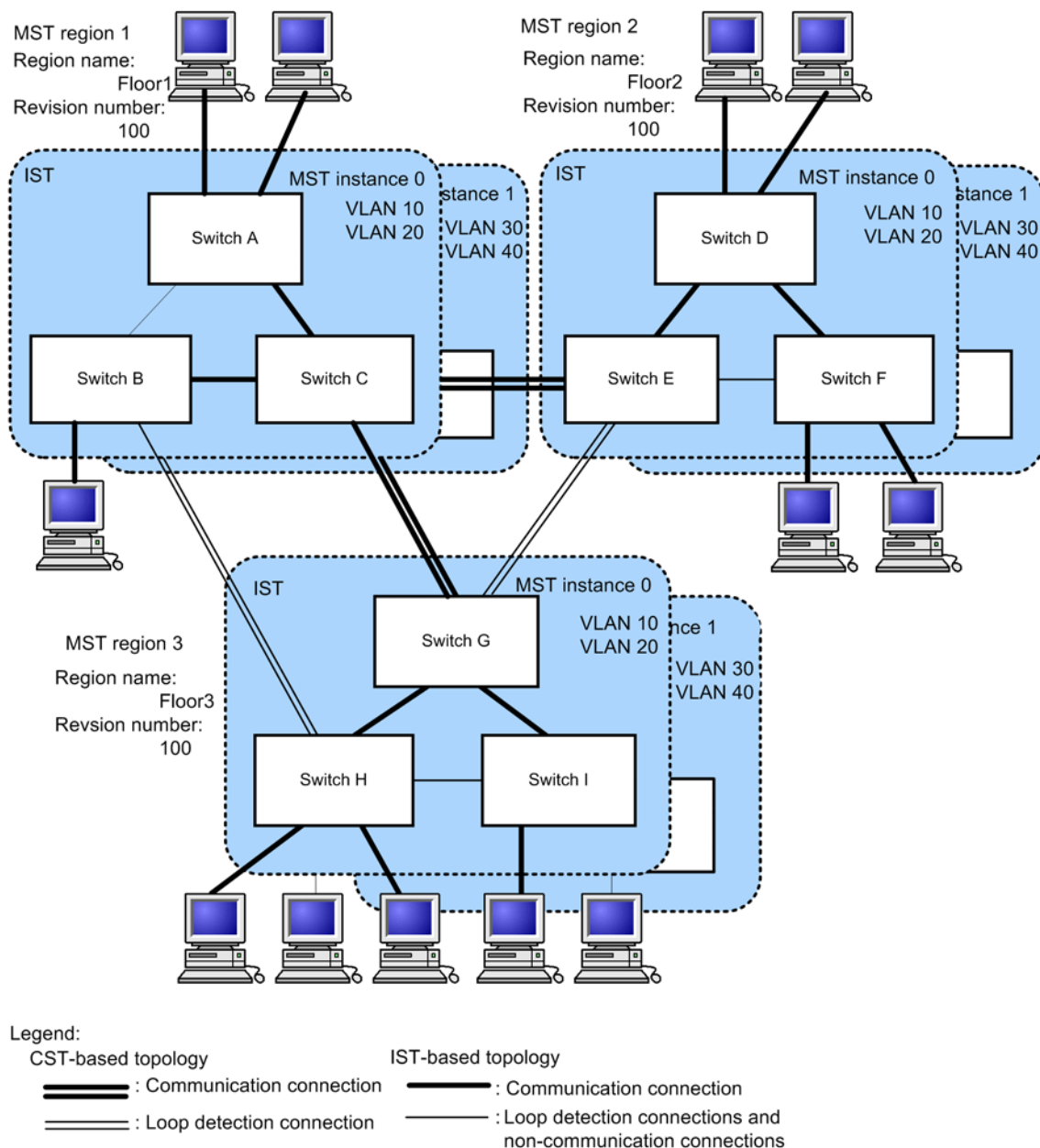
### (1) Configuring load balancing for each MST instance

Multiple Spanning Tree allows load balancing to be performed for each MST instance. The figure below shows an example configuration for load balancing. In this example, VLANs 10 and 20 are set for MST instance 1, VLANs 30 and 40 are set for MST instance 2, for load balancing in two parts. As shown in this example, Multiple Spanning Tree can enable load balancing by managing four VLANs with just two trees.

**Figure 19-14** 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 19-15** Network configuration by MST region

### 19.9.3 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. When a connection with one of these is established, the Switch handles it as another MST region. 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.

## 19.9.4 Notes on Multiple Spanning Tree usage

### (1) Notes on use with other functionality

For details, see *15.3 Compatibility between Layer 2 switch functionality and other functionality*.

### (2) MST regions

The range of VLANs that can be handled by the Switch and other switches might differ. To handle such switches as the same MST region, make sure that the corresponding VLANs belong to MST instance 0.

### (3) When time is required for topology convergence

When the events listed in the following table occur for CIST root bridges or MST instances, the topology might take a long time to settle, during which time communication might stop and MAC address tables might be cleared.

**Table 19-16** Events occurring on root bridges

| Event                  | Description                                                                                                                                                                                                                                                                                                                                                 | 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:<br>(1) <b>name</b> command for the MST configuration mode<br>(2) <b>revision</b> command for the MST configuration mode<br>(3) <b>instance</b> command for the MST configuration mode | CIST root bridge                                   | CIST                       |
|                        |                                                                                                                                                                                                                                                                                                                                                             | Root bridge on MST instance 0 (IST)                | CIST                       |
|                        |                                                                                                                                                                                                                                                                                                                                                             | Root bridge on MST instance 1 and those subsequent | Corresponding MST instance |
|                        | When the bridge priority is reduced by the <b>spanning-tree mst root priority</b> command (a larger value is currently set)                                                                                                                                                                                                                                 | CIST root bridge                                   | CIST                       |
|                        |                                                                                                                                                                                                                                                                                                                                                             | Root bridge on MST instance 1 and those subsequent | Corresponding MST instance |
| Additional Information | When the Switch is stopped                                                                                                                                                                                                                                                                                                                                  | CIST root bridge                                   | CIST                       |
|                        |                                                                                                                                                                                                                                                                                                                                                             | Root bridge on MST instance 0 (IST)                | CIST                       |
|                        |                                                                                                                                                                                                                                                                                                                                                             | Root bridge on MST instance 1 and those subsequent | Corresponding MST instance |
|                        | When all ports are down for the Switch in a loop configuration, on the partner switch connected to the switch (and the Switch is no longer the root bridge in the corresponding loop configuration)                                                                                                                                                         | CIST root bridge                                   | CIST                       |
|                        |                                                                                                                                                                                                                                                                                                                                                             | Root bridge on MST instance 0 (IST)                | CIST                       |
|                        |                                                                                                                                                                                                                                                                                                                                                             | Root bridge on MST instance 1 and those subsequent | Corresponding MST instance |

## 19.10 Configuration of Multiple Spanning Tree

### 19.10.1 List of configuration commands

The following table describes the commands used to configure Multiple Spanning Tree.

**Table 19-17** List of configuration commands

| Command name                         | Description                                                                                |
|--------------------------------------|--------------------------------------------------------------------------------------------|
| instance                             | Sets VLANs belonging to Multiple Spanning Tree MST instances.                              |
| name                                 | Sets a string to identify a Multiple Spanning Tree region.                                 |
| revision                             | Sets revision numbers to identify Multiple Spanning Tree regions.                          |
| spanning-tree cost                   | Sets the path cost for a port.                                                             |
| spanning-tree mode                   | Sets the operating mode for Spanning Tree functionality.                                   |
| spanning-tree mst configuration      | Sets the information required to form MST regions in Multiple Spanning Tree.               |
| spanning-tree mst cost               | Sets the path cost for each MST instance for Multiple Spanning Tree.                       |
| spanning-tree mst forward-time       | Sets the time required for port status transitions.                                        |
| spanning-tree mst hello-time         | Sets the sending interval for BPDUs.                                                       |
| spanning-tree mst max-age            | Sets the maximum enabled time for sent BPDUs.                                              |
| spanning-tree mst max-hops           | Sets the maximum number of hops within an MST region.                                      |
| spanning-tree mst port-priority      | Sets the port priority for each MST instance in Multiple Spanning Tree.                    |
| spanning-tree mst root priority      | Sets the bridge priority for each MST instance.                                            |
| spanning-tree mst transmission-limit | Sets the maximum number of BPDUs that can be sent per <a href="#">hello-time</a> interval. |
| spanning-tree port-priority          | Sets the port priority for a port.                                                         |

### 19.10.2 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 are stopped, and Multiple Spanning Tree operation is started.

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).

## 19.10.3 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. This makes it more likely for a high-speed port to be selected 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 lists the default values for path costs.

**Table 19-18** Default path cost value

| Port speed | Default path cost value |
|------------|-------------------------|
| 10 M bps   | 2000000                 |
| 100 M bps  | 200000                  |
| 1 G bps    | 20000                   |

## 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 fastethernet 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 to make connections between two switches redundant, but use this functionality when a Spanning Tree Protocol is needed for redundancy because the partner connected switch does not support link aggregation.

## Points to note

For port priorities, a lower value indicates a higher priority. When redundancy is used between two switches, the path whose switch is closer to the root bridge and whose port has a higher priority is used as the communication path. If this parameter is not set, the port with the lower port number is prioritized.

## Command examples

1. 

```
(config)# interface fastethernet 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 fastethernet 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.

**19.10.4 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 three 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. 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, the maximum enabled time (*max-age*) is a valid parameter only for ports connected to Single Spanning Tree switches. It does not need to be set for configurations in which Multiple Spanning Tree is run 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 Multiple Spanning Tree BPDUs to 10 seconds.

## 19.11 Operation for Multiple Spanning Tree

### 19.11.1 List of operation commands

The following table describes the operation commands for Multiple Spanning Tree.

**Table 19-19** List of operation commands

| Command name                          | Description                                                         |
|---------------------------------------|---------------------------------------------------------------------|
| show spanning-tree                    | Displays Spanning Tree information.                                 |
| show spanning-tree statistics         | Displays statistics about Spanning Tree Protocols.                  |
| clear spanning-tree statistics        | Clears statistics about Spanning Tree Protocols.                    |
| clear spanning-tree detected-protocol | Forces recovery of STP compatible mode for Spanning Tree Protocols. |
| show spanning-tree port-count         | Displays the number of accommodated Spanning Tree Protocols.        |

### 19.11.2 Checking the Multiple Spanning Tree status

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 the `show spanning-tree` command.

**Figure 19-16** Execution results of show spanning-tree

```
> show spanning-tree mst instance 4095

Date 2008/11/14 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)

## 19 Spanning Tree Protocol

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.

## 19.12 Description of common Spanning Tree functionality

### 19.12.1 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.

PortFast operates according to the PortFast settings and the port type. The following table describes the operating conditions of the PortFast functionality.

**Table 19-20** Operating conditions of the PortFast functionality

| Configuration definition                                |                                                                   | Port type                                |            |
|---------------------------------------------------------|-------------------------------------------------------------------|------------------------------------------|------------|
| Configuration for each port<br>(spanning-tree portfast) | Configuration for each switch<br>(spanning-tree portfast default) | Access port<br>Protocol port<br>MAC port | Trunk port |
| PortFast is set (trunk)                                 | (Priority is given to the configuration for each port.)           | Y                                        | Y          |
| PortFast disabled (disable)                             |                                                                   | --                                       | --         |
| Parameter omitted                                       |                                                                   | Y                                        | --         |
| No command specified                                    | Command specified                                                 | Y                                        | --         |
|                                                         | No command specified                                              | --                                       | --         |

Legend:

Y: Supported, --: 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 is stopped, and operation is started 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 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 be 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. This lets them link up again with PortFast ports with the BPDU guard functionality applied, and resume communication.

### 19.12.2 BPDU filter

#### (1) Overview

On ports with the BPDU filter functionality applied, BPDU sending and reception are stopped. The BPDU filter functionality is applied to ports with PortFast set, for which a terminal is connected and loops are known not to occur.

#### (2) Notes on BPDU filters

When the BPDU filter functionality is set for ports other than those with PortFast applied, because BPDU sending and reception are stopped, communication is cut off until a timer-based port status transition is completed.

### 19.12.3 Loop guard

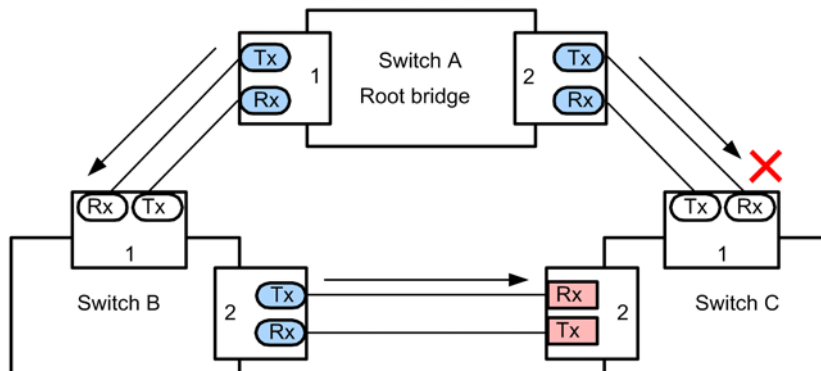
#### (1) Overview

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.

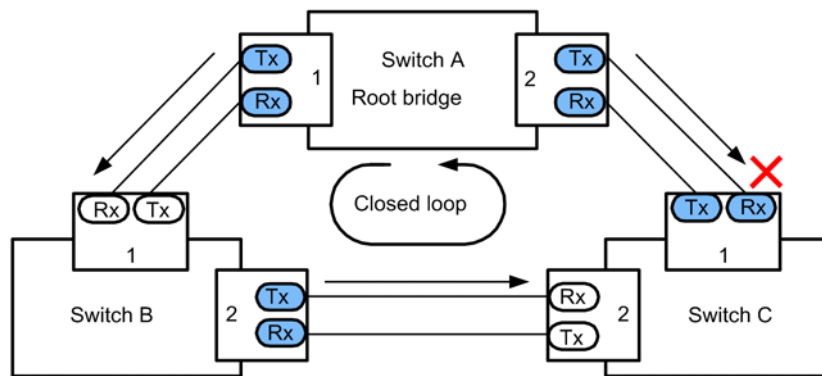
The following figure shows the problems that occur during unidirectional link faults.

**Figure 19-17** 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 a port for which the root guard functionality is set, or when the PortFast functionality is set for the Switch or for the port.

The following table describes the loop guard operating conditions.

**Table 19-21** Operating conditions of loop guard

| PortFast Functionality | Configuration definition                          |                                                                 | Loop guard operation |
|------------------------|---------------------------------------------------|-----------------------------------------------------------------|----------------------|
|                        | Configuration for each port (spanning-tree guard) | Configuration for each switch (spanning-tree loopguard default) |                      |
| Enabled                | Loop guard is set (loop)                          | (Priority is given to the configuration for each port.)         | --                   |
|                        | Guard disabled (none)                             |                                                                 | --                   |

| PortFast Functionality | Configuration definition                          |                                                                 | Loop guard operation |
|------------------------|---------------------------------------------------|-----------------------------------------------------------------|----------------------|
|                        | Configuration for each port (spanning-tree guard) | Configuration for each switch (spanning-tree loopguard default) |                      |
|                        | Root guard is set (root)                          |                                                                 | --                   |
|                        | No command specified                              | command specified                                               | --                   |
|                        |                                                   | No command specified                                            | --                   |
| Disabled               | Loop guard is set (loop)                          | (Priority is given to the configuration for each port.)         | Y                    |
|                        | Guard disabled (none)                             |                                                                 | --                   |
|                        | Root guard is set (root)                          |                                                                 | --                   |
|                        | No command specified                              | Command specified                                               | Y                    |
|                        |                                                   | No command specified                                            | --                   |

Legend:

Y: Supported, --: 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.

- Starting the switch
- A port goes up (including due to link aggregation)
- The type of Spanning Tree Protocol changes (to STP or high-speed STP, PVST+ or high-speed PVST+)

Configure loop guard functionality not only on designated ports, but also on partner switches. When it is configured only on designated ports, even when the above events occur, the designated ports might not receive BPDUs. In cases like this, removing loop guards might take a long time. This is because removing a loop guard requires waiting for BPDU transmission after a BPDU reception timeout is detected on a port on the partner switch.

Also, even if loop guards are set for both ports, removing the loop guard on a designated port might take a long time if no BPDUs are received. Specifically, this happens when a bridge, port priority, or path cost is changed so that the opposing port becomes a designated port, in which case a BPDU timeout is detected on the opposing port, and loop guard operation is performed. If this port is a designated port, BPDUs might not be received, and removing loop guards might take a long time.

When loop guard functionality is set during operation, the loop guard will not run immediately, but instead will run when a BPDU reception timeout occurs.

When a switch that does not forward BPDUs exists between the Switch and a partner switch, and a port is linked up while loop guard functionality is set on both ports, loop guards will continue running on both ports. To perform recovery, BPDU forwarding



functionality must be enabled on switches between both ports, and the ports must be linked up again.

## 19.12.4 Root guard

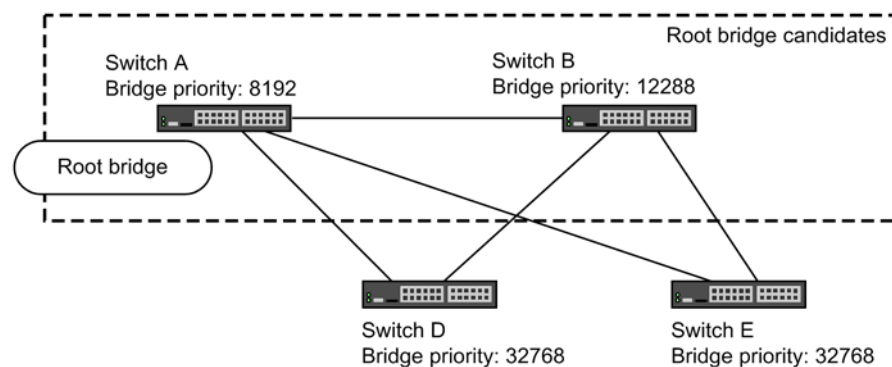
### (1) Overview

Unintended topologies might occur if a switch is accidentally connected or a setting is changed somewhere where the network is not managed. When performance of the root bridge in an unintended topology is poor, a network fault might occur when traffic is congested. Root guard functionality avoids such network faults by identifying root bridge candidates for situations like this.

The figures below show problems that occur when switches are accidentally connected.

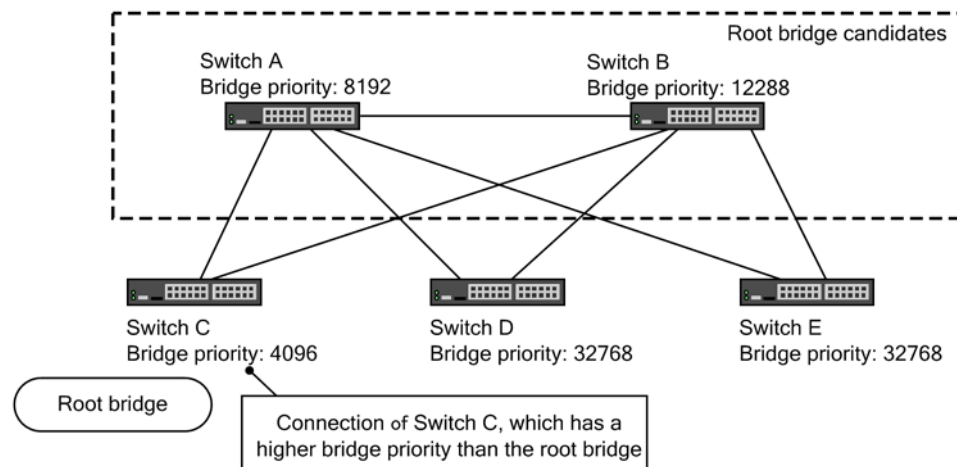
- Operation in which Switch A and Switch B run as root bridge candidates

**Figure 19-18** 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 19-19** 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 operating conditions of the root guard functionality.

**Table 19-22** Operating conditions of root guard

| Configuration definition                             |                                                                    | Root guard operation |
|------------------------------------------------------|--------------------------------------------------------------------|----------------------|
| Configuration for each port<br>(spanning-tree guard) | Configuration for each switch<br>(spanning-tree loopguard default) |                      |
| Loop guard is set (loop)                             | (Priority is given to the configuration of each port.)             | --                   |
| Guard disabled (none)                                |                                                                    | --                   |
| Root guard is set (root)                             |                                                                    | Y                    |
| No command specified                                 | Command specified                                                  | --                   |
|                                                      | No command specified                                               | --                   |

Legend:

Y: Supported, --: Not supported

## 19.13 Configuration of the common Spanning Tree functionality

### 19.13.1 List of configuration commands

The following table describes the commands used to configure common Spanning Tree functionality.

**Table 19-23** List of configuration commands

| Command name                             | Description                                                               |
|------------------------------------------|---------------------------------------------------------------------------|
| spanning-tree bpdupfilter                | Sets BPDU filter functionality for each port.                             |
| spanning-tree guard                      | Sets loop guard functionality and root guard functionality for each port. |
| spanning-tree link-type                  | Sets link types for ports.                                                |
| spanning-tree loopguard default          | Sets loop guard functionality to be used by default.                      |
| spanning-tree portfast                   | Sets PortFast functionality for each port.                                |
| spanning-tree bpduguard                  | Sets BPDU guard functionality for each port.                              |
| spanning-tree portfast bpduguard default | Sets BPDU guard functionality to be used by default.                      |
| spanning-tree portfast default           | Sets PortFast functionality to be used by default.                        |

### 19.13.2 Setting 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 executed, PortFast functionality is applied by default on access ports, protocol ports, and MAC ports. To disable PortFast for a port after it has been applied by default, use 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 fastethernet 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 fastethernet 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 ahead 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 to all ports to which the PortFast functionality is applied. To disable the BPDU guard for a port after it has been applied by default, use 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 fastethernet 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 fastethernet 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 can be set using the `spanning-tree bpduguard enable` configuration command.

### 19.13.3 Setting BPDU filters

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

BPDU filter functionality can be set for each interface.

## Command examples

1. 

```
(config)# interface fastethernet 0/1
(config-if)# spanning-tree bpdupfilter enable
(config-if)# exit
```

Sets BPDU filter functionality for port 0/1.

### 19.13.4 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` configuration command is used, loop guards are applied to all ports other than those with PortFast set. When loop guard has been applied by default, use the `spanning-tree guard none` configuration command to disable loop guards.

## Command examples

1. 

```
(config)# spanning-tree loopguard default
```

Sets that loop guard functionality is to be applied for all ports other than those with PortFast set.

2. 

```
(config)# interface fastethernet 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
(config)# interface fastethernet 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.

### 19.13.5 Setting 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 fastethernet 0/1
(config-if)# spanning-tree guard root
(config-if)# exit
```

Sets root guard functionality for port 0/1.

### 19.13.6 Configuring link types

Link types represent the connection status of a port. The connections between switches must be point-to-point to perform high-speed status transitions for Rapid PVST+, Rapid STP for Single Spanning Tree, or Multiple Spanning Tree. For shared types, high-speed status transitions are not performed, and status transitions are performed by timer as with PVST+ and STP for Single Spanning Tree.

Points to note

A connection status can be set for each port. If it is not set, point-to-point is used when the port is a full duplex connection, and shared is used when it is a half duplex connection.

Command examples

1. 

```
(config)# interface fastethernet 0/1
(config-if)# spanning-tree link-type point-to-point
(config-if)# exit
```

Causes port 0/1 to run 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.

## 19.14 Operation for common Spanning Tree functionality

### 19.14.1 List of operation commands

The following table describes the operation command for common Spanning Tree functionality.

**Table 19-24** List of operation commands

| Command name       | Description                         |
|--------------------|-------------------------------------|
| show spanning-tree | Displays Spanning Tree information. |

### 19.14.2 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.
- The RootGuard item can be checked for root guards, and the BPDUFilter item for BPDU filters. (In the following example, they are both OFF, which indicates that the functionality has not been set.)
- The Link Type item for each port can be used to check the link type. (In the following example, - is displayed because PVST+ is used.)

**Figure 19-20** Spanning Tree information

```
> show spanning-tree vlan 4094 detail

Date 2008/11/14 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(2008/11/14 11:26:47):
 Designated Root
```

## 19 Spanning Tree Protocol

```
 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
>
```



---

## 20. 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.

|                                                                 |
|-----------------------------------------------------------------|
| 20.1 Overview of the Ring Protocol                              |
| 20.2 Basic Ring Protocol principles                             |
| 20.3 Overview of single ring operation                          |
| 20.4 Overview of multi-ring operation                           |
| 20.5 Multi-fault monitoring functionality for the Ring Protocol |
| 20.6 Ring Protocol network design                               |
| 20.7 Notes on Ring Protocol usage                               |

## 20.1 Overview of the Ring Protocol

### 20.1.1 Overview

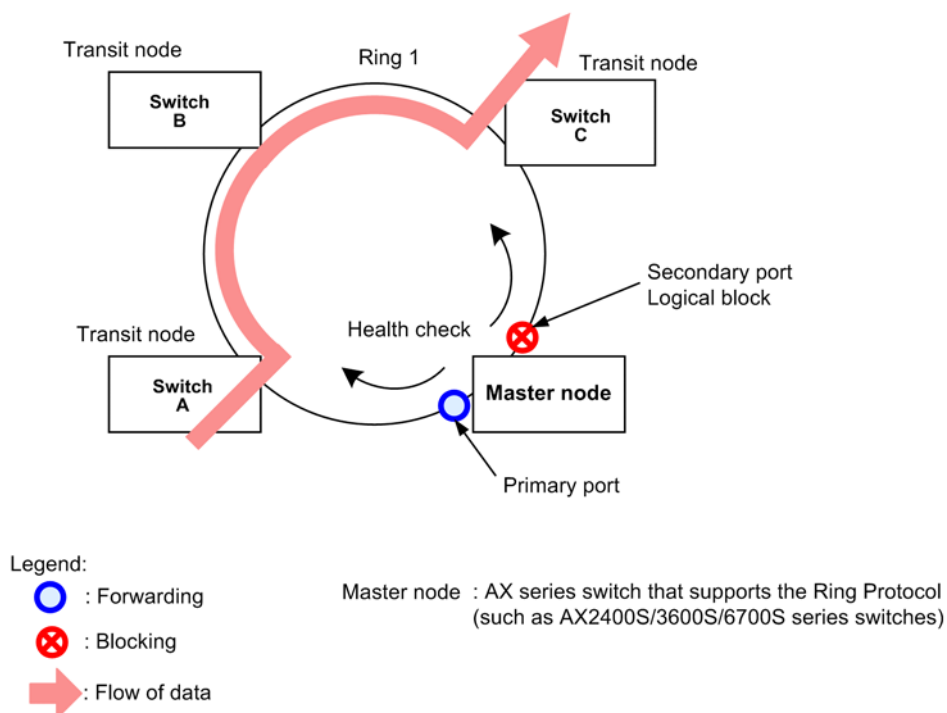
The Ring Protocol is a Layer 2 network redundancy protocol that detects faults in networks in which switches are connected in rings, and performs high-speed path switching accordingly.

Spanning Tree Protocols can be used as a Layer 2 network redundancy protocol, but suffer from shortcomings such as slow convergence for switching when faults occur. The Ring Protocol can be used to ensure that the path switching for when faults occur is performed at high speed. By using ring topology, the need for transmission paths and interfaces is reduced when compared to a mesh topology.

A switch in a ring topology (where the Ring Protocol is used) can be a master node or a transit node. The Switch supports the transit node functionality only. This manual describes the use of the Switch as a transit node. For details about master nodes, see the manuals for AX series switches that support the master node functionality.

The following figure provides an overview of a ring network based on the Ring Protocol.

**Figure 20-1** 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 switch paths and restore communication.

## 20.1.2 Features

### (1) Ethernet-based ring networks

The Ring Protocol is an Ethernet-based network redundancy protocol. Whereas conventional ring networks typically use dual-link fiber optics such as with FDDI, the Ring Protocol can be used to build ring networks using Ethernet.

The following figure shows an example Ring Protocol application.

**Figure 20-2** Example Ring Protocol application (part 1)

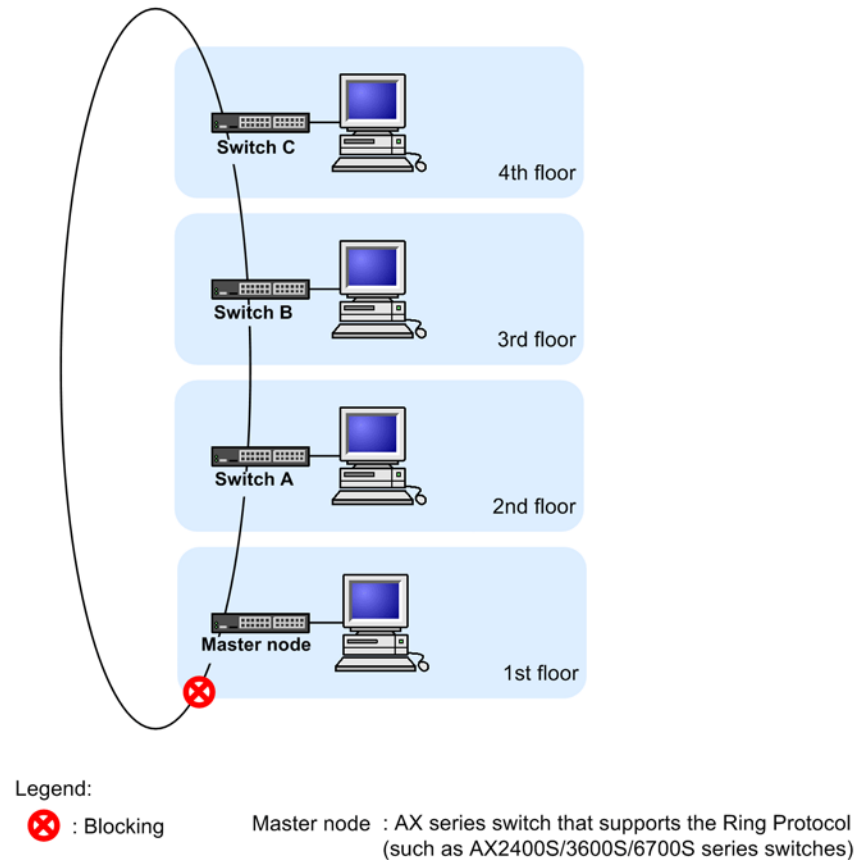
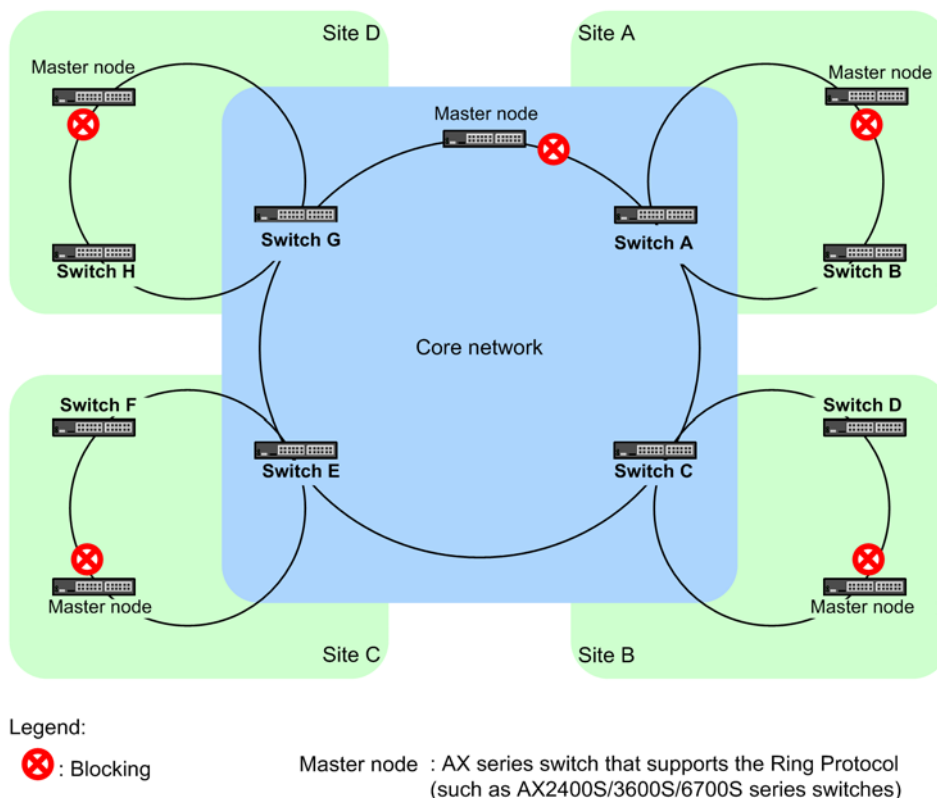


**Figure 20-3** Example Ring Protocol application (part 2)**(2) Simple operation method**

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 operations are primarily performed by the master node, and the other transit nodes switch paths according to instructions from the master node.

**(3) Control frames**

The Ring Protocol uses its own control frames. These control frames are used for monitoring the ring status by the master node, and in instructions for switching paths from the master node to transit nodes. Because control frame sending and reception are 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.

### 20.1.3 Supported specifications

The following table describes the items and specifications supported by the Ring Protocol.

**Table 20-1** 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                                                     | N                                                         |
|                                           | Transit node                                                     | Y                                                         |
|                                           | Shared nodes                                                     | N                                                         |
| Maximum number of ring IDs per switch     |                                                                  | 4                                                         |
| 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                         | 255                                                       |
| Sending intervals for health check frames |                                                                  | Depends on the master node.                               |
| Fault monitoring time                     |                                                                  | Depends on the master node.                               |
| Load balancing method                     |                                                                  | Depends on the master node.                               |
| 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                    | Depends on the master node.                               |
|                                           | Multi-fault monitoring time                                      | Depends on the master node.                               |

Legend Y: Supported, N: Not supported

## 20.2 Basic Ring Protocol principles

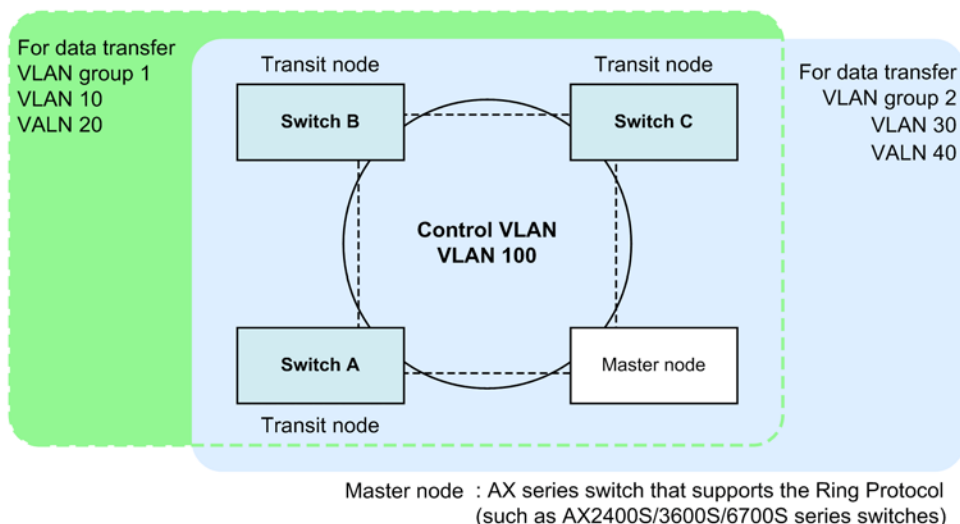
### 20.2.1 Network configuration

The following shows the basic network configurations when the Ring Protocol is used, and the positions of the Switches.

#### (1) Single ring configuration

The following figure shows the single ring configuration and the positions of the Switches.

**Figure 20-4** Single ring configuration

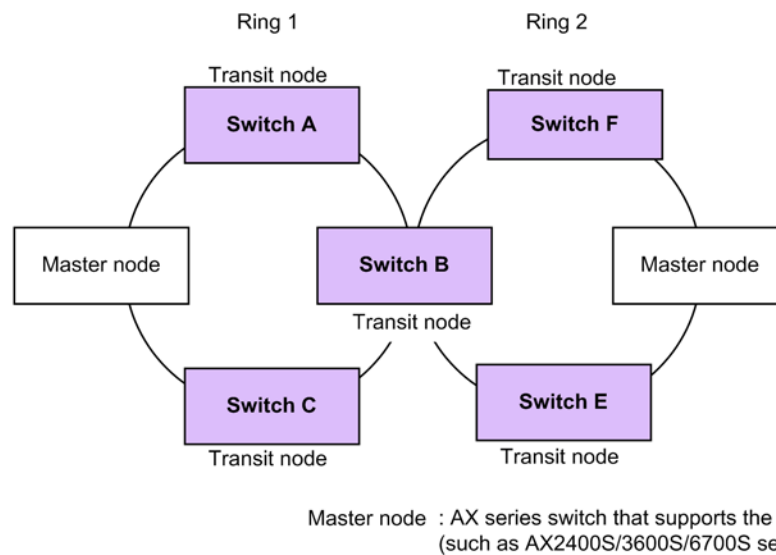


A single ring configuration consisting of one master node and multiple transit nodes is called a *single ring configuration*. The nodes in the ring are connected as ring ports by physical ports or link aggregations. Note that the same VLAN must be used as the control VLAN for all nodes in the ring, and 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

The figure below shows the positions of the Switches in a multi-ring configuration.

In this type of multi-ring configuration, the neighboring rings are connected at one node.

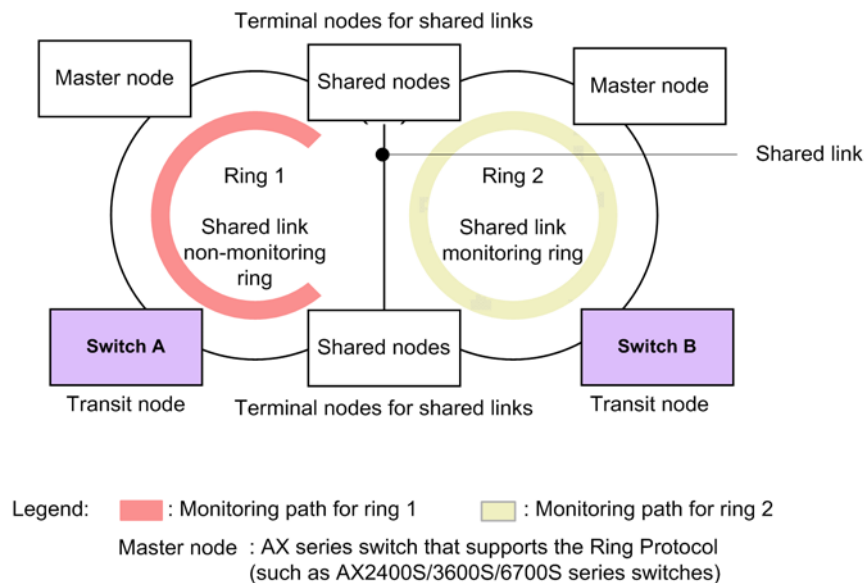
**Figure 20-5** Multi-ring configuration

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

The figure below shows the positions of the Switches in a multi-ring configuration with shared links.

In this type of multi-ring configuration, neighboring rings are connected at two or more nodes.

**Figure 20-6** Multi-ring configuration with shared links

When multiple single rings are connected by multiple nodes, links are shared by multiple rings. These links are called *shared links*, and multi-ring configuration with these links is called a *multi-ring configuration with shared links*. On the other hand, when, as in (2), multiple single rings are connected by a single node, because no shared links exist, this is called a *multi-ring configuration without shared links*.

## 20.2.2 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.

### 20.2.3 Fault monitoring methods

Ring faults are monitored under the Ring Protocol by the master node. For details, see the manuals that describe master nodes.

### 20.2.4 Switching communication paths

When a ring fault is detected by the master node, a control frame called a flush control frame is sent to the transit nodes that have the same control VLAN to request that MAC address table entries be cleared. When a Switch, as a transit node, receives this flush control frame, it clears MAC address table entries for the ring port. Because of this, flooding occurs until MAC address learning is performed. MAC address learning is performed by sending and receiving frames on the new path, and communication path switching is completed.

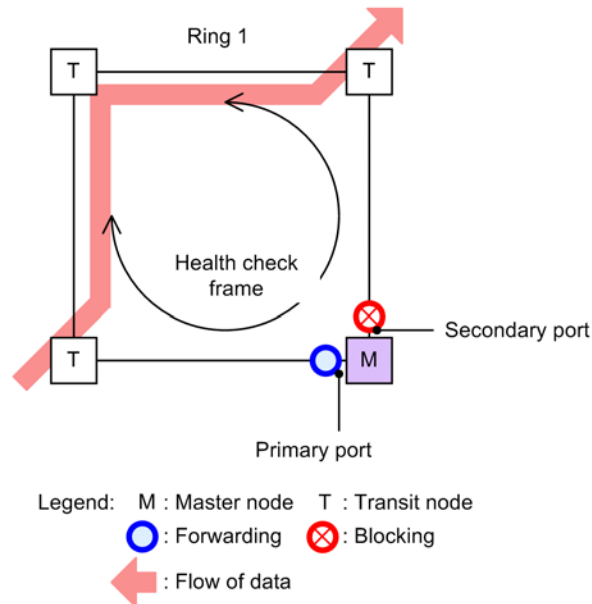


## 20.3 Overview of single ring operation

### 20.3.1 Normal ring operation

The following figure shows normal operation for a single ring.

**Figure 20-7** Normal ring operation



#### (1) Master node operation

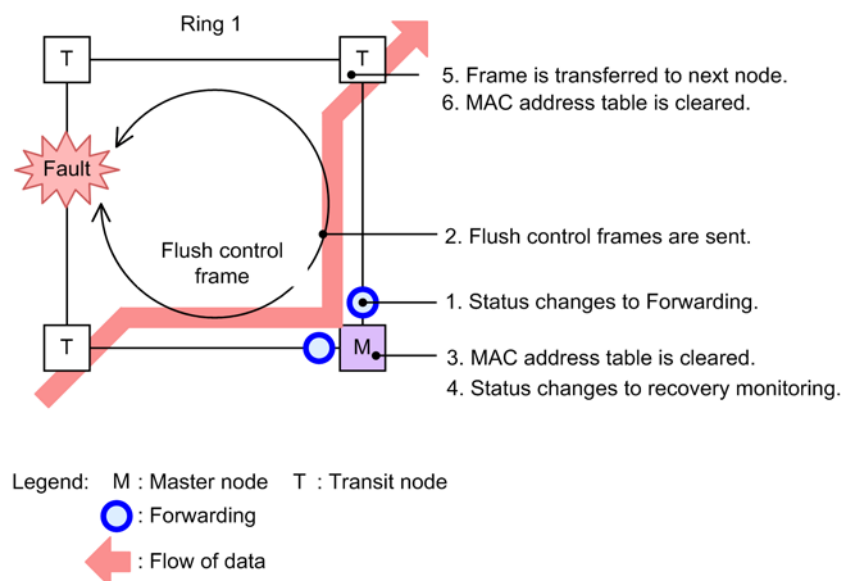
To prevent fault misdetection due to one-way link faults, health check frames are sent from two ring ports. Monitoring is performed to check that health check frames in both directions are received within the pre-determined time. Data frame transfer is performed on the primary port. Because the secondary 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.

### 20.3.2 Operation when a fault is detected

The following figure shows operation when a ring fault has been detected for a single ring.

**Figure 20-8** 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 20-2** VLAN status of rings for data transfer when a fault is detected

| Ring port      | Before (normal) | After (fault) |
|----------------|-----------------|---------------|
| Primary port   | Forwarding      | Forwarding    |
| Secondary port | Blocking        | Forwarding    |

2. Flush control frames are sent.

Flush control frames are sent from the primary port and secondary port of the master node.

3. The MAC address table is cleared.

The MAC address table entries pertaining to the ring port are cleared. Clearing the MAC address table entries allows paths to be switched quickly.

4. The monitoring status is changed.

When a ring fault is detected, the master node changes from the fault monitoring status to the recovery monitoring status.

**(2) Transit node operation**

The following operation is performed on a transit node that receives a flush control frame sent from a master node detecting a fault:

5. Flush control frames are transferred.

Any received flush control frames are transferred to the next node.

6. The MAC address table is cleared.

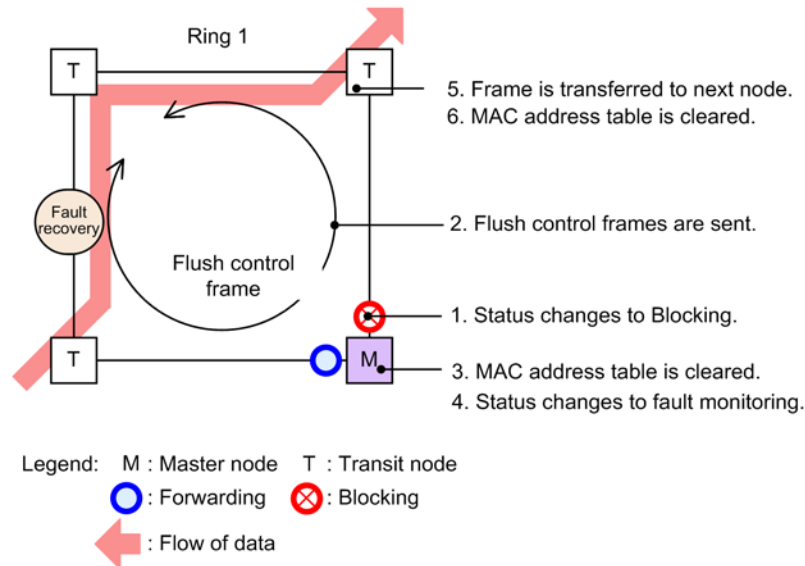
The MAC address table entries pertaining to the ring port are cleared. Clearing the

MAC address table entries allows paths to be switched quickly.

### 20.3.3 Operation when recovery is detected

The following figure shows operation when recovery from a ring fault is detected for a single ring.

**Figure 20-9** 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 20-3** 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 switching to the 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 switching to the 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*) of the ring port. The reception hold time for flush control frames (*forwarding-shift-time*) is set when recovery from a link fault on a ring port has occurred.

## 20.4 Overview of multi-ring operation

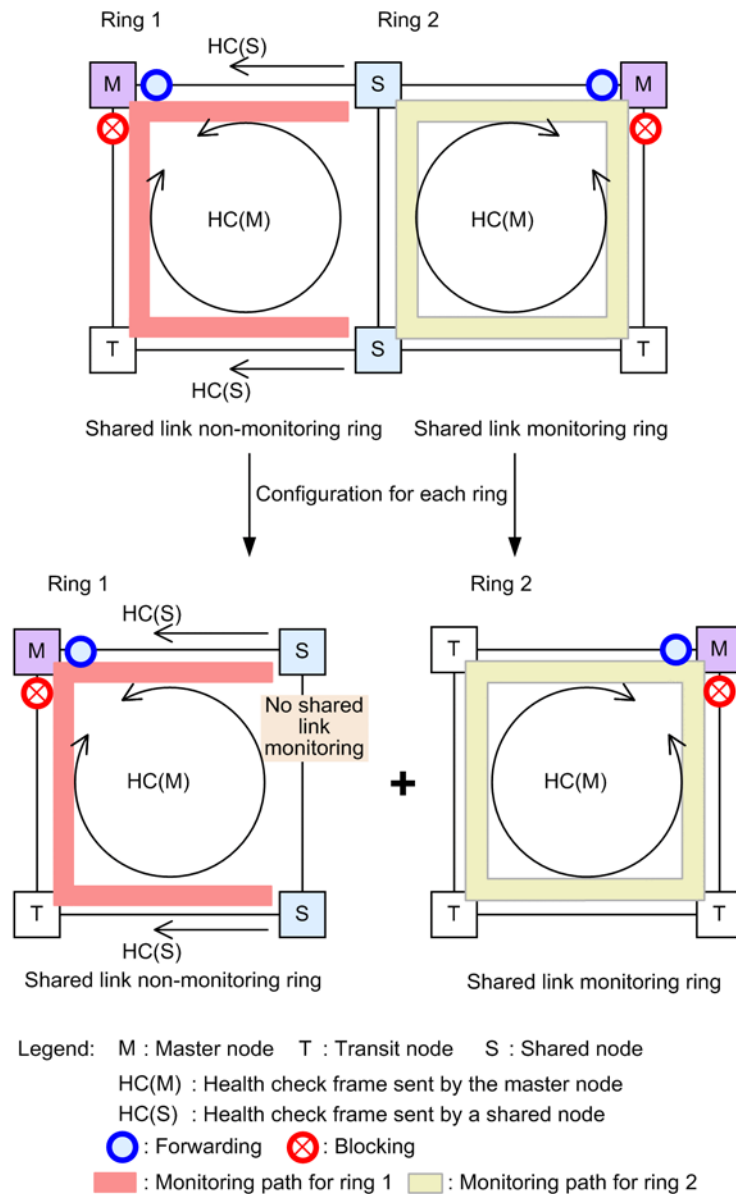
The following explains multi-ring configurations, focusing on those with shared links. For details about multi-ring configurations without shared links, because operation is the same as for single rings, see *20.3 Overview of single ring operation*.

In this section, *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.

### 20.4.1 Normal ring operation

The following figure shows normal operation for a multi-ring configuration with shared links.

**Figure 20-10** Normal ring status

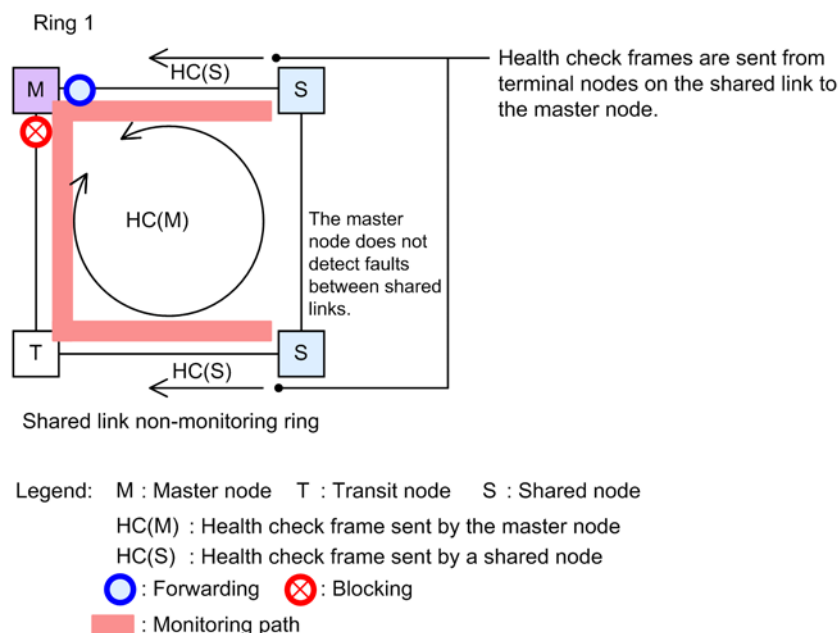


#### (1) Shared link non-monitoring rings

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 20-11** 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

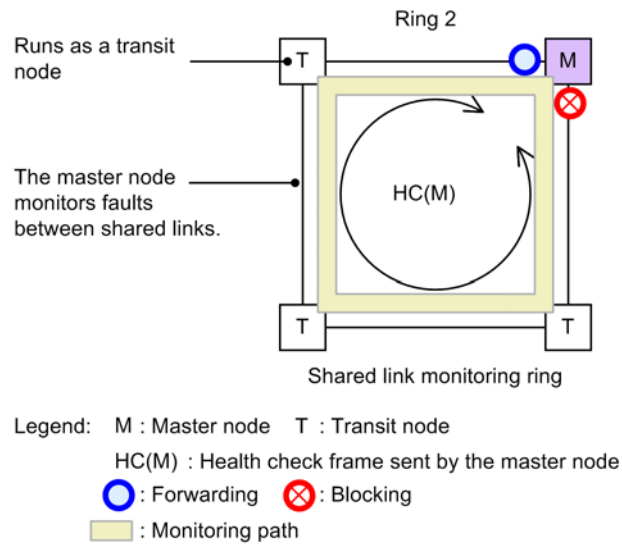
Transit node operation is the same as for single rings. Transit nodes do not monitor HC(M)s and HC(S)s. When an HC(M) or HC(S) is received, it is transferred to the next node in the ring. Data frame transfer is performed on both ring ports.

### (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 as for a single ring, as master nodes or transit nodes.

**Figure 20-12** 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**

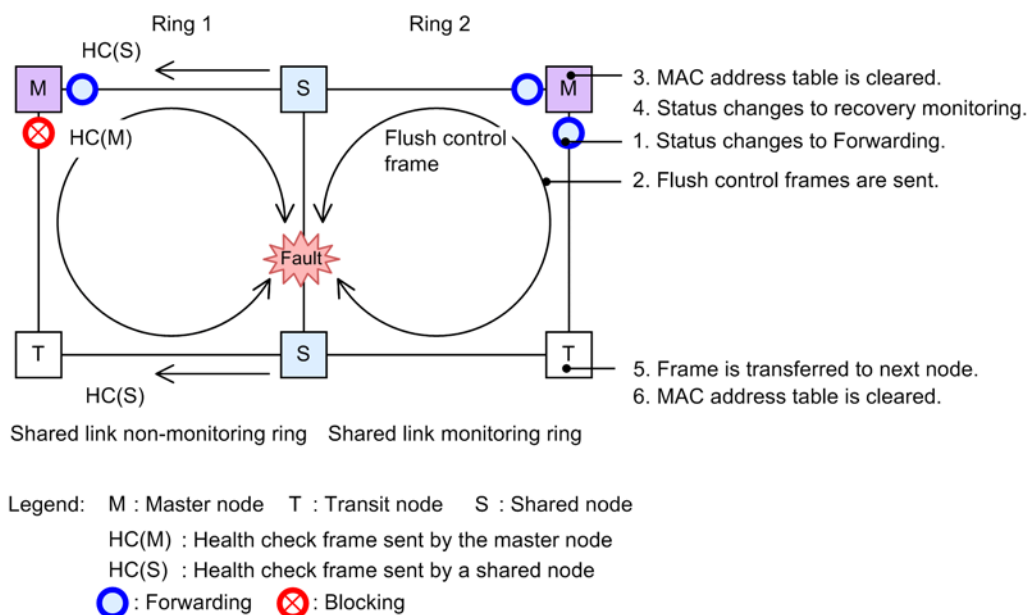
Transit node operation is the same as for single rings. Transit nodes do not monitor the HC(M)s sent by the master node. When an HC(M) is received, it is transferred to the next node in the ring. Data frame transfer is performed on both ring ports.

**20.4.2 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 20-13** 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.

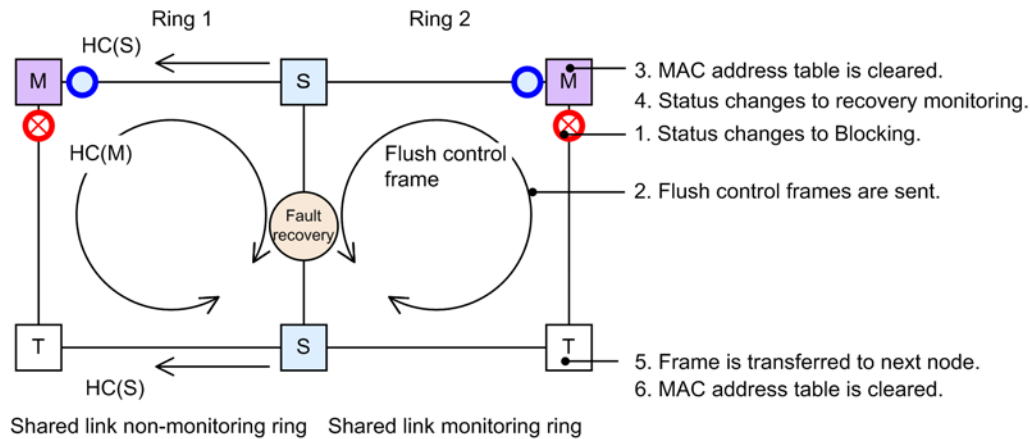
**(c) Master node and transit node operation for shared link non-monitoring rings**

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 20-14** Operation during shared link recovery

Legend: M : Master node    T : Transit node    S : Shared node  
 HC(M) : Health check frame sent by the master node  
 HC(S) : Health check frame sent by a shared node  
 Blue circle : Forwarding    Red X : Blocking

#### (a) Master node operation for shared link monitoring rings

When a ring fault has been detected, and the master node receives an HC(M) it sent itself, it determines that recovery from the ring fault has occurred. As with a single ring, the following restoration operations are performed:

1. The VLAN status of the ring for data transfer is changed.
2. Flush control frames are sent.
3. The MAC address table is cleared.
4. The monitoring status is changed.

#### (b) Transit node operation for shared link monitoring rings

As with single rings, the following operations are performed when a flush control frame sent from the master node is received:

5. Flush control frames are transferred.
6. The MAC address table is cleared.

#### (c) Master node and transit node operation for shared link non-monitoring rings

Because the master node in a shared link non-monitoring ring does not detect ring faults, no restoration is performed, including for transit nodes.

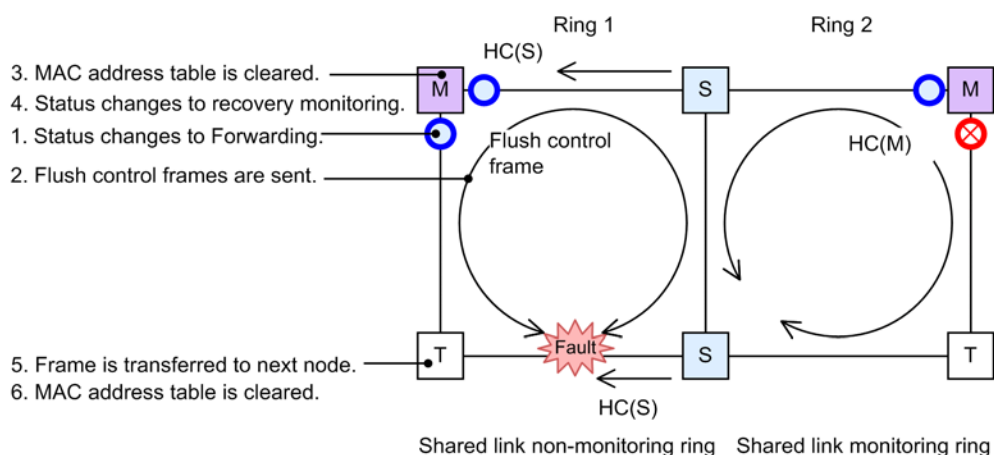
### 20.4.3 Operation for faults and restoration other than for shared links in a shared link non-monitoring ring

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 20-15** Operation during a ring fault other than for shared links on shared link non-monitoring rings



Legend: M : Master node T : Transit node S : Shared node

HC(M) : Health check frame sent by the master node

HC(S) : Health check frame sent by a shared node

○ : Forwarding ⊗ : Blocking

#### (a) Master node operation for shared link non-monitoring rings

The master node of a shared link non-monitoring ring detects a ring fault when it receives neither the two-way HC(M) sent by itself nor the HC(S) sent by a shared node. As with a single ring, the following operations are performed for the master node detecting the fault:

1. The VLAN status of the ring for data transfer is changed.
2. Flush control frames are sent.
3. The MAC address table is cleared.
4. The monitoring status is changed.

#### (b) Transit node and shared node operation for shared link non-monitoring rings

As with single rings, the following operations are performed when a flush control frame sent from the master node is received:

5. Flush control frames are transferred.
6. The MAC address table is cleared.

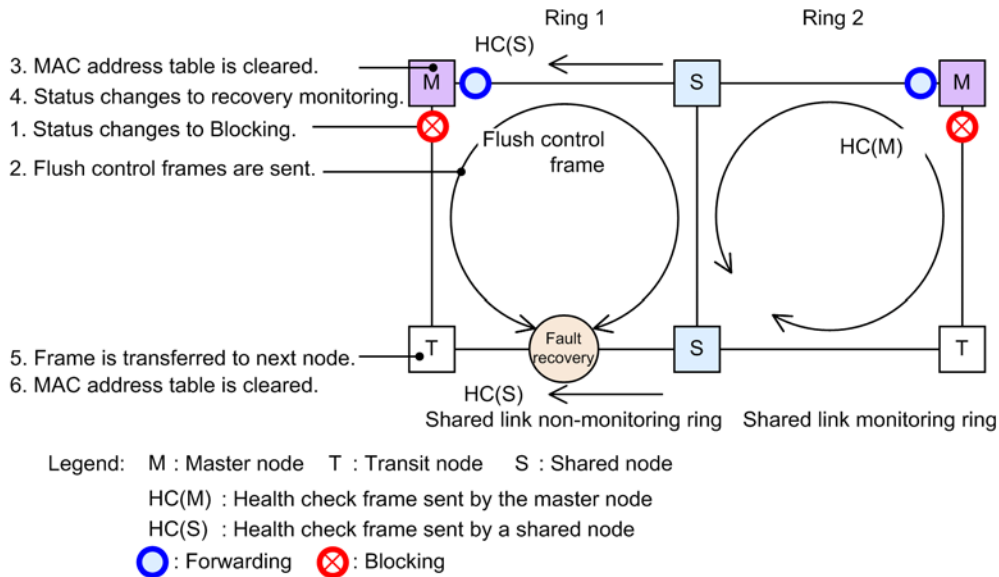
#### (c) Master node and transit node operation for shared link monitoring rings

Because no faults occur within a shared link monitoring ring, fault operation is not performed.

### (2) Operation when recovery is detected

The following figure shows operation when a fault is restored other than for shared links in a shared link non-monitoring ring.

**Figure 20-16** 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 are received from both directions, recovery from the ring fault is determined. As with a single ring, the following restoration operations are performed:

1. The VLAN status of the ring for data transfer is changed.
2. Flush control frames are sent.
3. The MAC address table is cleared.
4. The monitoring status is changed.

**(b) Transit node and shared node operation for shared link non-monitoring rings**

As with single rings, the following operations are performed when a flush control frame sent from the master node is received:

5. Flush control frames are transferred.
6. The MAC address table is cleared.

**(c) Master node and transit node operation for shared link monitoring rings**

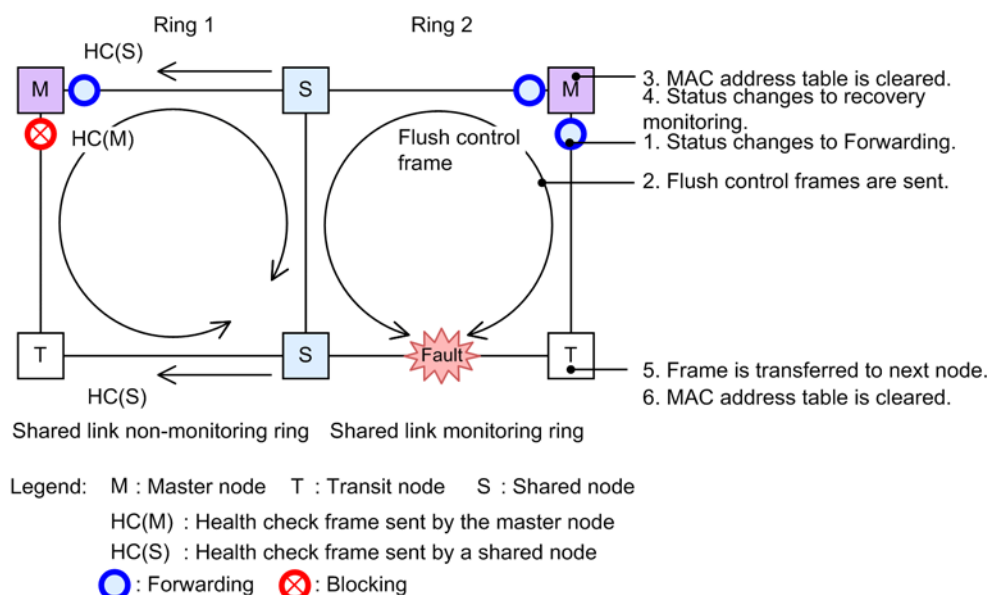
Because no faults occur within a shared link monitoring ring, restoration is not performed.

#### 20.4.4 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 20-17** 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 occurs 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.

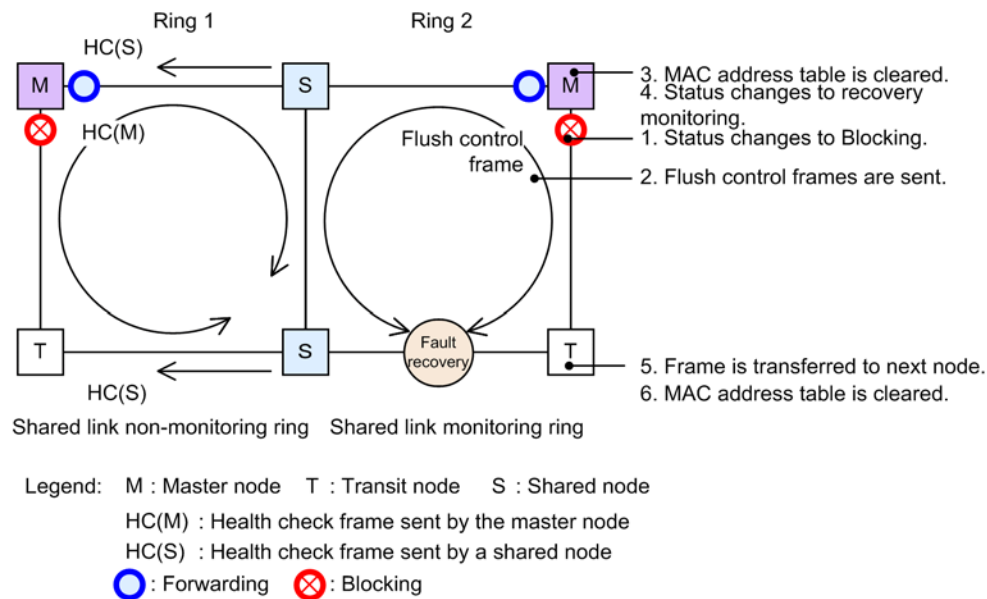
**(c) Master node and transit node (shared node) operation for shared link non-monitoring rings**

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 20-18** 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.

## 20.5 Multi-fault monitoring functionality for the Ring Protocol

### 20.5.1 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 switch 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.

Note that the Switch supports only transit nodes (not including terminal nodes).

**Figure 20-19** Example of a fault on a shared link monitoring ring

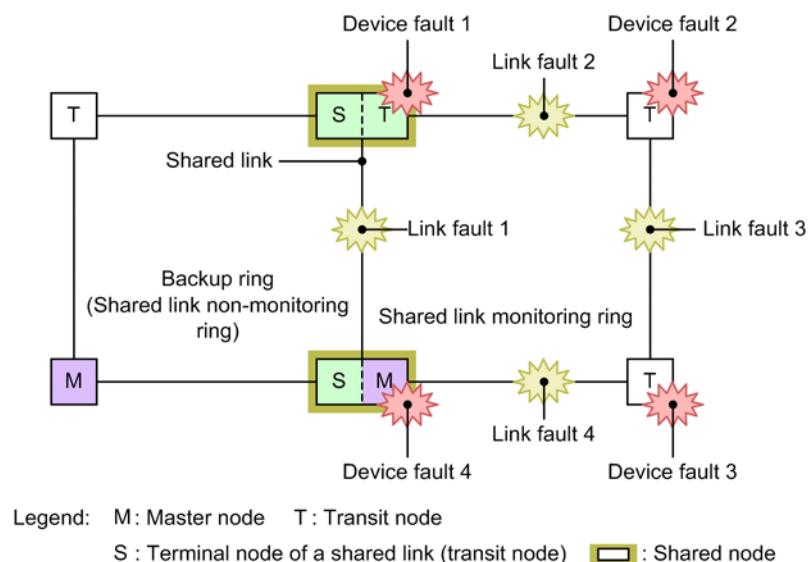


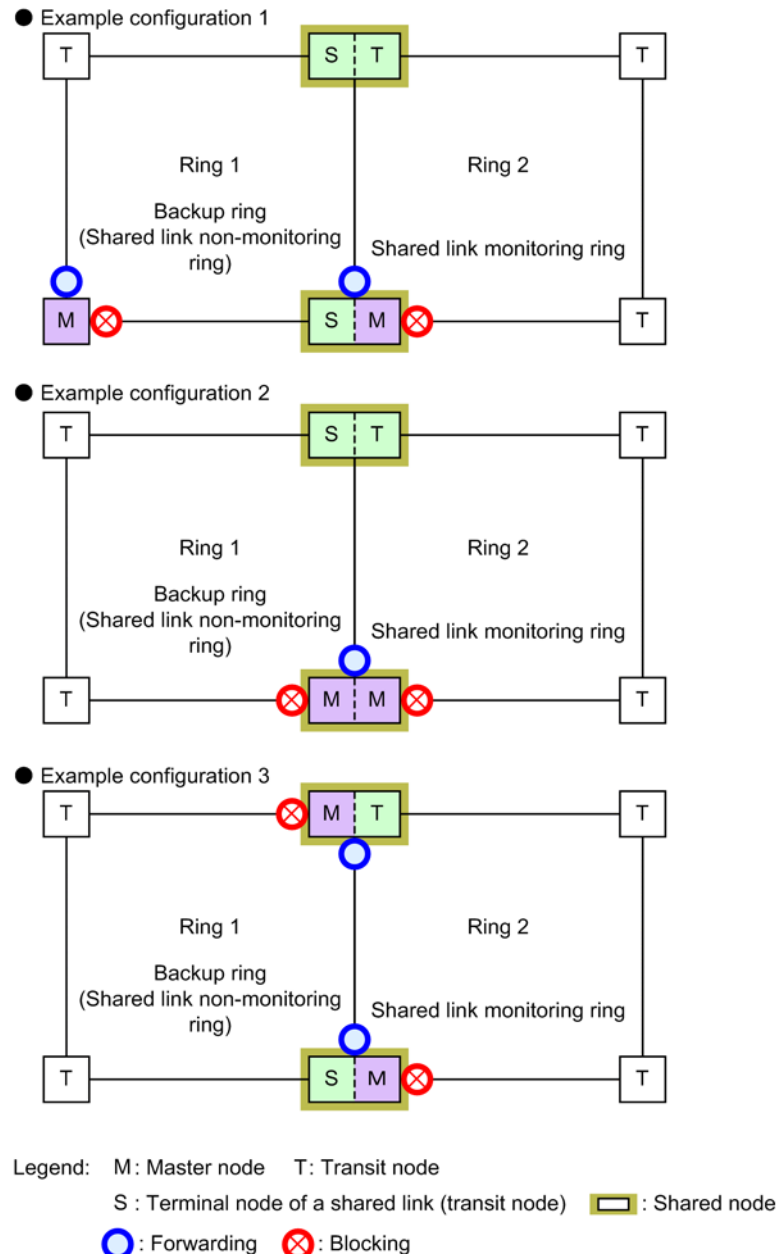
**Table 20-4** Combinations of faults that can be detected by the multi-fault monitoring functionality

| Failure type | Detectable combinations                 |                                  |
|--------------|-----------------------------------------|----------------------------------|
| Link fault   | Link fault 1 (shared link fault)        | Link fault 2 (other link fault)  |
|              | Link fault 1 (shared link fault)        | Link fault 3 (other link fault)  |
|              | Link fault 1 (shared link fault)        | Link fault 4 (other link fault)  |
| Switch fault | Switch fault 1 (shared node fault) only |                                  |
|              | Switch fault 4 (shared node fault) only |                                  |
|              | Switch fault 2 (transit node fault)     | Link fault 1 (shared link fault) |
|              | Switch fault 3 (transit node fault)     | Link fault 1 (shared link fault) |

### 20.5.2 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 20-20** Basic configuration example for multi-fault monitoring



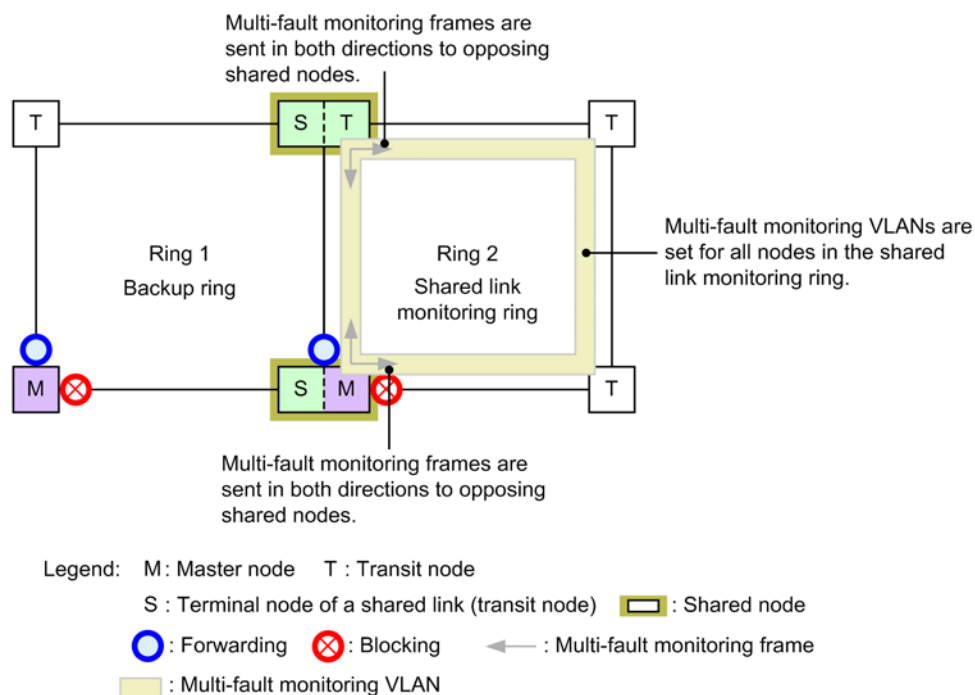
### 20.5.3 Overview of operation for multi-fault monitoring

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 Switch supports receipt and forwarding of multi-fault monitoring frames and clearing of MAC address table entries.

The following figure gives an overview of multi-fault monitoring operation.

**Figure 20-21** 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 (2) *Shared link monitoring rings* in 20.4.1 *Normal ring operation*.

For shared nodes, multi-faults for shared link monitoring rings are monitored. Shared nodes send multi-fault monitoring frames from both ring ports, and monitor whether multi-fault monitoring frames sent from both ring ports by opposing shared nodes are received within the pre-determined time.

### (2) Operation for each node in a backup ring

For details about the operation for master nodes and transit nodes in a backup ring, because operation is the same as that for multi-rings, see (1) *Shared link non-monitoring rings* in 20.4.1 *Normal ring operation*.

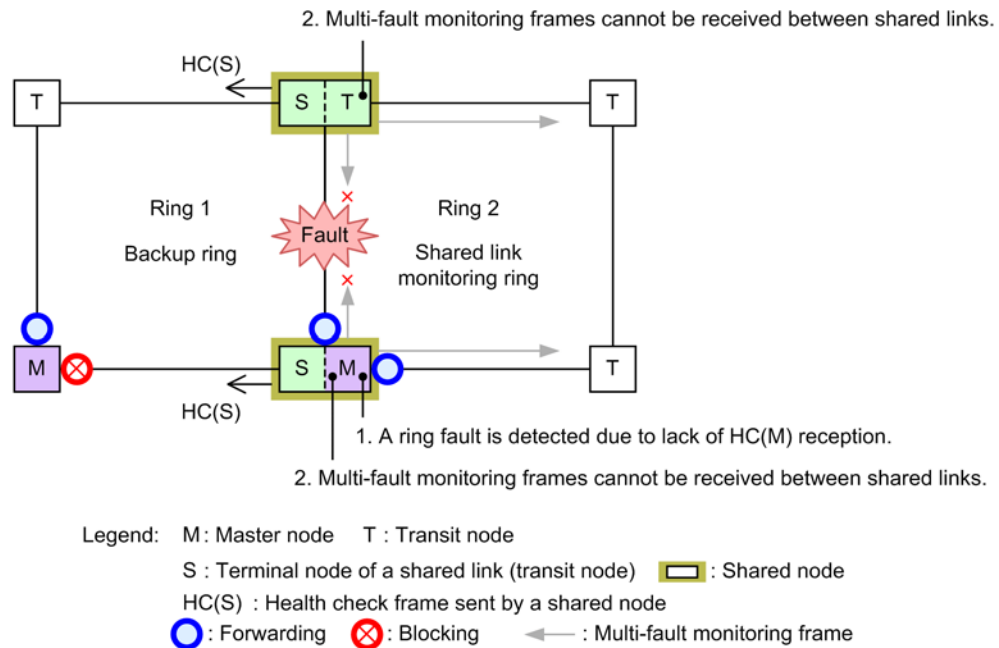
## 20.5.4 Operation when multi-faults occur

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 20-22** Operation during shared link faults**(a) Operation for each node in a shared link monitoring ring**

1. A ring fault is detected because HC(M)s are not received.

The master node can no longer receive HC(M)s from both directions, and detects a ring fault. For details about master node and transit node operation during ring fault detection, because operation is the same as multi-ring operation, see *(1) Operation when a fault is detected in 20.4.2 Operation for shared link faults and restoration*.

2. Multi-fault monitoring frames cannot be received between shared links.

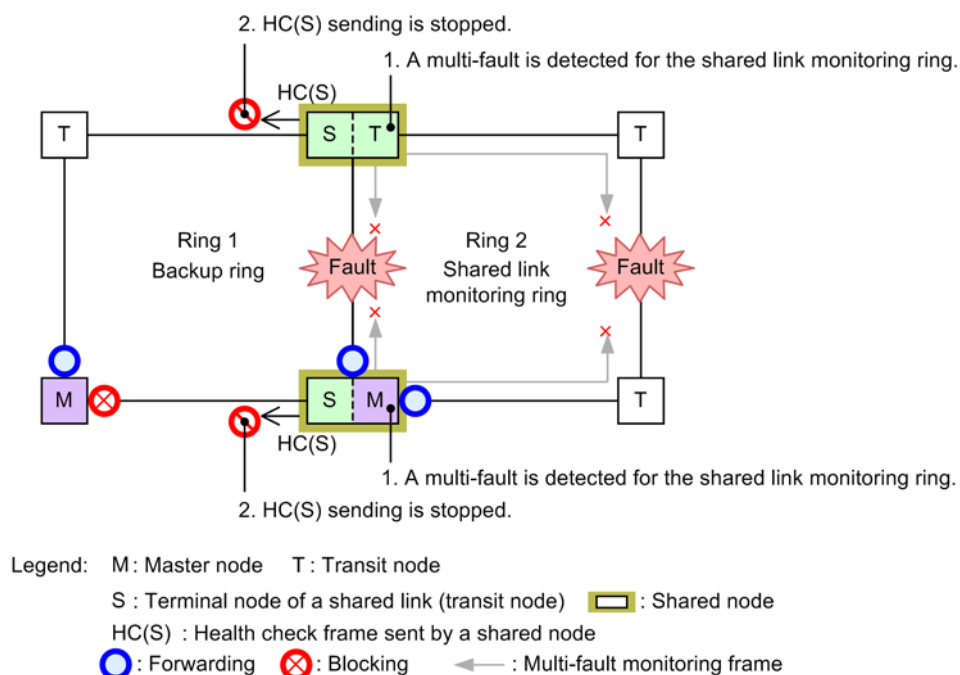
Shared nodes can no longer receive multi-fault monitoring frames between shared links, but because reception is still possible on the other ring port, multi-fault monitoring continues.

**(b) Operation for each node in a backup ring**

HC(M)s sent by the master node can no longer be received on a backup ring, but because HC(S)s sent by shared nodes can be received, no fault operation is performed.

**(2) Operation when multi-faults occur**

The following figure shows operation when multi-faults occur due to shared link faults or other link faults within a shared link monitoring ring.

**Figure 20-23** Operation when multi-faults occur**(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.

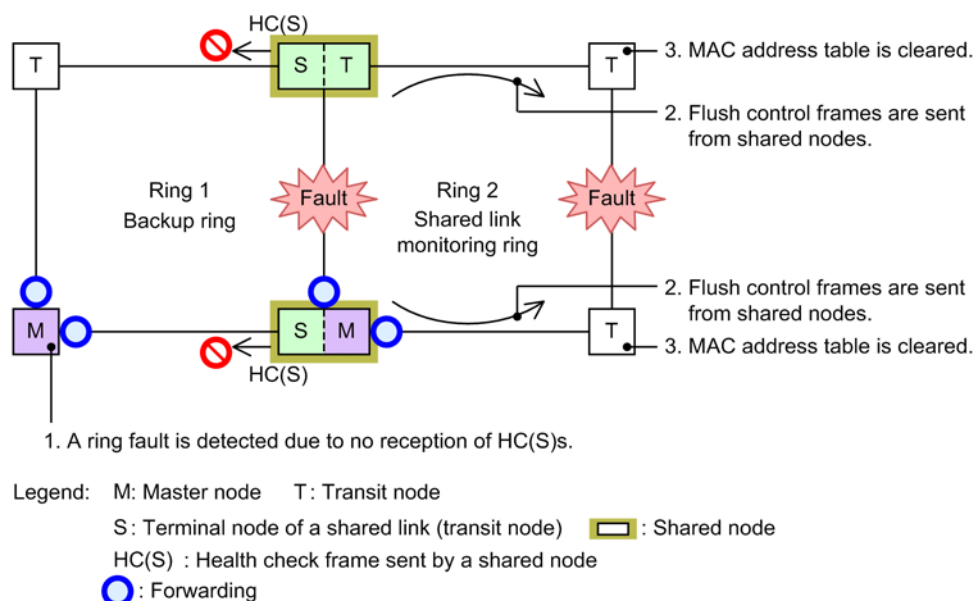
**(b) Operation for each node in a backup ring**

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 20-24** 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 (1) *Operation when a fault is detected* in 20.4.3 *Operation for faults and restoration other than for shared links in a shared link non-monitoring ring*.

**(b) Operation for each node in a shared link monitoring ring**

2. Flush control frames are sent from shared nodes.

When shared nodes receive a flush control frame from the master node of the backup ring, they send to the shared link monitoring ring only flush control frames that clear the MAC address table.

3. The MAC address table is cleared.

Transit nodes receive flush control frames sent from shared nodes, and clear the MAC address table.

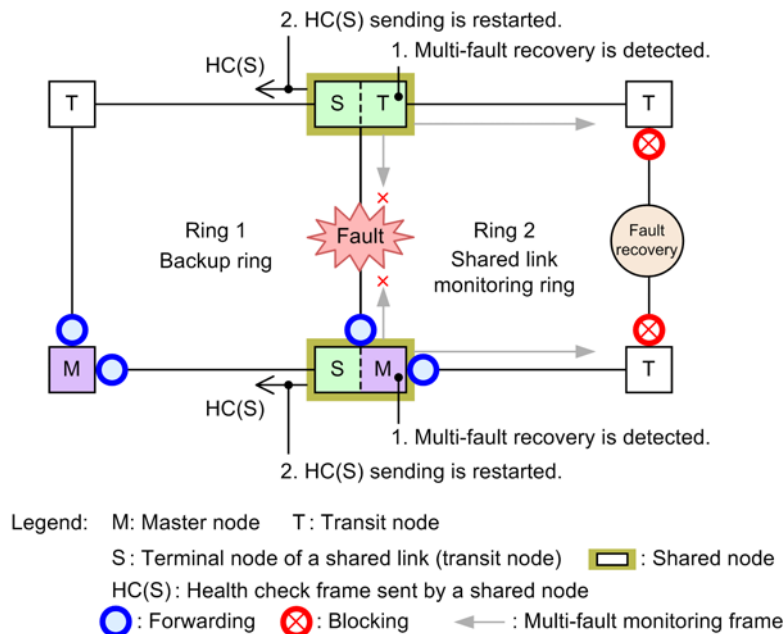
**20.5.5 Operation during multi-fault recovery**

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 20-25** 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**

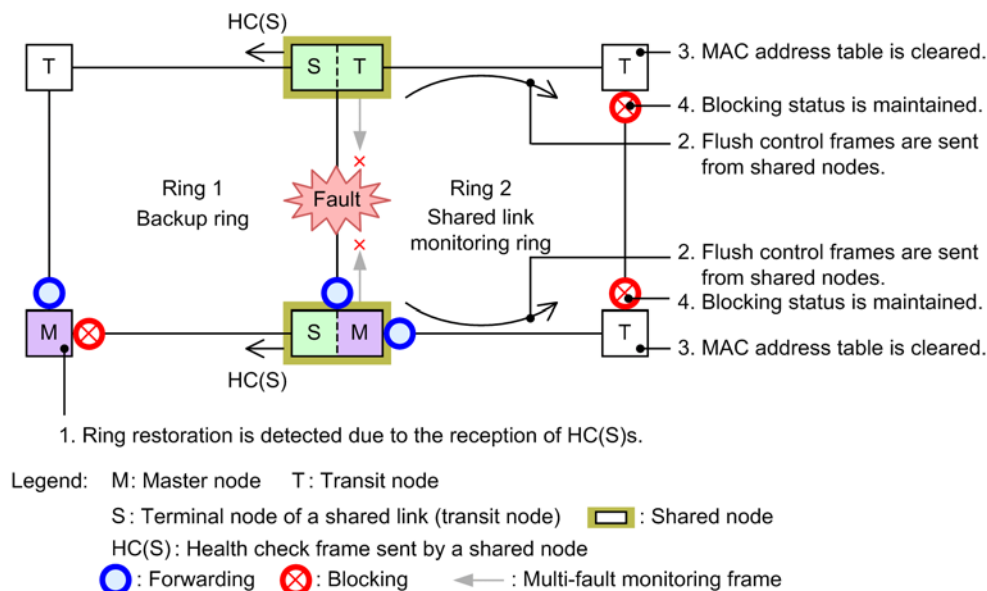
2. HC(S) sending is restarted.

The shared node that detected multi-fault recovery starts sending backup ring HC(S)s again.

**(2) Switchback operation from backup rings**

The following figure shows switchback operation from a backup ring.

**Figure 20-26** Switchback from backup rings

**(a) Operation for each node in a backup ring**

1. Ring restoration is detected due to reception of HC(S)s.

When the master node receives HC(S)s sent by shared nodes from both directions, it determines that recovery from the ring fault has occurred, and performs restoration operations. For details about operation for the master node and transit nodes when recovery is detected, because operation is the same as for multi-rings, see (2) *Operation when recovery is detected in 20.4.3 Operation for faults and restoration other than for shared links in a shared link non-monitoring ring.*

**(b) Operation for each node in a shared link monitoring ring**

2. Flush control frames are sent from shared nodes.

When shared nodes receive a flush control frame from the master node of the backup ring, they send to the shared link monitoring ring only flush control frames that clear the MAC address table.

3. The MAC address table is cleared.

Transit nodes receive flush control frames sent from shared nodes, and clear the MAC address table.

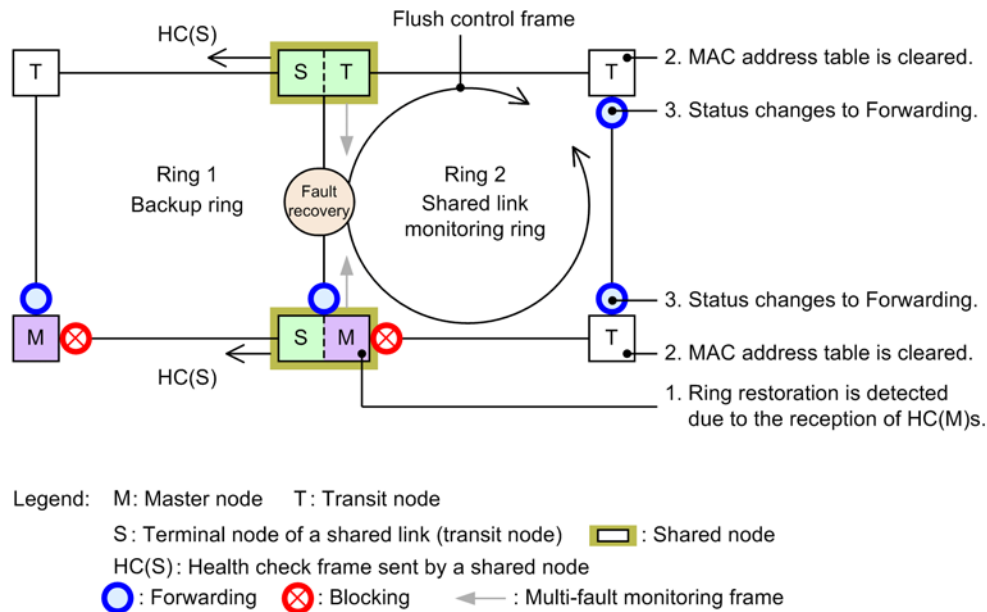
4. The Blocking status is maintained.

Blocking is maintained for the ring VLAN status of the ring ports after recovery from the link fault, because the master node has not detected ring restoration.

For details about when Blocking is cleared, see (11) *Communication during partial multi-fault recovery in 20.7 Notes on Ring Protocol usage.*

**(3) Operation during recovery from a shared link fault**

The following figure shows operation during shared link fault restoration.

**Figure 20-27** 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 (2) *Operation when recovery is detected* in 20.4.2 *Operation for shared link faults and restoration*.

2. The MAC address table is cleared.

Transit nodes receive flush control frames sent from the master node, and clear the MAC address table.

3. The status is changes to Forwarding.

When transit nodes receive flush control frames sent from the master node, they change the ring VLAN status of the ring port after recovery from the link fault to Forwarding.

## 20.6 Ring Protocol network design

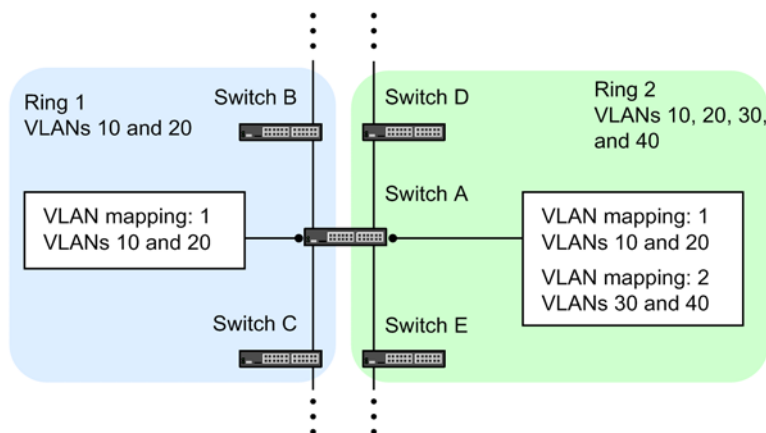
### 20.6.1 Using VLAN mappings

#### (1) VLAN mappings and VLANs for data transfer

When multiple ring IDs are set for a single switch, such as in a multi-ring configuration, the same VLAN needs to be set multiple times for each ring ID. In such cases, the list of VLANs used as data transfer VLANs (called *VLAN mapping*) can be set in advance to simplify data transfer VLAN settings in a multi-ring configuration, and prevent loops due to mistakes in configuration settings.

VLAN mappings assign VLANs used for data transfer to VLAN mapping IDs. These VLAN mapping IDs are set for VLAN groups, and are managed as data transfer VLANs.

**Figure 20-28** Example VLAN mapping assignment for each ring



### 20.6.2 Using forwarding-delay-time for control VLANs

When the Ring Protocol is run from the initial status at switch startup for a transit node, data transfer VLANs are logically blocked. Transit nodes remove this logical block when they receive a flush control sent from the master node. However, if the fault monitoring time (*health-check holdtime*) for the master node is long when the switch is restarted, status changes for the ring network might not be recognized. In this case, because the logical block is not released until the reception hold time for flush control frames (*forwarding-shift-time*) times out, the data VLAN for the transit node cannot communicate. Because operation is performed as follows when a forwarding transition time (*forwarding-delay-time*) is set for the control VLAN, this kind of case can be avoided.

1. The transit node performs an immediate logical block of the control VLAN during switch 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 switch startup). Therefore, communication is switched to an alternate path.
3. The transit node removes Blocking for the control VLAN, due to a timeout of the forwarding transition time (*forwarding-delay-time*) for the control VLAN.
4. The master node receives a health check frame, detects recovery, and sends a flush control frame.
5. The transit node receives this flush control frame, and removes the logical block on the data transfer VLAN. With this, communication on the data transfer VLAN is restarted, and restoration of the normal communication path is performed on the entire ring network.

#### (1) Relationship between the forwarding transition time for the control VLAN

**(forwarding-delay-time) and the reception hold time for flush control frames (forwarding-shift-time)**

Set a smaller value for the forwarding transition time for the control VLAN ([forwarding-delay-time](#)) than the value for the reception hold time for flush control frames for the data transfer VLAN ([forwarding-shift-time](#)). If you set a larger value than the value for the reception hold time for flush control frames ([forwarding-shift-time](#)), forwarding starts on the data transfer VLAN before the master node detects a fault, and a loop might occur.

**20.6.3 Prohibited Ring Protocol configurations**

For details about prohibited configurations, see the manuals that describe the master node.

**20.6.4 Prohibited configurations for the multi-fault monitoring functionality**

For details about prohibited configurations, see the manuals that describe the master node.

## 20.7 Notes on Ring Protocol usage

### (1) Notes on use with other functionality

For details, see *15.3 Compatibility between Layer 2 switch functionality and other functionality*.

### (2) 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.

### (3) Ring VLAN status for transit nodes

For transit nodes, when a fault occurs for a switch or ring port, and recovery succeeds, the ring VLAN status of the ring port is set to Blocking to prevent loops from occurring. One of the ways in which this Blocking status is cleared is when the reception hold time (*forwarding-shift-time*) for flush control frames times out. When the reception hold time for flush control frames (*forwarding-shift-time*) is shorter than the health check sending interval of the master node (*health-check interval*), a loop might occur. This can happen if the transit node ring port changes to the Forwarding status before the master node detects recovery from the ring fault and changes the secondary port to the Blocking status. Therefore, set the reception hold time for flush control frames (*forwarding-shift-time*) to a value greater than the health check sending interval (*health-check interval*).

### (4) VLAN configurations in multi-rings with shared links

For shared links used in common among multiple rings, the same VLAN needs to be used for each ring. Port Forwarding/Blocking control for VLANs between shared links is performed by shared link monitoring rings. Therefore, when different VLANs are used for shared link monitoring/non-monitoring rings, VLANs used for the shared link non-monitoring rings remain in Blocking status, and are no longer able to communicate.

### (5) Building networks when the Ring Protocol is used

Fundamentally, networks using the Ring Protocol have looped configurations. Take the measures below to avoid loops when building networks.

- Before setting the Ring Protocol configuration, use `shutdown` or another command to take the ring port (physical port or channel group) of the ring configuration node down.
- Bring the ring port back up (such as by clearing the `shutdown` command) when the Ring Protocol is set for all switches in the network.

### (6) Configuration changes during operation

When changing the Ring Protocol configuration during operation, take care that loops do not occur. Take the following action for the target configuration:

1. When changing the control VLAN (using the `control-vlan` configuration command) or a data transfer VLAN (using the `axrp vlan-mapping` and `vlan-group` configuration commands):

When changing the control VLAN or a data transfer VLAN that is used in a ring, which will cause loops on the network, stop the target VLAN or shut down the ring port in advance.

### (7) Interoperability

The Ring Protocol is functionality specific to the Switch. It cannot be used interoperably with third-party switches.



**(8) 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 *20.5 Multi-fault monitoring functionality for the Ring Protocol*.

**(9) Sending and receiving flush control frames when the master node switch restarts**

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).

**(10) 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.

**(11) Communication during partial multi-fault recovery**

Because the master node does not detect ring restoration during partial multi-fault recovery, the transit node ring port is logically blocked until the reception hold time (*forwarding-shift-time*) for flush control frames elapses. To clear the logical block status, either shorten the reception hold time for flush control frames (initial value:10 seconds), or recover remaining link faults to have the master node detect ring restoration. Also, when setting the reception hold time for flush control frames, set a value greater than the sending interval for multi-fault monitoring frames for the master node (using the *multi-fault-detection interval* configuration command). When a small value is set, loops might occur temporarily.

**(12) 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.



---

## 21. Settings and Operation for the Ring Protocol

This chapter explains example settings for the Ring Protocol.

---

|                    |
|--------------------|
| 21.1 Configuration |
|--------------------|

|                |
|----------------|
| 21.2 Operation |
|----------------|

---

## 21.1 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.

### 21.1.1 List of configuration commands

The following table describes the configuration commands used to configure the Ring Protocol on the Switch.

**Table 21-1** List of configuration commands

| Command name                            | Description                                                                                    |
|-----------------------------------------|------------------------------------------------------------------------------------------------|
| <code>axrp</code>                       | Sets the ring ID.                                                                              |
| <code>axrp vlan-mapping</code>          | Sets the VLAN mapping and VLANs participating in the mapping.                                  |
| <code>axrp-ring-port</code>             | Sets the ring port.                                                                            |
| <code>control-vlan</code>               | Sets the VLAN to be used as a control VLAN.                                                    |
| <code>disable</code>                    | Disables the Ring Protocol functionality.                                                      |
| <code>forwarding-shift-time</code>      | Sets the reception hold time for flush control frames.                                         |
| <code>mode</code>                       | Sets the operating mode for a ring.                                                            |
| <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 a ring.                                                          |
| <code>vlan-group</code>                 | Sets the VLAN group for which to run the Ring Protocol functionality, and the VLAN mapping ID. |

### 21.1.2 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

Stop Spanning Tree Protocols before using the Ring Protocol. For details about stopping Spanning Trees, see 19. *Spanning Tree Protocol*.

#### (2) Performing settings common to the Ring Protocol

Perform ring configuration settings and common settings that do not depend on the placement of the Switch within a ring.

- Ring ID
- Control VLAN
- VLAN mapping
- VLAN group

**(3) Setting the mode and port**

Perform ring configuration settings and settings related to the placement of the Switch within a ring. If the combination of settings contains a conflict, the Ring Protocol functionality will not operate properly.

- Mode
- Ring port

**(4) Setting various parameters**

The Ring Protocol functionality runs using the initial values if the following configurations are not set. To change these values, set them using commands.

- Disabling functionality
- Reception hold time for flush control frames

**21.1.3 Configuring ring IDs**

Points to note

The ring ID can be set. The same ring ID needs to be set for all switches belonging to the same ring.

Command examples

1. `(config)# axrp 1`  
Sets the ring ID to 1.

**21.1.4 Setting control VLANs****(1) Setting control VLANs**

Points to note

You can specify the VLAN to be used as the control VLAN. Note that the following VLANs cannot be set:

- VLANs used as the data transfer VLAN
- VLANs that have VLAN IDs used for other 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

You can set the forwarding transition time for the control VLAN of a transit node for when the Ring Protocol is in the initial status. 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` configuration command). However, set a value smaller than that set for the reception hold time for flush control frames (value set for the `forwarding-shift-time` configuration

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)# control-vlan 2 forwarding-delay-time 10
(config-axrp)# exit
```

Sets the forwarding transition time for the control VLAN to 10 seconds.

### 21.1.5 Setting VLAN mappings

#### (1) Setting new VLANs

Points to note

VLANs used for data transfer can be bound to a VLAN mapping. A single VLAN mapping can be used on multiple rings as a common definition. As many as 128 VLAN mappings can be set. Multiple VLANs can be set for a VLAN mapping by using lists.

The VLAN for data transfer used within a ring network must be the same for all nodes. However, because only VLANs for VLAN mappings specified for VLAN groups need to match, there is no need to match the VLAN mapping IDs for all nodes in a ring network.

Command examples

1. 

```
(config)# axrp vlan-mapping 1 vlan 5-7
```

Sets VLAN IDs 5, 6, and 7 for VLAN mapping ID 1.

#### (2) Adding VLANs

Points to note

VLAN IDs can be added to VLAN mappings already set. When the ring to which an added VLAN mapping is applied is running, the mapping is reflected immediately. Also, when additions are applied for multiple rings, they are all applied 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

A VLAN ID can be deleted from a VLAN mapping already set. If the ring to which the deleted VLAN mapping is applied is running, the deletion is reflected immediately. Also, when deletions are applied for multiple rings, they are all reflected at the same time. If a VLAN mapping is changed during ring operation, a loop might occur.

Command examples

1. 

```
(config)# axrp vlan-mapping 1 vlan remove 8-9
```

Deletes VLAN IDs 8 and 9 from VLAN mapping ID 1.

### 21.1.6 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.

### 21.1.7 Settings for modes and ring ports (for single rings and multi-ring configurations without shared links)

*Figure 21-1 Single ring configuration* shows a single ring configuration, and *Figure 21-2 Multi-ring configuration without shared links* shows a multi-ring configuration without shared links.

**Figure 21-1** Single ring configuration

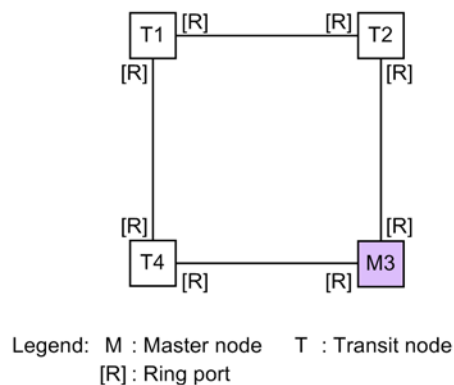
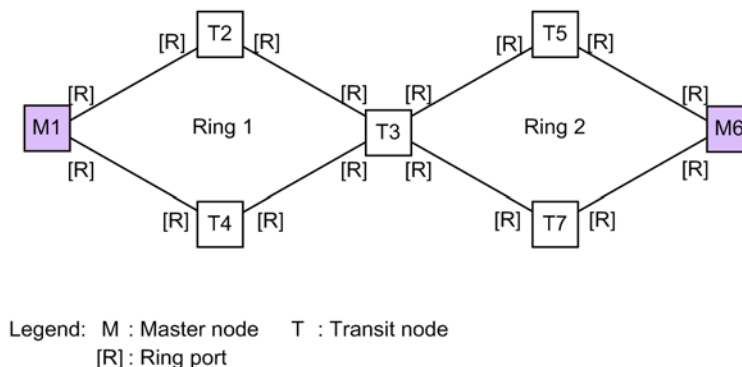


**Figure 21-2** Multi-ring configuration without shared links



The Switch supports transit nodes only. This section describes the transit node of the Switch. For details about the master node, see the manuals for AX series switches that support the master node functionality.

### (1) Transit node

#### Points to note

The operating mode can be set 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 21-1 Single ring configuration*, and the T2, T3, T4, T5, and T7 nodes in *Figure 21-2 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 fastethernet 0/1`

`(config-if)# axrp-ring-port 2`

`(config-if)# exit`

`(config)# interface fastethernet 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.

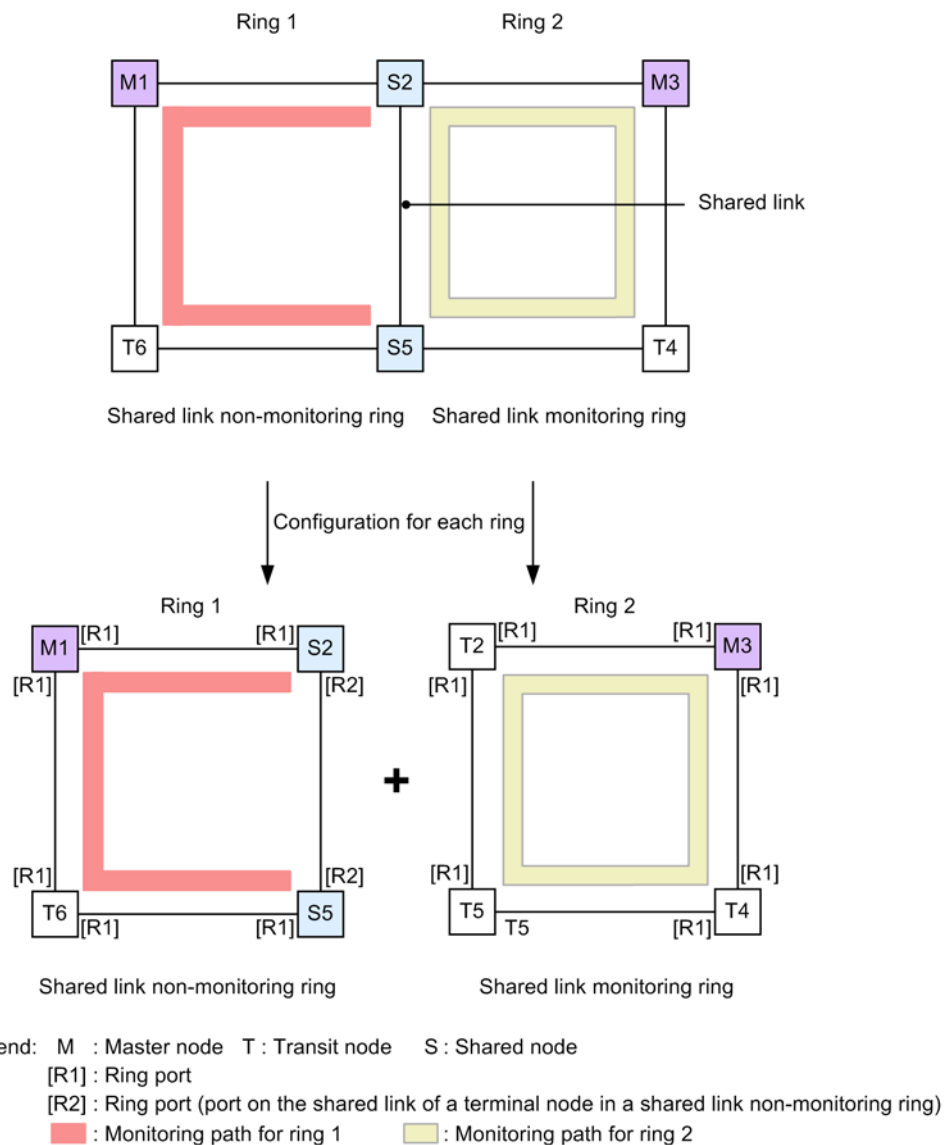
### 21.1.8 Configuring modes and ring ports (for multi-ring configurations with shared links)

This section gives the parameter setting patterns for modes and ring ports for multi-ring configurations with shared links.

#### (1) Multi-ring configurations with shared links (basic configuration)

The following figure shows a multi-ring configuration with shared links (basic configuration).



**Figure 21-3** Multi-ring configurations with shared links (basic configuration)**(a) Transit nodes for shared link monitoring rings**

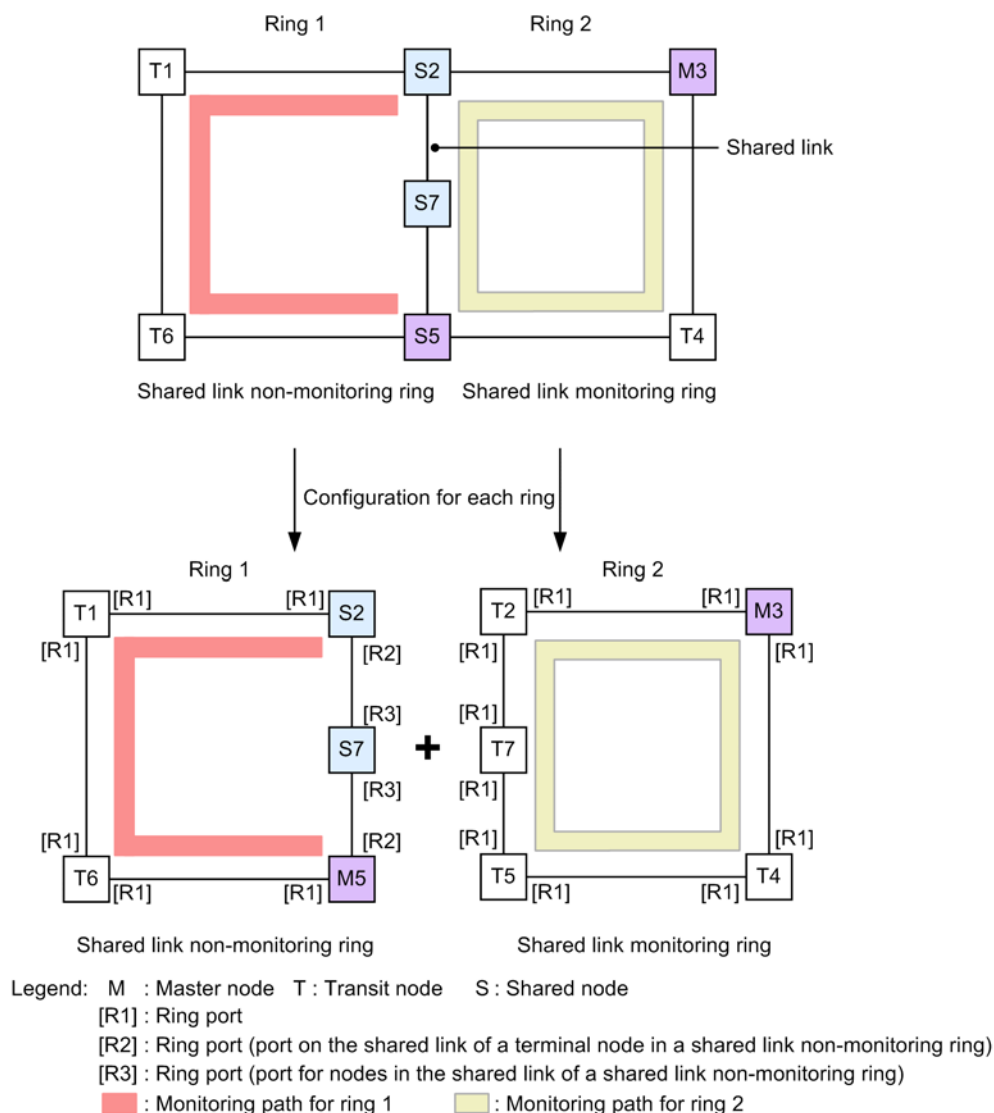
This is the same as transit nodes for a single ring. For details, see (1) *Transit node* in 21.1.7 *Settings for modes and ring ports (for single rings and multi-ring configurations without shared links)*. The T2, T4, and T5 nodes in *Figure 21-3 Multi-ring configurations with shared links (basic configuration)* correspond to this setting.

**(b) Transit nodes for shared link non-monitoring rings**

This is the same as transit nodes for a single ring. For details, see (1) *Transit node* in 21.1.7 *Settings for modes and ring ports (for single rings and multi-ring configurations without shared links)*. The T6 node in *Figure 21-3 Multi-ring configurations with shared links (basic configuration)* corresponds to this setting.

**(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 21-4** Multi-ring configurations with shared links (extended configuration)**(a) Nodes (transit) within shared links for shared link non-monitoring rings**

Points to note

The operating mode for the Switch can be set the operating mode for the Switch to transit mode in a ring. The S7 node in *Figure 21-4 Multi-ring configurations with shared links (extended configuration)* corresponds to this setting. The **shared** parameter is specified for both ring ports, and they are set as the shared port. Ring port [R3] for the S7 node in *Figure 21-4 Multi-ring configurations with shared links (extended configuration)* corresponds to this setting.

Command examples

- ```
(config)# axrp 1
(config-axrp)# mode transit
(config-axrp)# exit
```

Sets the operating mode for ring ID 1 to transit mode.
- ```
(config)# interface fastethernet 0/1
(config-if)# axrp-ring-port 1 shared
```

```
(config-if)# exit
(config)# interface fastethernet 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.

## 21.1.9 Setting various parameters

### (1) Disabling the Ring Protocol functionality

#### Points to note

You can disable the Ring Protocol functionality by specifying a command. 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) Reception hold time for flush control frames

#### Points to note

Sets the reception hold time for flush control frames for transit nodes. Set the reception hold time for flush control frames for transit nodes (value set using the `forwarding-shift-time` command) to 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 reception hold time for flush control frames to 100 seconds.

## 21.1.10 Setting the multi-fault monitoring functionality

### (1) Setting multi-fault monitoring VLANs

#### Points to note

A VLAN can be set 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.

## 21 Settings and Operation for the Ring Protocol

### Command examples

1. `(config)# axrp 1`  
Switches to axrp configuration mode for ring ID 1.
2. `(config-axrp)# multi-fault-detection vlan 20`  
`(config-axrp)# exit`  
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

Sets the monitoring mode for the Switch to `transport-only`. (The Switch supports `transport-only` only.)

### Command examples

1. `(config)# axrp 1`  
Switches to axrp configuration mode for ring ID 1.
2. `(config-axrp)# multi-fault-detection mode transport-only`  
`(config-axrp)# exit`  
Sets the monitoring mode for multi-fault monitoring to `transport-only`.

## 21.2 Operation

### 21.2.1 List of operation commands

The following table describes the operation commands for the Ring Protocol.

**Table 21-2** List of operation commands

| Command name | Description                                                |
|--------------|------------------------------------------------------------|
| show axrp    | Displays Ring Protocol information.                        |
| show port    | Displays the usage status of the Ring Protocol for a port. |
| show vlan    | Displays the usage status of the Ring Protocol for a VLAN. |

### 21.2.2 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 `Oper State` item. If `enable` is displayed for `Oper State`, the Ring Protocol functionality is running. The operation status of all items is indicated by the contents displayed. When `-` is displayed for `Oper State`, the item has not had its status obtained by the required configuration command. When `Not Operating` is displayed for `Oper State`, the Ring Protocol functionality cannot run because a conflict exists in the configuration. When `-` or `Not Operating` is displayed for `Oper State`, check the configuration.

The following figures show examples of the `show axrp` and `show axrp detail` configuration commands.

**Figure 21-5** Execution results of show axrp

```
> show axrp

Date 2011/09/01 15:34:11 UTC
Total Ring Counts:1

Ring ID:2
Name:0-Ring
Oper State:enable Mode:Transit

VLAN Group ID Ring Port Role/State Ring Port Role/State
1 0/25 -/forwarding 0/26 -/forwarding
2 - -/- - -/-

>
```

The `show axrp detail` operation command can be used to check the details about the ring status.

**Figure 21-6** Execution results of show axrp detail

```
> show axrp detail

Date 2011/09/01 15:35:15 UTC
Total Ring Counts:1
```

## 21 Settings and Operation for the Ring Protocol

```
Ring ID:2
Name:0-Ring
Oper State:enable Mode:Transit
Control VLAN ID:20
Forwarding Shift Time (sec):15
Last Forwarding:flush request receive

VLAN Group ID:1
VLAN ID:200
Ring Port:0/25 Role:- State:forwarding
Ring Port:0/26 Role:- State:forwarding

VLAN Group ID:2
VLAN ID:-
Ring Port:- Role:- State:-
Ring Port:- Role:- State:-

Multi Fault Detection State:-
Mode:transport
Control VLAN ID:1000
>
```

---

## 22. Using the Ring Protocol with Spanning Tree Protocols/GSRP

This chapter explains how to use the Ring Protocol on the same switch as a Spanning Tree Protocol or GSRP.

---

22.1 Using the Ring Protocol with Spanning Tree Protocols

---

22.2 Using the Ring Protocol with GSRP

---

## 22.1 Using the Ring Protocol with Spanning Tree Protocols

The Switch cannot use the Ring Protocol together with a Spanning Tree Protocol. However, if a switch that can use the Ring Protocol together with a Spanning Tree Protocol (such as AX2400S, AX3600S, and AX6700S series switches) exists in the ring, the Switch can be in the ring configuration as a transit node.

### 22.1.1 Overview

The figures below show examples of the Switches included as transit nodes in the single ring configuration and multi-ring configuration in which a switch that can use the Ring Protocol together with a Spanning Tree Protocol exists. Switches A/F/G, B/E/H, and C/D/I each comprise a Spanning Tree topology. The Ring Protocol and Spanning Tree Protocol are used at the same time for switches A to D. Switches ① and ② use the Ring Protocol (as transit nodes) only.

**Figure 22-1** Example of using the Ring Protocol together with a Spanning Tree Protocol and the positions of the Switches (single ring configuration)

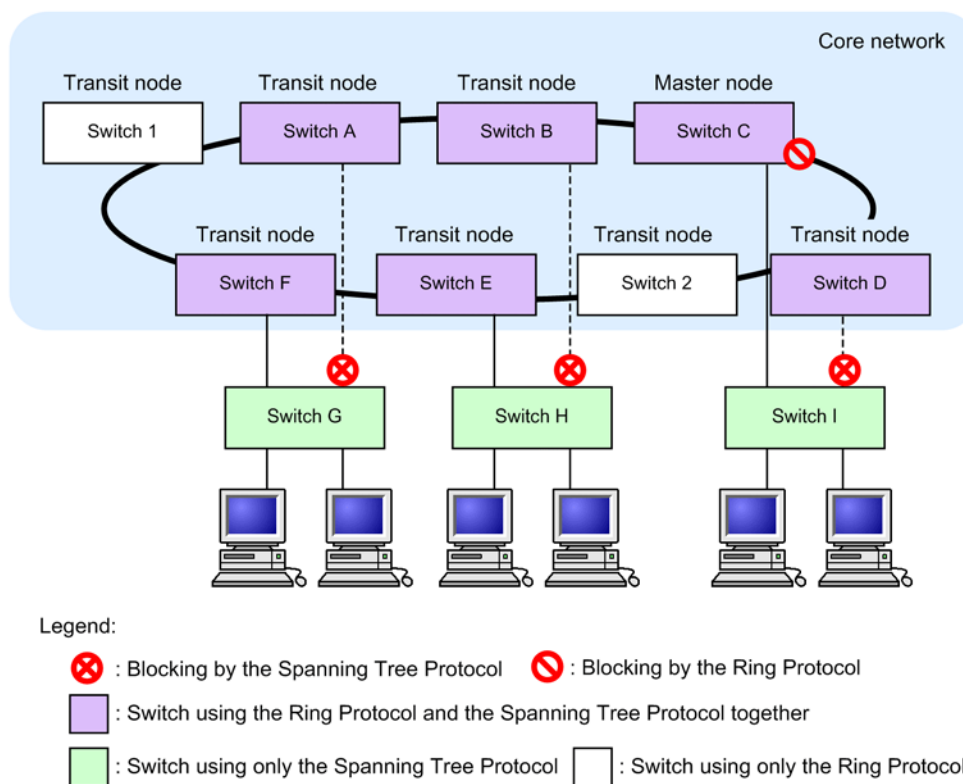
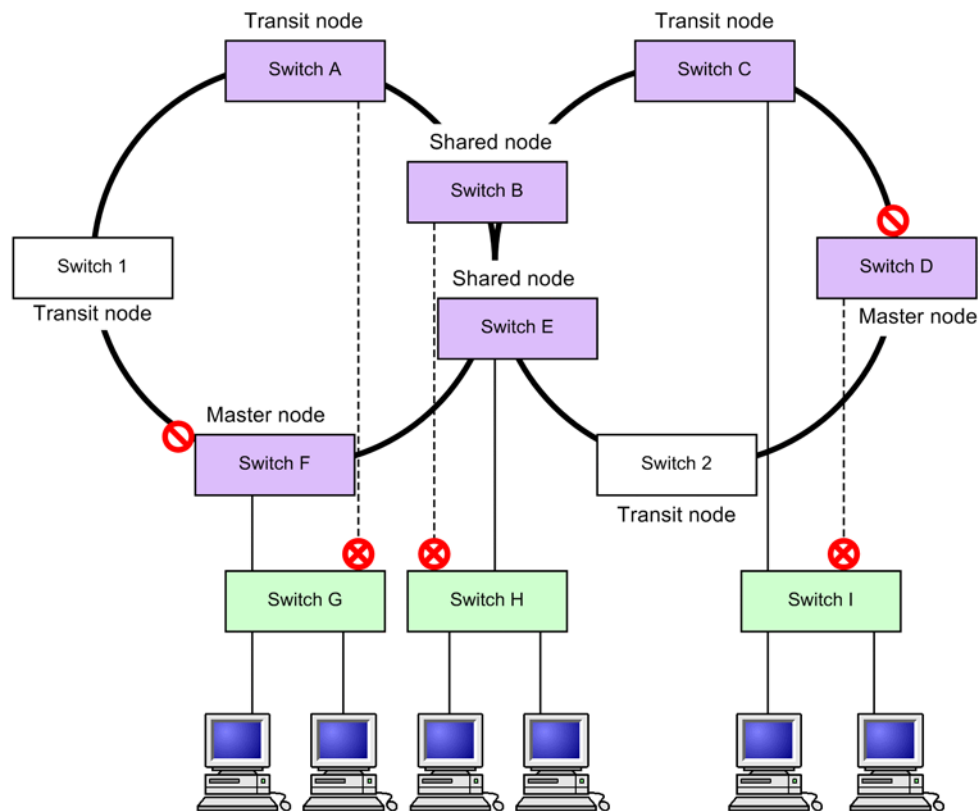




**Figure 22-2** Example of using the Ring Protocol together with a Spanning Tree Protocol and the positions of the Switches (multi-ring configuration)

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

The Switches only perform forwarding of virtual link control frames (described below) and clearing of MAC address table entries. For details about operations when using the Ring Protocol together with a Spanning Tree Protocol 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 a Spanning Tree Protocol

Any two switches that use the Ring Protocol together with a Spanning Tree Protocol are connected by virtual links. Virtual links are built between two switches on a ring network. A virtual VLAN set on the ring network is used to send and receive control frames between virtual links (virtual link control frames). A VLAN belonging to the data transfer VLAN group on the ring ports is used as the virtual VLAN.

The Switch in the ring network only performs forwarding of virtual link control frames.

### (2) 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 on the virtual link VLAN so that MAC address table entries are cleared for the entire single ring or multi-ring network. Each switch receiving this in the ring network clears MAC address table entries for ring ports for which the Ring Protocol is running.

The Switch in the ring network also clears MAC address table entries when a flush control frame is received.

## 22.2 Using the Ring Protocol with GSRP

The Switch cannot use the Ring Protocol together with GSRP. However, if a switch that can use the Ring Protocol together with GSRP (such as AX2400S, AX3600S, and AX6700S series switches) exists in the ring, the Switch can be in the ring configuration as a transit node.

### 22.2.1 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 switching on a GSRP network clear the MAC address table for GSRP switches and aware/unaware switches. At the same time, a flush control frame for the ring network is sent to clear the MAC address tables of switches configuring the ring network.

The following figure shows an example of the Ring Protocol and GSRP being used together.

**Figure 22-3** Example of the Ring Protocol and GSRP being used together and the positions of the Switches (when direct links are used on a ring network)

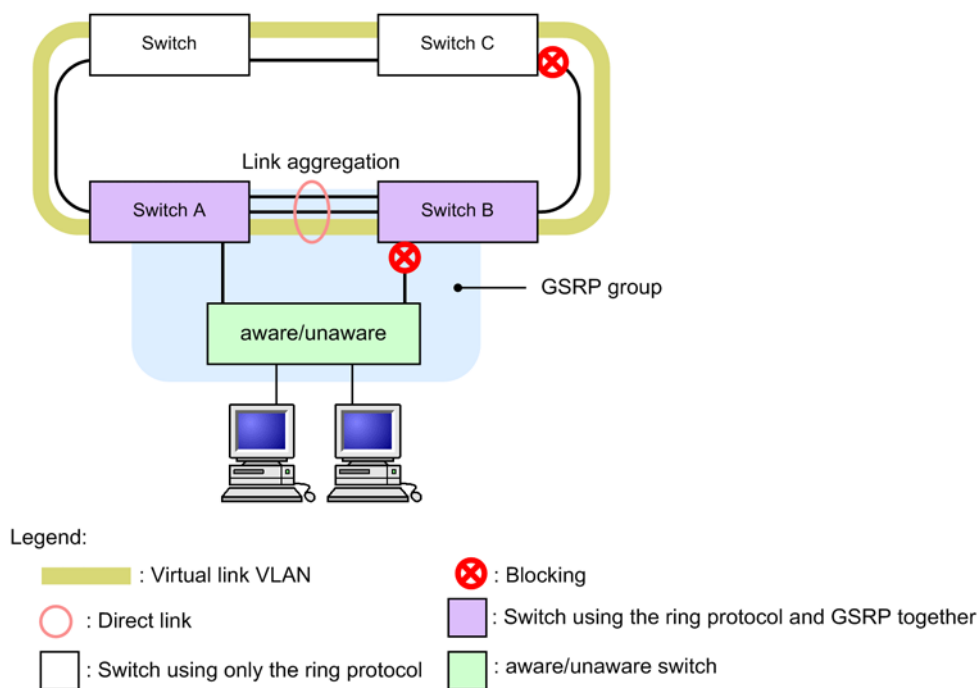
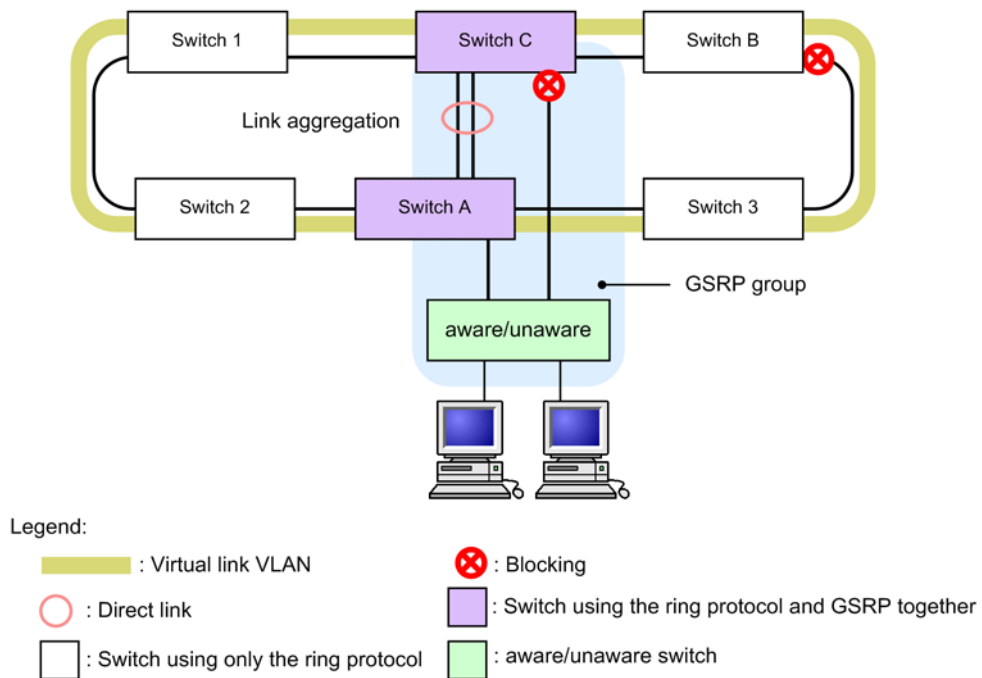


**Figure 22-4** Example of the Ring Protocol and GSRP being used together and the positions of the Switches (when direct links are not used on a ring network)



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

Any two switches that use the Ring Protocol together with GSRP are connected by virtual links. This is the same as for the switches that use the Ring Protocol together with a Spanning Tree Protocol described above. Virtual links are built between two switches on a ring network. The virtual VLAN 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 Switch in the ring network only performs forwarding of virtual link control frames.

### (2) Clearing MAC address tables during GSRP network switching

When GSRP network path switching occurs, the GSRP master uses the virtual link VLAN to send a flush control frame to switches in the ring network so that MAC address table entries are cleared. Each switch receiving this in the ring network clears its MAC address table entries.

The Switch receiving a flush control frame in the ring network also clears its MAC address table entries.



---

## 23. DHCP Snooping

This chapter describes the DHCP snooping functionality and how to use it.

---

|      |                                                |
|------|------------------------------------------------|
| 23.1 | Description of the DHCP snooping functionality |
|------|------------------------------------------------|

---

|      |                                |
|------|--------------------------------|
| 23.2 | Configuration of DHCP snooping |
|------|--------------------------------|

---

|      |                         |
|------|-------------------------|
| 23.3 | DHCP snooping operation |
|------|-------------------------|

---

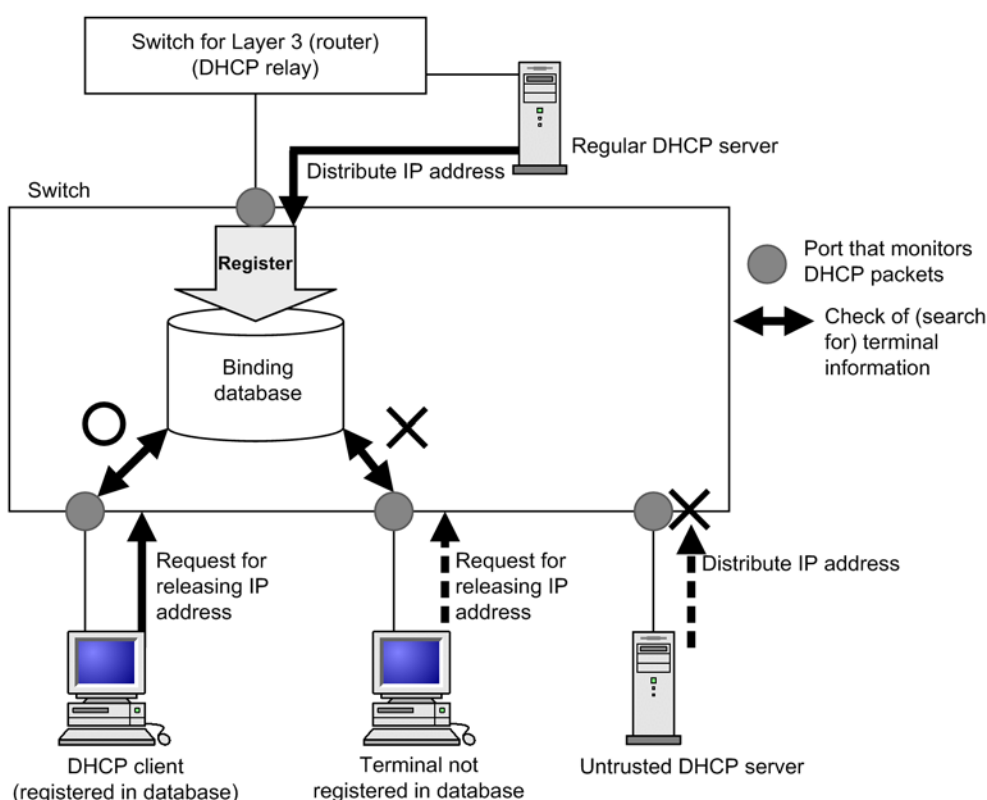
## 23.1 Description of the DHCP snooping functionality

DHCP snooping monitors the DHCP packets that pass through the Switch to restrict access from untrusted terminals.

- With DHCP snooping, clients whose IP addresses have been assigned by DHCP servers and terminals with fixed IP addresses are registered for management in a binding database.
- DHCP snooping suppresses IP address release requests from untrusted terminals (terminals that have not been registered in the binding database; hereafter called *terminals not registered in the DB*).
- DHCP snooping prevents untrusted DHCP servers from handing out IP addresses.

To enable DHCP snooping, place the Switch between the DHCP server and DHCP clients as shown in the following figure.

**Figure 23-1** Overview of DHCP snooping

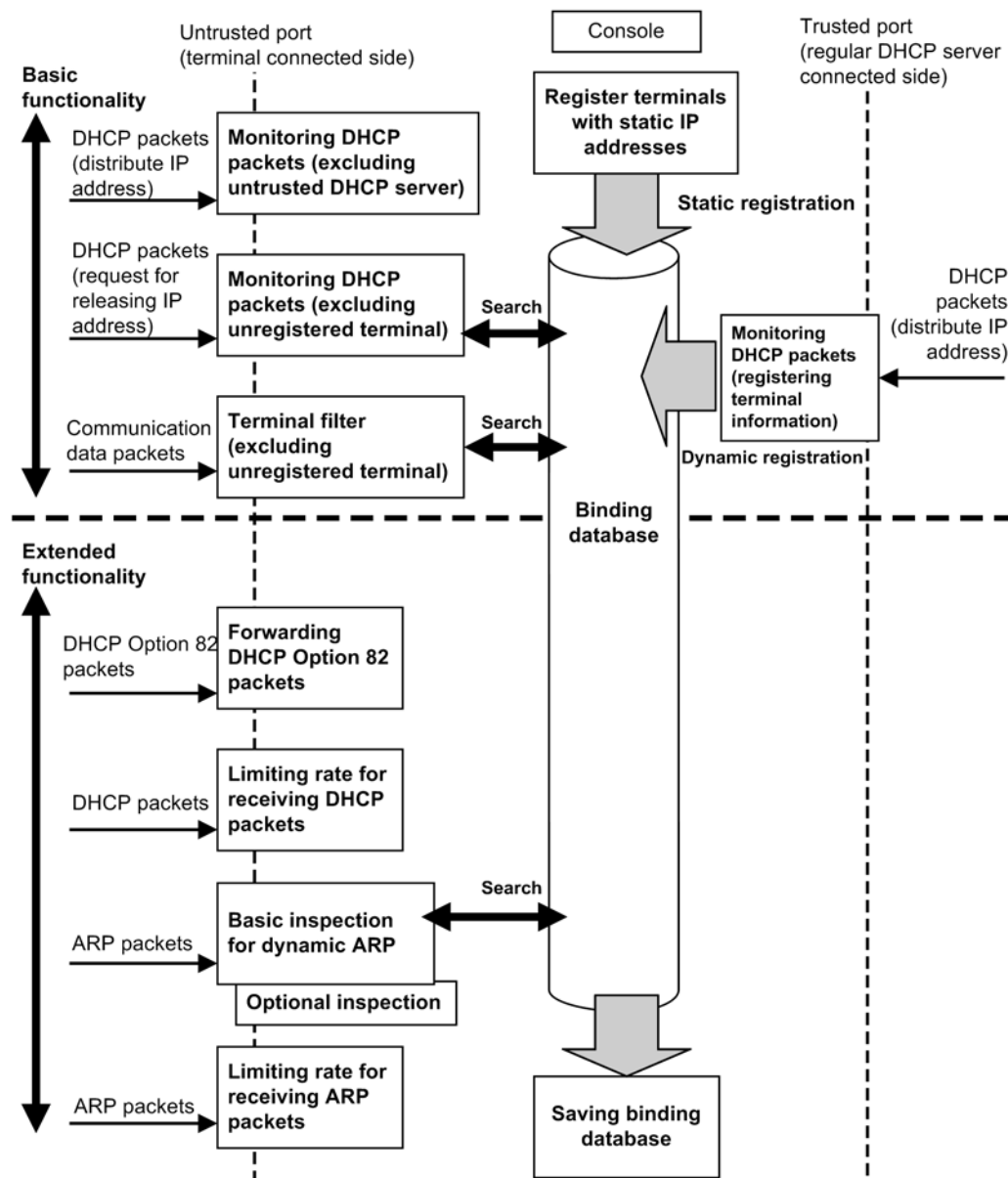


DHCP snooping also supports terminal filtering, which discards all the communication data packets sent from terminals not registered in the DB.

DHCP snooping supports the following extended functionality, in addition to the above functionality:

- Forwarding DHCP packets with Option 82
- Limiting the rate of DHCP packet reception
- Dynamic ARP inspection
- Saving a binding database

The following figure shows the relationship between the functionality and behavior of the binding database.

**Figure 23-2** Relationship between the functionality and behavior of the binding database

The following table cross-references functionality details and explains the settings.

**Table 23-1** Supported functionality of DHCP snooping

| Functionality | Item                                                           | Functionality reference | Settings reference |
|---------------|----------------------------------------------------------------|-------------------------|--------------------|
| Basic         | Monitoring DHCP packets                                        | See 23.1.1.             | See 23.2.3.        |
|               | Terminal filtering                                             | See 23.1.2.             | See 23.2.3.        |
|               | Permitting communication by a terminal with a fixed-IP address | See 23.1.2.             | See 23.2.3.        |
| Ext           | Forwarding DHCP packets with Option 82                         | See 23.1.3.             | See 23.2.4.        |

| Functionality | Item                                       | Functionality reference | Settings reference |
|---------------|--------------------------------------------|-------------------------|--------------------|
| ended         |                                            |                         |                    |
|               | Limiting the rate of DHCP packet reception | See 23.1.4.             | See 23.2.5.        |
|               | Dynamic ARP inspection                     |                         |                    |
|               | Basic inspection                           | See 23.1.5.             | See 23.2.6.        |
|               | Optional inspection                        | See 23.1.5.             | See 23.2.6.        |
|               | Limiting the rate of ARP packet reception  | See 23.1.5.             | See 23.2.6.        |
|               | Saving a binding database                  |                         |                    |
|               | Saving when the wait-to-write time expires | See 23.1.6.             | See 23.2.7.        |
|               | Saving by a specific operation             | See 23.1.6.             | --                 |

### 23.1.1 Monitoring DHCP packets

#### (1) Port types and DHCP packet monitoring operations

DHCP snooping classifies ports into the following types to monitor DHCP packets:

1. Trusted ports

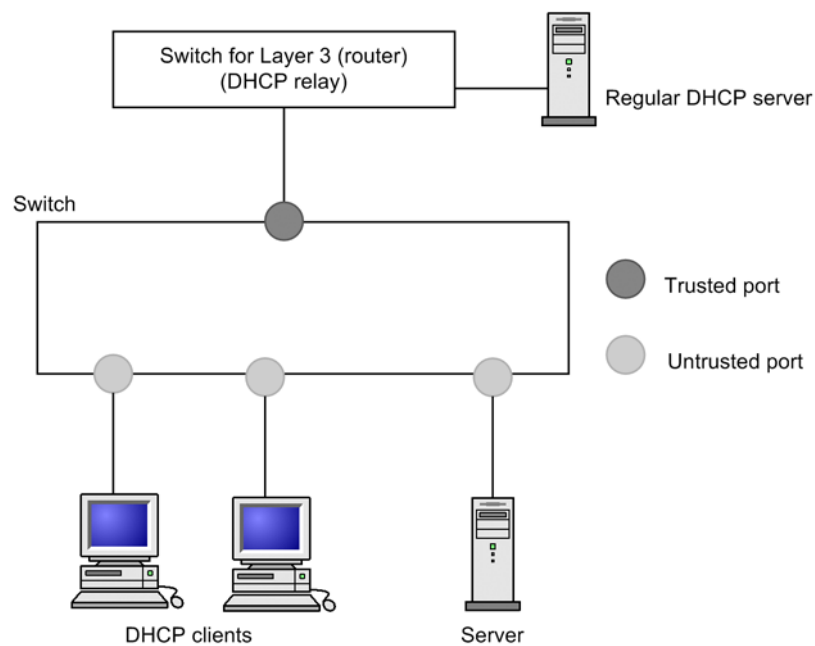
These are ports to which the authorized DHCP servers are connected.

The Switch monitors DHCP server packets received on trusted ports, and dynamically registers the terminal information in the binding database.

2. Untrusted ports

These are ports to which unspecified terminals, such as DHCP clients and department servers, are connected. DHCP servers are not connected to these types of ports.

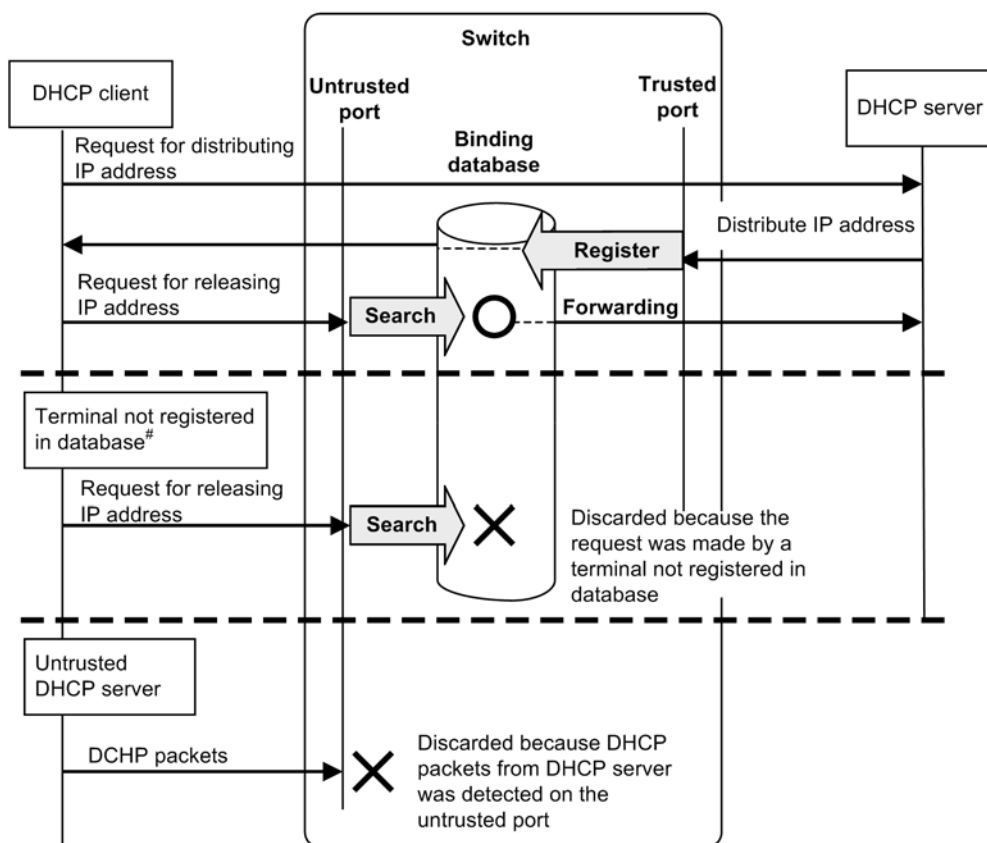


**Figure 23-3** DHCP snooping port types

The Switch monitors DHCP packets for terminals connected to untrusted ports, and excludes the following types of access:

- Suppressing IP address release requests from terminals not registered in the DB  
The Switch discards IP address release requests received on untrusted ports from terminals not registered in the DB. This allows the suppressing of IP address release requests from terminals for which IP addresses have not been assigned by authorized DHCP servers.
- Discarding DHCP packets sent from DHCP servers  
The Switch monitors DHCP packets received on untrusted ports, and discards the packets sent from DHCP servers. This prevents untrusted DHCP servers from handing out IP addresses.

The following figure provides an overview of DHCP packet monitoring.

**Figure 23-4** Overview of DHCP packet monitoring

#: A terminal not registered in database indicates a terminal that is not registered in the binding database.

When you use the `ip dhcp snooping` configuration command to enable DHCP snooping, all the ports are untrusted by default. Set the port to which an authorized DHCP server is connected as a trusted port. To do so, use the `ip dhcp snooping trust` configuration command.

## (2) Registration in the binding database

There are two types of registration in the binding database: dynamic registration and static registration.

- **Dynamic registration:** The Switch registers terminal information when an IP address is handed out from a DHCP server.
- **Static registration:** The `ip source binding` configuration command is used to register terminal information.

The following items are registered in the binding database.

**Table 23-2** Items registered in the binding database

| Item              |             | Dynamic registration                                                                                                              | Static registration |
|-------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Number of entries | 246 entries | Total number of dynamic entries and static entries that can be registered.<br>(A maximum of 64 static entries can be registered.) |                     |

| Item                         |                       | Dynamic registration                                                                                                                                                                                                       | Static registration                                |
|------------------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| Information to be registered | Terminal MAC address. | MAC address of a DHCP client                                                                                                                                                                                               | MAC addresses of terminals with fixed-IP addresses |
|                              | Terminal IP address   | IP address handed out by the DHCP server                                                                                                                                                                                   | IP addresses of terminals with fixed-IP addresses  |
|                              |                       | IP addresses in the following ranges are available for dynamic registration or static registration: <ul style="list-style-type: none"> <li>● 1.0.0.0 to 126.255.255.255</li> <li>● 128.0.0.0 to 223.255.255.255</li> </ul> |                                                    |
|                              | Terminal VLAN ID      | ID of the VLAN containing the port or channel group to which the terminal is connected                                                                                                                                     |                                                    |
|                              | Terminal port number  | Number of the port or channel group to which the terminal is connected                                                                                                                                                     |                                                    |
| Aging timer                  | Lease time            | Period of time between when an entry is dynamically registered and when the entry is aged. The lease time of the IP address handed out by the DHCP server is used for this item.                                           | Aging is not applicable.                           |

## 23.1.2 Terminal filtering

### (1) Overview of terminal filtering

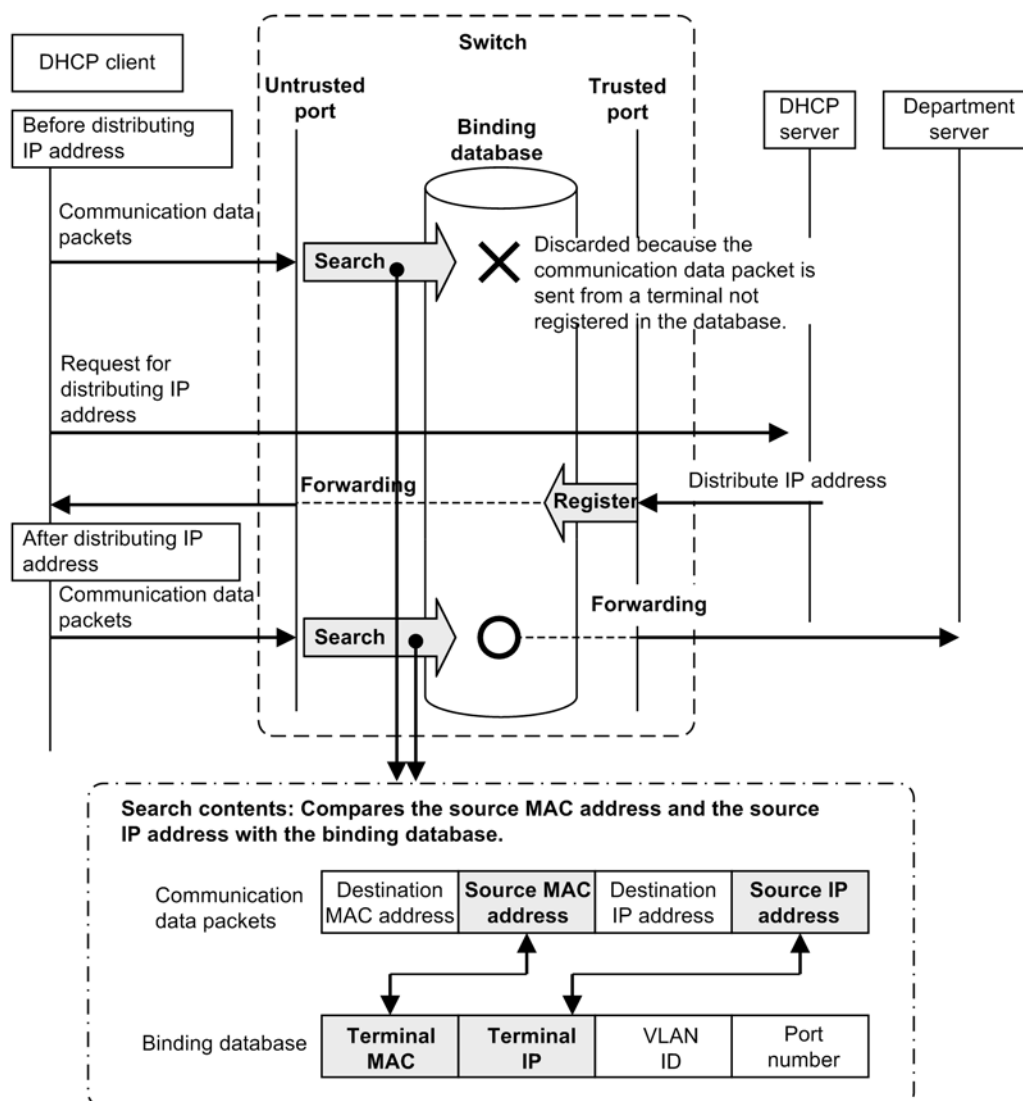
Terminal filtering discards all the communication data packets sent from terminals not registered in the DB. Communication data packets sent from the terminals connected to untrusted ports are subject to terminal filtering.

Enable terminal filtering, and then set filter conditions. Set one of the following three filter conditions according to the security policy:

- Terminal filtering for source IP addresses only
- Terminal filtering for source IP addresses and source MAC addresses
- Terminal filtering for source MAC addresses only

You can set terminal filtering for each port by using the `ip verify source` configuration command.

**Figure 23-5** Overview of terminal filtering (example of terminal filtering for source IP addresses and source MAC addresses)



This discards packets with source IP addresses and source MAC addresses that have not been registered in the binding database.

## (2) Permitting communication by a terminal with a fixed-IP address

You can permit communication by a terminal with a fixed-IP address (such as a department server) connected to an untrusted port, by statically registering terminal information in the binding database.

To permit communication by a terminal with a fixed-IP address, use the [ip source binding](#) configuration command and register the following information:

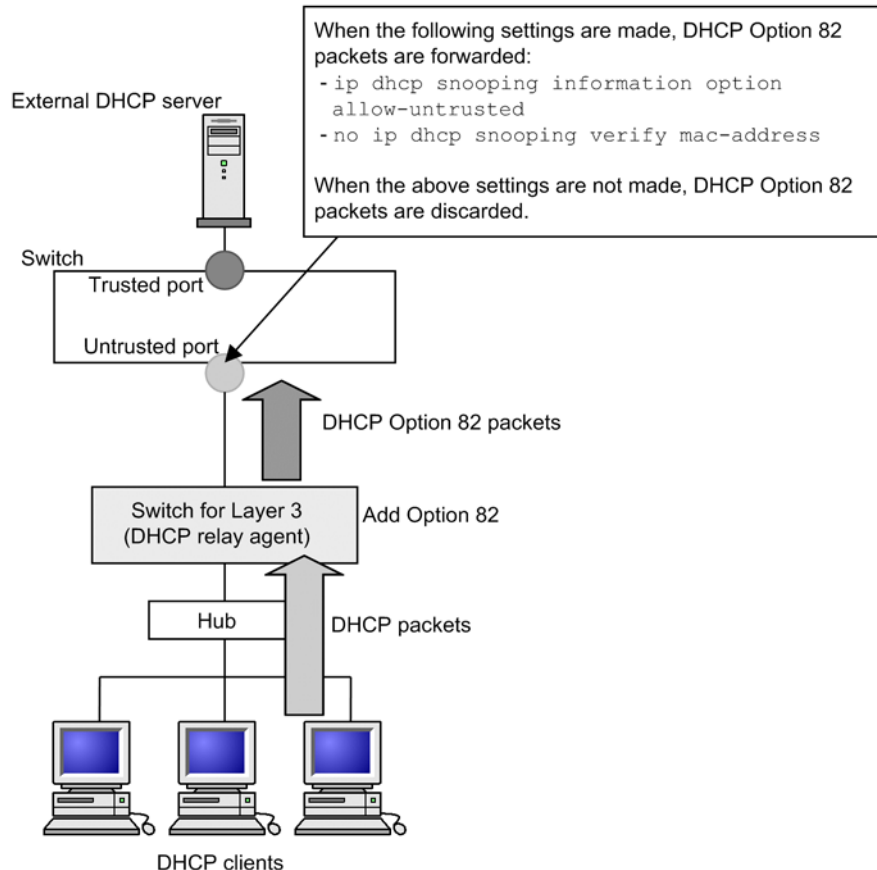
- Terminal IP address
- Terminal MAC address.
- Number of the port or channel group to which the terminal is connected
- ID of the VLAN containing the port or channel group to which the terminal is connected

For details about the number of entries that can be set by this command, see *Table 23-2 Items registered in the binding database*.

### 23.1.3 Forwarding DHCP packets with Option 82

In a configuration with a DHCP relay agent, such as a Layer 3 switch, placed between the Switch and a DHCP client, the DHCP relay agent might add Option 82 information to DHCP packets sent from the DHCP client.

**Figure 23-6** Example configuration when Option 82 information is added to the packets



Packets with Option 82 contain information used by a DHCP relay agent to transfer extended information about the DHCP client, such as the MAC address of the terminal, connection port number, and host name.

When DHCP snooping is enabled, packets with Option 82 received on untrusted ports are discarded. Therefore, if the Switch is placed between a DHCP server and a DHCP relay agent, and the DHCP relay agent adds Option 82 information to the packets, DHCP snooping on the Switch cannot operate correctly.

In this case, execute the `ip dhcp snooping information option allow-untrusted` configuration command to set the Switch to permit communication using packets with Option 82.

Also, DHCP snooping checks if the source MAC address of a DHCP packet received on an untrusted port matches the client hardware address in the DHCP packet (MAC address matching). If a DHCP relay agent is connected to an untrusted port, the source MAC address of a DHCP packet is rewritten by the DHCP relay agent, and the Switch judges the DHCP packet as illegal and discards it.

Therefore, in addition to the setting of permitting communication using packets with Option 82, you need to execute the `no ip dhcp snooping verify mac-address` configuration command to cancel MAC address matching.

### 23.1.4 Limiting the rate of DHCP packet reception

If DHCP snooping is enabled to monitor the receipt of DHCP packets and the number of

DHCP packets exceeds the specified reception rate, this function discards the excess DHCP packets.

You can set the reception rate by using the `ip dhcp snooping limit rate` configuration command. If the reception rate is not set, it has no limit.

The rate of DHCP packet reception is limited only on untrusted ports, not on trusted ports.

DHCP packets exceeding the rate are dropped, and the incident is logged in the operation log. However, traps are not issued. Use the `show logging` operation command to check the operation log information, and use the `show ip dhcp snooping statistics` operation command to check the number of discarded packets.

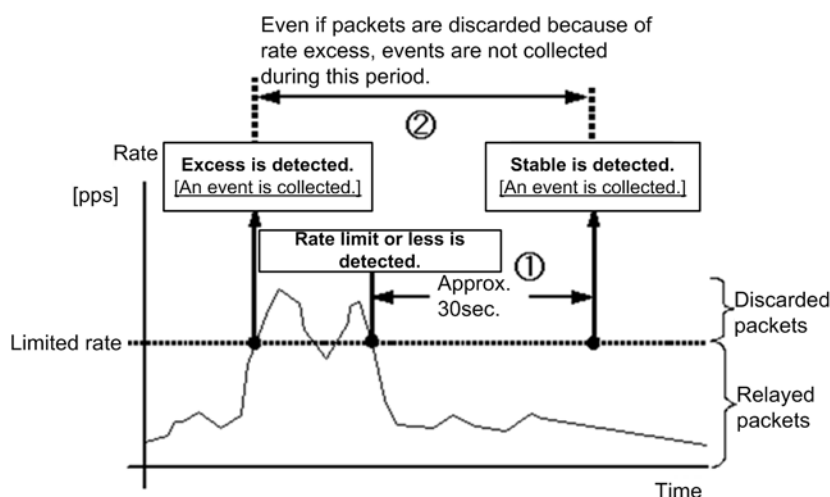
The collection of operation log information is triggered by the following events:

- A Limit Exceeded event is collected when the configured reception rate is exceeded.
- A Stable State event is collected after a Limit Exceeded event is collected and when the reception rate continues below the configured reception rate limit for about 30 seconds ((1) in the figure).

During the period after the Limit Exceeded event is collected until the Stable State event is collected ((2) in the figure), no event is collected even if packets are discarded due to being in excess of the configured rate.

The following figure shows the events logged in the operation log.

**Figure 23-7** Events logged in the operation log related to the rate of DHCP packet reception



### 23.1.5 Dynamic ARP inspection functionality

In this functionality, if DHCP snooping is enabled, the Switch checks whether the sender IP address and sender MAC address in an ARP packet received on an untrusted port on the Switch are those of a legitimate terminal registered in the binding database. This functionality prevents a spoofed ARP packet sent from a terminal not registered in the DB, from taking over communication of a legitimate terminal.

#### (1) Targets of dynamic ARP inspection

ARP packets that meet all the following conditions are subject to dynamic ARP inspection:

- ARP packets received on ports belonging to the VLANs that are subject to ARP inspection  
(To set VLANs that are subject to ARP inspection, use the `ip arp inspection vlan` configuration command.)
- ARP packets received on untrusted ports (ports which have not been set as trusted)

by the `ip arp inspection trust` configuration command)

## (2) Basic inspection of dynamic ARP inspection

In the basic inspection, the Switch checks whether the information in the ARP packets received on untrusted ports matches the entries in the binding database.

The following figure shows the basic inspection of dynamic ARP inspection.

**Figure 23-8** Overview of the basic inspection of dynamic ARP inspection

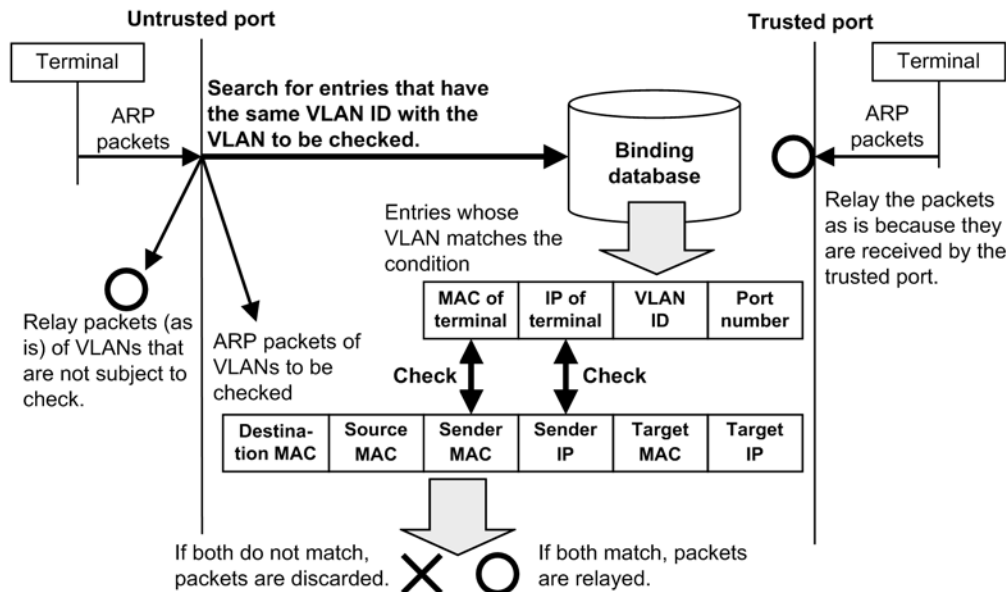


**Table 23-3** Fields of an ARP packet subject to basic inspection

| Field of an ARP packet |             |     | Request | Reply | Remarks                                            |
|------------------------|-------------|-----|---------|-------|----------------------------------------------------|
| Ethernet header        | Destination | MAC | --      | --    | --                                                 |
|                        | Source      | MAC | --      | --    | --                                                 |
| ARP header             | Sender      | MAC | Y       | Y     | Compared with the entries in the binding database. |
|                        |             | IP  | Y       | Y     | Compared with the entries in the binding database. |
|                        | Target      | MAC | --      | --    | --                                                 |
|                        |             | IP  | --      | --    | --                                                 |

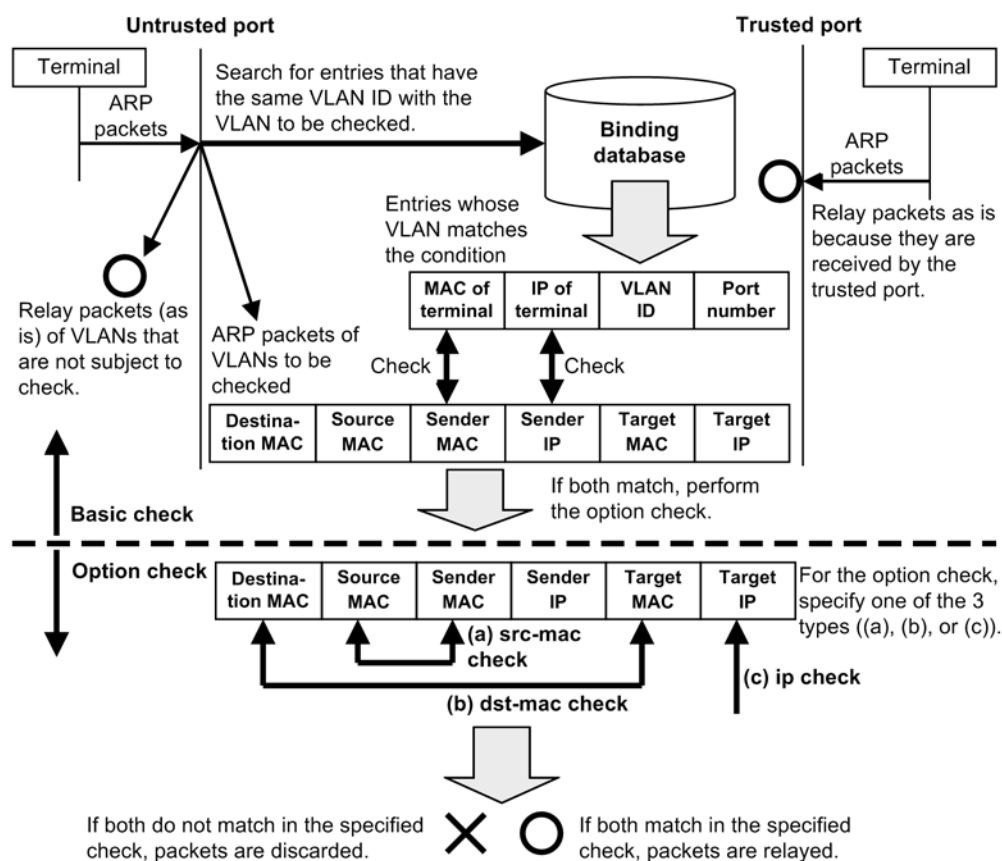
Legend:

Y: Subject to inspection

--: Not subject to inspection

## (3) Optional inspection of dynamic ARP inspection

The dynamic ARP inspection functionality checks the matching with the binding database. As an optional functionality, it also supports inspection of the matching of data in ARP packets.

**Figure 23-9** Relationship between a basic inspection and an optional inspection of dynamic ARP inspection**(a) Source MAC address specification (src-mac check)**

This inspection item checks if the source MAC address and the sender MAC address of a received ARP packet are the same.

This inspection is performed on both ARP requests and ARP replies.

**(b) Destination MAC address specification (dst-mac check)**

This inspection item checks if the destination MAC address and the target MAC address of a received ARP packet are the same.

This inspection is performed on an ARP reply only.

**(c) IP address specification (ip check)**

This inspection item checks if the target IP address of the received ARP packet is within the following ranges.

- 1.0.0.0 to 126.255.255.255
- 128.0.0.0 to 223.255.255.255

This inspection is performed on an ARP reply only.

**Table 23-4** Fields of an ARP packet subject to the optional inspection

| Fields of an ARP packet | src-mac check |       | dst-mac check |       | ip check    |       |
|-------------------------|---------------|-------|---------------|-------|-------------|-------|
|                         | Reque<br>st   | Reply | Reque<br>st   | Reply | Reque<br>st | Reply |



| Fields of an ARP packet |             |     | src-mac check |       | dst-mac check |       | ip check |       |
|-------------------------|-------------|-----|---------------|-------|---------------|-------|----------|-------|
|                         |             |     | Request       | Reply | Request       | Reply | Request  | Reply |
| Ethernet header         | Destination | MAC | --            | --    | --            | Y     | --       | --    |
|                         | Source      | MAC | Y             | Y     | --            | --    | --       | --    |
| ARP header              | Sender      | MAC | Y             | Y     | --            | --    | --       | --    |
|                         |             | IP  | --            | --    | --            | --    | --       | --    |
|                         | Target      | MAC | --            | --    | --            | Y     | --       | --    |
|                         |             | IP  | --            | --    | --            | --    | --       | Y     |

Legend:

Y: Subject to inspection

--: Not subject to inspection

#### (4) Limiting the rate of ARP packet reception

If the dynamic ARP inspection is enabled, ARP packets that are received on ports belonging to VLANs subject to dynamic ARP inspections and that exceed the configured reception rate are discarded.

To set the reception rate, use the `ip arp inspection limit rate` configuration command. If this reception rate has not been set, it has no limit.

The ARP packets exceeding the rate are dropped, and the incident is logged in the operation log. However, traps are not issued. Use the `show logging` operation command to check the operation log information, and use the `show ip arp inspection statistics` operation command to check the number of discarded packets.

The events logged in the operation log when the ARP packet reception rate exceeds the limit are the same as those logged when a limit is applied to the DHCP packet reception rate. For details, see *Figure 23-7 Events logged in the operation log related to the rate of DHCP packet reception* in 23.1.3 Forwarding DHCP packets with Option 82.

### 23.1.6 Saving a binding database

The binding database can be configured so that it is saved and restored when the Switch restarts.

#### (1) Operating conditions for saving a binding database

You can set the operating conditions for saving the binding database by setting the following configuration commands:

- `ip dhcp snooping`: Sets DHCP snooping enabled.
- `ip dhcp snooping vlan`: Sets the VLANs for which DHCP snooping is performed.
- `ip dhcp snooping database url`: Sets the location the binding database is saved to.

The Switch saves the binding database by specific operations or when the wait-to-write time expires.

## (2) Saving when the wait-to-write time expires

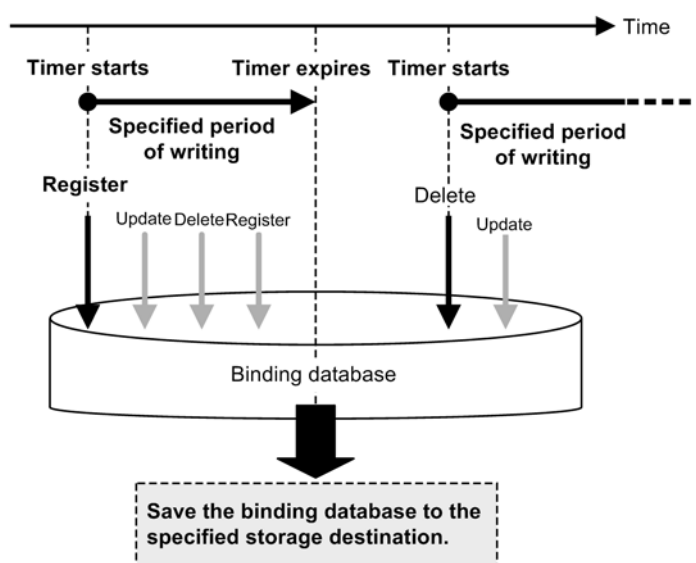
The timer for the wait-to-write time is triggered by one of the following save events. The binding database is saved to the specified location when the timer expires.

- A dynamic binding database is registered, updated, or deleted.
- When the `ip dhcp snooping database url` configuration command is specified (includes a change of save location)
- When the `clear ip dhcp snooping binding` operation command is executed

Use the `ip dhcp snooping database write-delay` configuration command to set the wait-to-write time.

Once the timer for the wait-to-write time is triggered by one of the above save events, it does not stop until it expires. Even if the binding database is registered, updated, or deleted while the timer is operating, the timer does not restart.

**Figure 23-10** Overview of the operation related to save events and the wait-to-write time (example when triggered by binding database registration)



## (3) Saving by a certain operation

If either of the operations below, which prompt the restart of the Switch, is performed, the binding database at that moment is saved to the save location specified in the configuration.

If the save location is not specified in the configuration, the binding database is not saved even if the following operations are performed.

**Table 23-5** Saving by specific operation

| Operation | Save location                                | Activation triggers                                       |
|-----------|----------------------------------------------|-----------------------------------------------------------|
| reload    | Save location specified in the configuration | An operation command is input from an operation terminal. |
| ppupdate  |                                              | An operation command is input from an operation terminal. |
| backup    |                                              | An operation command is input from an operation           |

| Operation   | Save location | Activation triggers   |
|-------------|---------------|-----------------------|
|             |               | terminal.             |
| copy-config |               | Executed from an OAN. |

#### (4) Save location for the binding database

The binding database can be saved to internal flash memory or to a memory card. The save location must be specified in the configuration. In both cases, all entries are saved when the database is saved, and they are overwritten each time the database is subsequently saved.

To set the save location, use the `ip dhcp snooping database url` configuration command.

#### (5) Restoring a saved binding database

The saved binding database is restored when the Switch is started. Check the following before restarting the Switch:

- The save location has been set by using the `ip dhcp snooping database url` configuration command.
- If the save location is an external memory card, the applicable card has been inserted.

### 23.1.7 Notes on using DHCP snooping

#### (1) Use with other functionality

##### (a) When used with the Layer 2 switch functionality

For details, see *15.3 Compatibility between Layer 2 switch functionality and other functionality*.

##### (b) When used with the filtering functionality

For details, see *1.1.7 Notes on using the filter* in the *Configuration Guide Vol. 2*.

##### (c) When used with the Layer 2 authentication functionality

DHCP snooping, terminal filtering, and authentication methods (IEEE802.1X authentication, Web authentication, or MAC-based authentication) can be used on the same port.

In this case, the authentication method takes precedence over terminal filtering. Even if a terminal is permitted communication by terminal filtering, it cannot communicate with the Switch if it is not permitted communication by the authentication method.

Also, authentication methods can coexist, without depending on whether the port is a trusted port or an untrusted port.

When DHCP snooping and a Layer 2 authentication method are used together, the maximum number of terminals that can communicate is the number of the DHCP snooping controlled terminals (a maximum of 246 terminals).

##### (d) When used with CFM

For details, see *20.1.9 Notes on using the CFM functionality* in the *Configuration Guide Vol. 2*.

##### (e) When used with the power saving functionality

For details, see *11.1.7 Notes when the power saving functionality is used*.

**(2) Using the dynamic ARP inspection functionality**

To use the dynamic ARP inspection, you need to set the following DHCP snooping configurations to generate the binding database.

- Configuration command `ip dhcp snooping`: Enables DHCP snooping.
- Configuration command `ip dhcp snooping vlan`: Sets the VLANs for which DHCP snooping is performed.

Dynamic ARP inspection also checks the entries that are statically registered in a binding database by using the `ip source binding` configuration command.

**(3) Notes on saving and restoring a binding database**

- If the save location has not been set with the `ip dhcp snooping database url` configuration command (initial status), the binding database will not be saved. Therefore, restarting the Switch will erase the registered binding database, disabling communication from DHCP clients. In this case, clear and update the IP addresses on the DHCP client. In Windows, for example, execute `ipconfig /release` and then `ipconfig /renew` from the command prompt.

This re-registers terminal information in the binding database and enables communication by DHCP clients.

- Entries that have exceeded the lease time of the DHCP server will not be restored. After the binding database is saved, if the clock setting is changed before the Switch is turned off, the restoration processing for the binding database might be performed incorrectly after the Switch is turned on.
- Restoration of the entries that were statically registered by the `ip source binding` configuration command is performed according to the startup configuration file at startup.
- If you have saved the binding database on a memory card, do not remove the memory card until a prompt appears on the screen after the switch restarts.
- Before executing the `backup` operation command to save the binding database and executing the `restore` operation command to restore the database, check that the `ip dhcp snooping database url` configuration command has not been used to set a save location on the device to which the database is being restored. If you execute the `restore` operation command when the binding database location setting remains configured, the restoration processing of the binding database might be performed incorrectly.

## 23.2 Configuration of DHCP snooping

### 23.2.1 List of configuration commands

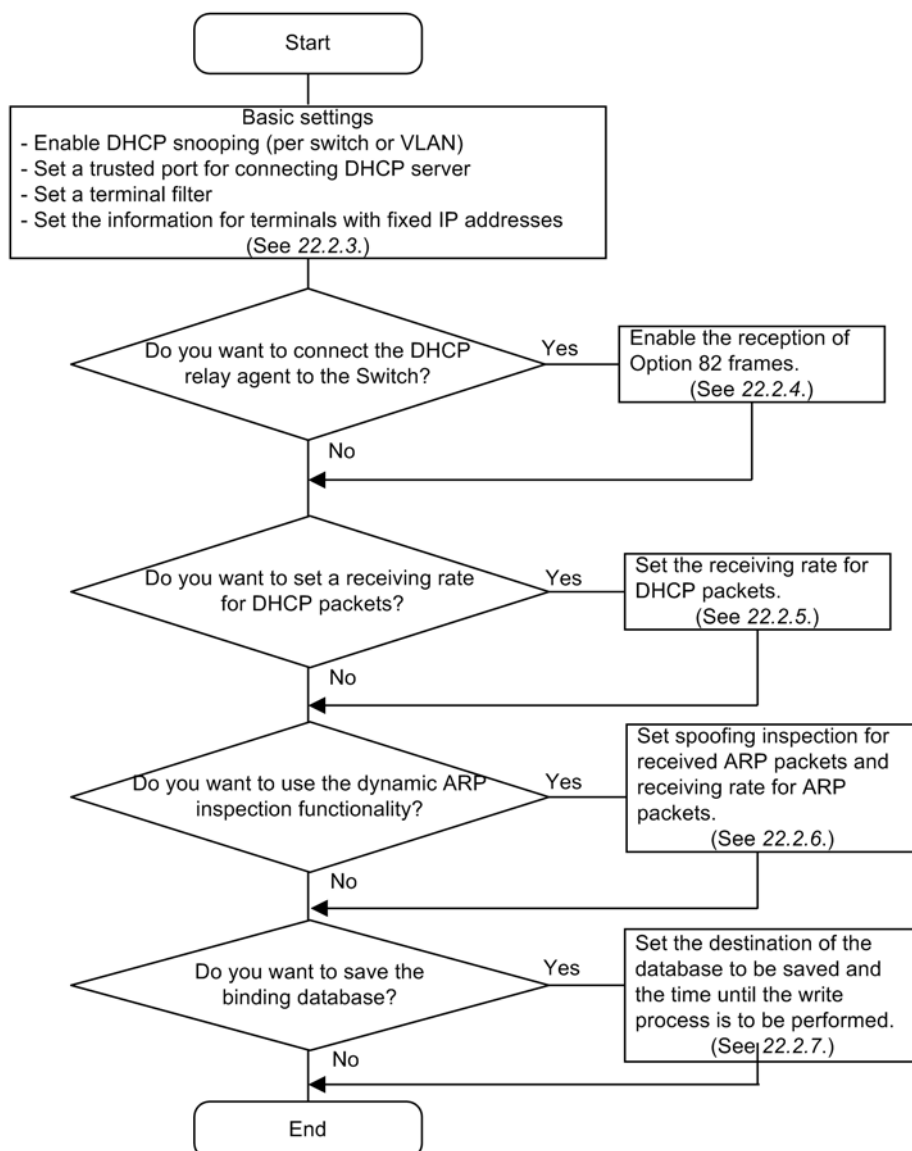
The following table describes the commands used to configure DHCP snooping.

**Table 23-6** List of configuration commands

| Command name                                        | Description                                                                                                                                   |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| ip arp inspection limit rate                        | Sets the ARP packet reception rate (the number of ARP packets that can be received per second) on the applicable port.                        |
| ip arp inspection trust                             | Sets ports for which dynamic ARP inspection is not performed.                                                                                 |
| ip arp inspection validate                          | Sets inspection items to be added to improve the accuracy of dynamic ARP inspection when the dynamic ARP inspection functionality is enabled. |
| ip arp inspection vlan                              | Sets the VLANs used for dynamic ARP inspection.                                                                                               |
| ip dhcp snooping                                    | Sets whether to enable or disable DHCP snooping.                                                                                              |
| ip dhcp snooping database url                       | Specifies where a binding database is to be saved.                                                                                            |
| ip dhcp snooping database write-delay               | Sets the wait-to-write time used when a binding database is saved.                                                                            |
| ip dhcp snooping information option allow-untrusted | Sets whether DHCP packets with Option 82 can be received on untrusted ports.                                                                  |
| ip dhcp snooping limit rate                         | Sets the DHCP packet reception rate (the number of DHCP packets that can be received per second) on the applicable port.                      |
| ip dhcp snooping trust                              | Sets an interface as a trusted port.                                                                                                          |
| no ip dhcp snooping verify mac-address              | Sets whether to check that the source MAC address in a DHCP packet received on an untrusted port matches the hardware address of the client.  |
| ip dhcp snooping vlan                               | Enables DHCP snooping in a VLAN.                                                                                                              |
| ip source binding                                   | Sets the binding database for terminals with fixed IP addresses.                                                                              |
| ip verify source                                    | Set this command to use the terminal filter based on the DHCP snooping binding database.                                                      |

### 23.2.2 Configuration procedure for DHCP snooping

This subsection gives a configuration example where DHCP snooping is performed via a Layer 3 switch as the basic configuration. It also gives examples of configuration of DHCP snooping. Configure the settings according to the following procedure.

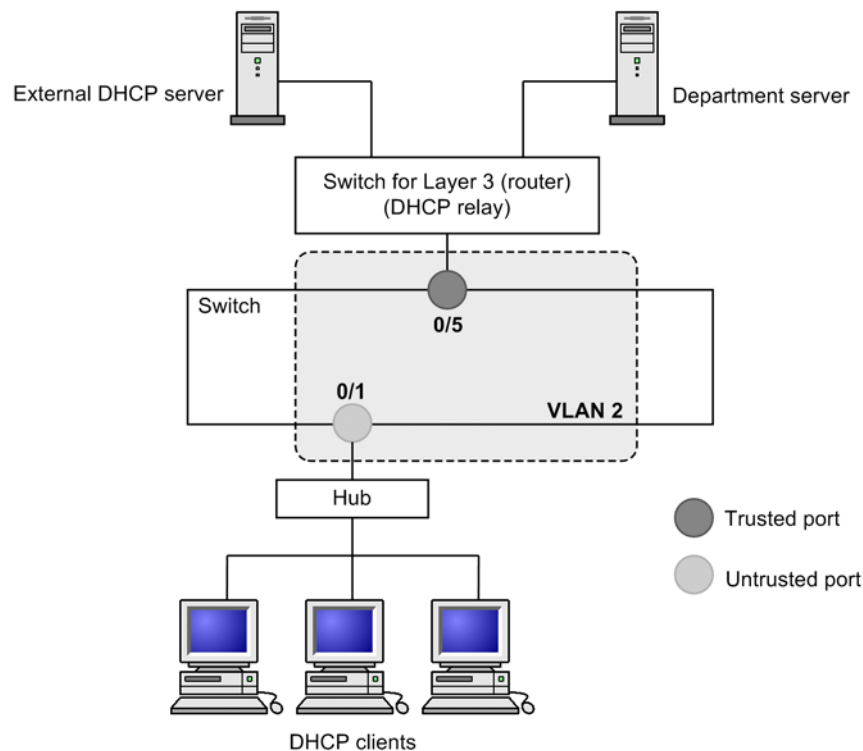
**Figure 23-11** Configuration procedure for DHCP snooping

### 23.2.3 Basic configuration (when DHCP snooping is performed via a Layer 3 switch)

This subsection describes the basic configuration for using DHCP snooping.

In a configuration where a DHCP server and a department server are connected via a Layer 3 switch, set the port connecting to the Layer 3 switch as a trust port.

**Figure 23-12** Configuration example where DHCP snooping is performed via a Layer 3 switch



### (1) Enabling DHCP snooping

Points to note

Enable DHCP snooping on the entire Switch and configure the following:

- Set the VLANs on which DHCP snooping is to be enabled.
- Set the port to which a DHCP server is connected as a trusted port.
- Set terminal filtering for untrusted ports. This discards packets from terminals not registered in the DB.

Command examples

1. `(config)# ip dhcp snooping`

Enables DHCP snooping on the entire Switch.

2. `(config)# vlan 2`  
`(config-vlan)# exit`

`(config)# ip dhcp snooping vlan 2`

Enables DHCP snooping on VLAN ID 2. DHCP snooping is enabled only on the VLANs that are specified by using this command.

3. `(config)# interface fastethernet 0/1`  
`(config-if)# switchport mode access`  
`(config-if)# switchport access vlan 2`  
`(config-if)# exit`

Sets port 0/1 as an access port, and sets VLAN ID 2 as the VLAN containing port 0/1.

**(2) Setting a trusted port**

## Points to note

Set the interface that uses the port to which a DHCP server is connected (port to which the Layer 3 switch is connected in the figure of configuration example) as a trusted port.

## Command examples

1. 

```
(config)# interface fastethernet 0/5
(config-if)# ip dhcp snooping trust
(config-if)# switchport mode access
(config-if)# switchport access vlan 2
(config-if)# exit
```

Sets port 0/5 as a trusted port. Other ports will be untrusted ports. The sequence also sets port 0/5 as an access port and sets VLAN ID 2 as the VLAN containing port 0/5.

**(3) Terminal filter setting**

## Points to note

Configure terminal filtering for the ports on which packets are to be discarded based on the binding database.

## Command examples

1. 

```
(config)# interface fastethernet 0/1
(config-if)# ip verify source port-security
(config-if)# exit
```

Configures terminal filtering on port 0/1 and sets the source IP addresses and source MAC addresses as the filtering conditions.

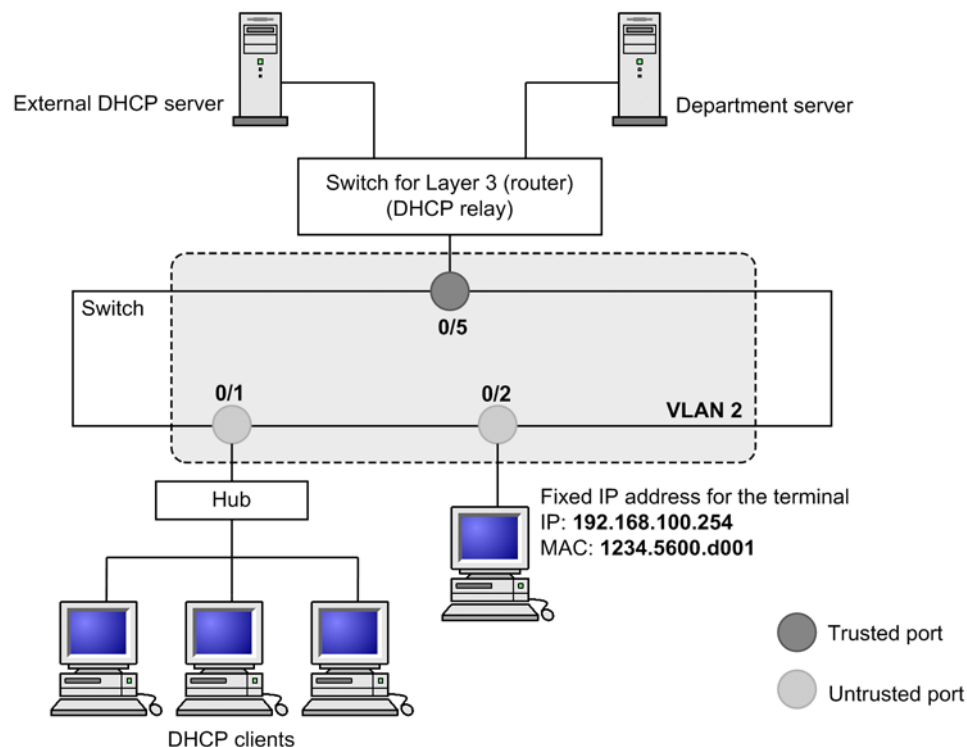
## Notes

Terminal filters are disabled on trusted ports even when this command is set. Also note that when DHCP snooping is enabled, terminal filtering is enabled for VLANs that are not specified by the `ip dhcp snooping vlan` command.

**(4) When connecting terminals with a fixed IP address**

The following describes how to connect a terminal with a fixed IP address to the Switch.



**Figure 23-13** Configuration example when connecting terminals with a fixed IP address

You can configure DHCP snooping as described in 23.2.3 *Basic configuration (when DHCP snooping is performed via a Layer 3 switch)*. In the example here, the terminal with a fixed IP address is connected to an untrusted port, and must therefore be registered in the binding database.

To configure the above settings, use configuration commands.

#### Points to note

The following example sets the binding database for a terminal with a fixed IP address.

#### Command examples

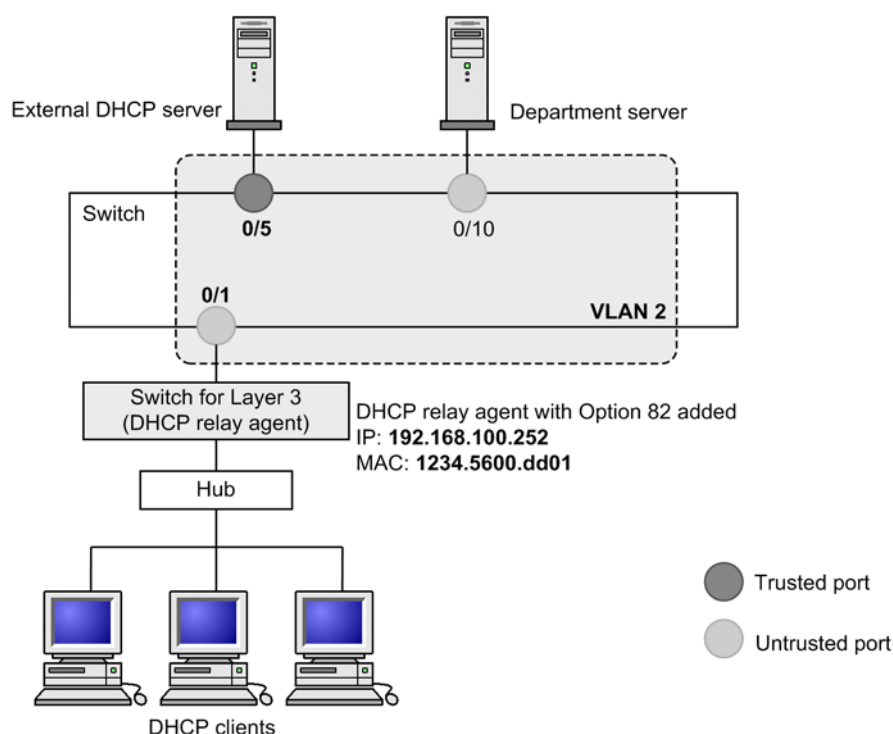
- ```
(config)# interface fastethernet 0/2
(config-if)# switchport mode access
(config-if)# switchport access vlan 2
(config-if)# exit
```

Sets VLAN ID 2 for port 0/2 to which a terminal with a fixed IP address is connected.
- ```
(config)# ip source binding 1234.5600.d001 vlan 2 192.168.100.254
interface fastethernet 0/2
```

Enters the MAC address of the terminal, the ID of the VLAN containing the terminal, the IP address of the terminal, and the number of the port to which the terminal is connected, in the binding database.

### 23.2.4 When connecting a DHCP relay agent to the Switch

When connecting a DHCP relay agent to the Switch which sends DHCP packets with Option 82, set the Switch so that it can forward packets with Option 82.

**Figure 23-14** Example configuration when a DHCP relay agent is connected under the Switch

You can configure DHCP snooping as described in 23.2.3 *Basic configuration (when DHCP snooping is performed via a Layer 3 switch)*. In this example, because the DHCP relay agent sends DHCP packets with Option 82, you need to set the Switch so that it permits forwarding of the packets with Option 82 on untrusted ports to which the DHCP relay agent is connected. In addition, you need to configure the following settings: not checking the source address in DHCP packets on the same untrusted port, permitting the forwarding of ARP packets, and using only IP addresses for terminal filtering.

To configure the above settings, use configuration commands.

### (1) Setting of permitting reception of the packets with Option 82 on untrusted ports

Points to note

Sets that DHCP packets with Option 82 can be received on untrusted ports.

Command examples

1. `(config)# ip dhcp snooping information option allow-untrusted`

Sets that DHCP packets with Option 82 can be received on untrusted ports.

### (2) Setting of canceling the check for the source addresses in DHCP packets on untrusted ports

Points to note

The following example sets the cancellation of the address check functionality so that the source MAC address in a DHCP packet is forwarded on an untrusted port without checking.

Command examples

1. `(config)# no ip dhcp snooping verify mac-address`

Sets the configuration so that the source MAC addresses in DHCP packets received on untrusted ports are not to be checked.

## Notes

If this is not set, the DHCP relay agent cannot be connected to an untrusted port because the source MAC address is checked.

### (3) Setting the binding database for which forwarding of ARP packets is to be permitted on untrusted ports

## Points to note

To forward ARP packets sent from a DHCP relay agent connected to an untrusted port, set the address of the DHCP relay agent in the binding database.

## Command examples

1. `(config)# ip source binding 1234.5600.dd01 vlan 2 192.168.100.252 interface fastethernet 0/1`

Enters the MAC address of the DHCP relay agent, the VLAN ID containing the DHCP relay agent, the IP address of the DHCP agent, and the number of the port to which the DHCP relay agent is connected, in the binding database.

### (4) Setting terminal filtering that filters only IP addresses on untrusted ports

## Points to note

Because the source MAC addresses in the packets sent from the DHCP clients are rewritten while the packets go through the Layer 3 switch, configure terminal filtering so that it filters only IP addresses on the untrusted port.

## Command examples

1. `(config)# interface fastethernet 0/1`  
`(config-if)# ip verify source`  
`(config-if)# exit`

Configures terminal filtering that filters only IP addresses on port 0/1.

## 23.2.5 Setting the rate of DHCP packet reception

Use the configuration to limit the reception rate on ports that receive DHCP packets.

You can configure DHCP snooping as described in 23.2.3 *Basic configuration (when DHCP snooping is performed via a Layer 3 switch)*.

### (1) Setting the reception rate

## Points to note

The following example sets the reception rate of port 0/1 that receives DHCP packets from the terminal.

## Command examples

1. `(config)# interface fastethernet 0/1`  
`(config-if)# ip dhcp snooping limit rate 50`  
`(config-if)# exit`

Set 50 packets per second as the reception rate for port 0/1.

## 23.2.6 Setting the dynamic ARP inspection functionality

This subsection describes the basic configuration for using the dynamic ARP inspection functionality.

You can configure DHCP snooping as described in 23.2.3 *Basic configuration (when DHCP snooping is performed via a Layer 3 switch)*.

### (1) Setting the VLANs used for dynamic ARP inspection (targets for the basic

**inspection)**

## Points to note

Of the VLANs for which DHCP snooping is enabled, set the VLAN IDs of the VLANs to be used for dynamic ARP inspection. ARP packets received in the specified VLANs are subject to the basic inspection.

## Command examples

1. `(config)# ip arp inspection vlan 2`

Sets VLAN ID 2 as a VLAN subject to dynamic ARP inspection. Dynamic ARP inspection will be performed only for VLANs for which this command is set.

## Notes

1. Specify the VLAN ID that was set by using the `ip dhcp snooping vlan` configuration command.
2. If this command sets a VLAN ID for dynamic ARP inspection, the binding database entries registered by the `ip source binding` configuration command are also subject to dynamic ARP inspection.
3. If you use the `ip arp inspection trust` configuration command to set a port belonging to the VLANs for which this command has been set, dynamic ARP inspection will not be performed on the port.

**(2) Setting ports on which dynamic ARP inspection is not performed**

## Points to note

The following example configures this setting for a port for which dynamic ARP inspection is not performed.

## Command examples

1. `(config)# interface fastethernet 0/5`  
`(config-if)# ip arp inspection trust`  
`(config-if)# exit`

Sets port 0/5 as the port on which dynamic ARP inspection is not performed. The other ports are set as ports on which dynamic ARP inspection is performed.

## Notes

1. Even if the ports which have been set by this command belong to VLANs subject to dynamic ARP inspection, dynamic ARP inspection will not be performed for those ports.
2. The ARP packet reception rate of the ports set by this command has no limit.

**(3) Setting the optional inspection of dynamic ARP inspection**

## Points to note

Set the optional inspection for the ARP packets for which the basic inspection was performed. In this example, set the configuration so that inspection is performed to check if the source MAC address and the sender MAC address of received ARP packets are the same.

## Command examples

1. `(config)# ip arp inspection validate src-mac`

Sets the src-mac check that checks if the source MAC address and the sender MAC address of received ARP packets are the same.

**(4) Setting the rate of ARP packet reception**

## Points to note

The following example sets the reception rate of port 0/1 that receives ARP packets from the terminal.

## Command examples

1. 

```
(config)# interface fastethernet 0/1
(config-if)# ip arp inspection limit rate 100
(config-if)# exit
```

Sets 100 packets per second as the reception rate for port 0/1.

**23.2.7 Setting how to save the binding database****(1) Setting the save location****(a) Saving the binding database in internal flash memory**

## Points to note

Internal flash memory can be specified as the location for saving the binding database.

## Command examples

1. 

```
(config)# ip dhcp snooping database url flash
```

Sets internal flash memory as the save location.

## Notes

If the **backup** operation command is executed, the binding database saved on internal flash memory is also backed up. You can use the **restore** operation command to restore the binding database.

**(b) Saving a binding database on a memory card**

## Points to note

A memory card can be specified as the location for saving a binding database. If you set a memory card, you can specify the name of the file for saving the database.

## Command examples

1. 

```
(config)# ip dhcp snooping database url mc dhcpsn-db
```

Sets a memory card as the save location and sets **dhcpsn-db** as the name of the file for saving the binding database.

## Notes

Before you set a memory card as the save location, make sure a card is already inserted in the memory card slot on the Switch. In addition, use memory cards manufactured by ALAXALA (AX-F2430-SD128).

**(2) Setting the wait-to-write time**

## Points to note

The following example sets the wait-to-write time used when a binding database is saved.

## Command examples

1. 

```
(config)# ip dhcp snooping database write-delay 3600
```

Sets 3600 seconds as the length of time to wait after one of the following save events occurs before the save processing is actually executed:

  - A dynamic binding database is registered, updated, or deleted.
  - When the **ip dhcp snooping database url** configuration command is specified (includes a change of save location)
  - When the **clear ip dhcp snooping binding** operation command is executed

## Notes

The length of time set by this command becomes operationally effective from the

## 23 DHCP Snooping

next save event.

## 23.3 DHCP snooping operation

### 23.3.1 List of operation commands

The following table describes the operation commands for DHCP snooping.

**Table 23-7** List of operation commands

| Command name                       | Description                                                    |
|------------------------------------|----------------------------------------------------------------|
| show ip arp inspection statistics  | Displays the dynamic ARP inspection statistics.                |
| clear ip arp inspection statistics | Clears the dynamic ARP inspection statistics.                  |
| show ip dhcp snooping              | Displays DHCP snooping information.                            |
| show ip dhcp snooping binding      | Displays information about the DHCP snooping binding database. |
| clear ip dhcp snooping binding     | Clears information in the DHCP snooping binding database.      |
| show ip dhcp snooping statistics   | Displays the DHCP snooping statistics.                         |
| clear ip dhcp snooping statistics  | Clears the DHCP snooping statistics.                           |

### 23.3.2 Checking DHCP snooping

#### (1) Checking information about DHCP snooping

Use the `show ip dhcp snooping` operation command to display information about DHCP snooping. This command displays the status of permission for the packets with Option 82, whether the source MAC addresses of DHCP packets can be checked, and a list of VLANs on which DHCP snooping is running.

The following figure shows the results of executing the `show ip dhcp snooping` operation command.

**Figure 23-15** Results of executing show ip dhcp binding

```
> show ip dhcp snooping

Date 2008/11/13 16:34:10 UTC
Switch DHCP snooping is Enable
Option allow untrusted: off, Verify mac-address: on
DHCP snooping is configured on the following VLANs:
 1,10,100,1000
Interface Trusted Verify source Rate limit(pps)
fastethernet 0/1 no off unlimited
fastethernet 0/2 yes off unlimited
:
:
port-channel 1 no off 200
port-channel 2 yes off unlimited

>
```

#### (2) Checking the binding database

Use the `show ip dhcp snooping binding` operation command to display the information in the binding database. The information includes the MAC addresses and IP addresses of terminals and the aging time of the binding database.

The following figure shows the results of executing the `show ip dhcp snooping binding` operation command.

**Figure 23-16** Result of executing show ip dhcp snooping binding

```
> show ip dhcp snooping binding

Date 2008/11/13 13:09:31 UTC

Agent URL: flash
Last succeeded time: 2008/11/13 13:07:34 UTC

Total Bindings: 14
MAC Address IP Address Expire(min) Type VLAN Interface 0/7
0000.0010.1010 192.168.100.250 8 dynamic 10 fastethernet 0/7
0000.e228.15a9 192.168.200.201 58 dynamic 10 fastethernet 0/8
:
:
```

### (3) Checking DHCP snooping statistics

Use the `show ip dhcp snooping statistics` operation command to display the DHCP snooping statistics. The statistics include the total number of DHCP packets received on untrusted ports, the number of DHCP packets received by each interface, the number of DHCP packets filtered out, and the number of DHCP packets discarded due to being in excess of the reception rate limit.

The following figure shows the results of executing the `show ip dhcp snooping statistics` operation command.

**Figure 23-17** Result of executing show ip dhcp snooping statistics

```
> show ip dhcp snooping statistics

Date 2008/11/13 18:19:28 UTC
Database Exceeded: 0
Total DHCP Packets: 8995
Interface Recv Filter Rate over
fastethernet 0/1 170 170 0
fastethernet 0/3 1789 10 1779
:
:
gigabitethernet 0/25 0 0 0
port-channel 1 3646 2457 1189
```

## 23.3.3 Checking dynamic ARP inspection

### (1) Checking the dynamic ARP inspection statistics

Use the `show ip arp inspection statistics` operation command to display the dynamic ARP inspection statistics. The statistics include the number of relayed ARP packets, the number of dropped ARP packets, and details about the dropped ARP packets.

The following figure shows the results of executing the `show ip arp inspection statistics` operation command.

**Figure 23-18** Result of executing show ip arp inspection statistics

```
show ip arp inspection statistics

Date 2008/11/14 13:09:52 UTC
```



| Port  | VLAN | Forwarded | Dropped ( | Rate over | DB unmatched | Invalid ) |
|-------|------|-----------|-----------|-----------|--------------|-----------|
| 0/1   | 11   | 0         | 15 (      | 0         | 15           | 0 )       |
| 0/2   | 11   | 584       | 883 (     | 0         | 883          | 0 )       |
| 0/3   | 11   | 0         | 0 (       | 0         | 0            | 0 )       |
| :     |      |           | :         |           |              |           |
| ChGr2 | 11   | 170       | 53 (      | 0         | 53           | 0 )       |
| #     |      |           |           |           |              |           |



---

## 24. Description of IGMP Snooping and MLD Snooping

IGMP snooping and MLD snooping are functionality that control multicast traffic within a VLAN for Layer 2 switching. This chapter explains IGMP snooping and MLD snooping.

---

|                                                 |
|-------------------------------------------------|
| 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 |
|----------------------------------------------------|

---

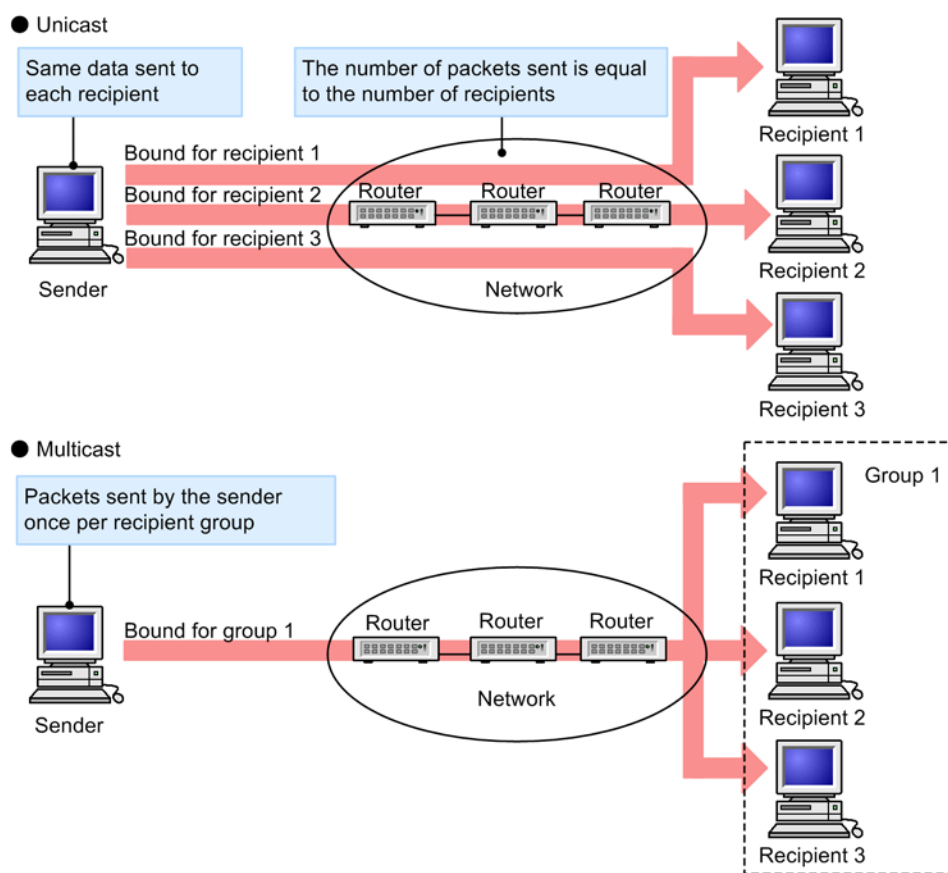
## 24.1 Overview of IGMP snooping and MLD snooping

This section gives 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 gives an overview of multicast.

**Figure 24-1** Overview of multicasting



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) |

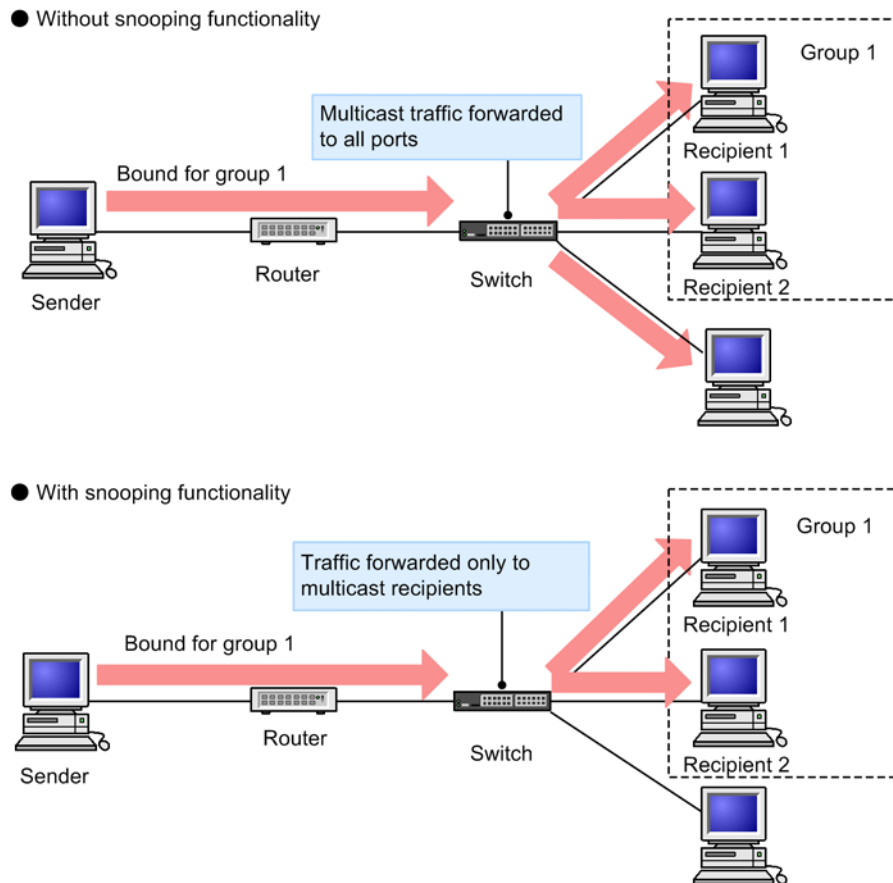
### 24.1.2 Overview of IGMP snooping and MLD snooping

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 gives 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 router hosts by using IGMP on IPv4 networks and MLD on IPv6 networks. The protocol detects packets sent from the host, indicating group participation and detachment, 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 lists the IGMP snooping and MLD snooping functionality supported by the Switch.

**Table 24-2** Supported functions

| Item                                            |      | Support                                                                                | Remarks                    |
|-------------------------------------------------|------|----------------------------------------------------------------------------------------|----------------------------|
| Interface type                                  |      | Full Ethernet support<br>Only Ethernet V2 frame formats                                | --                         |
| Supported IGMP version<br>Supported MLD version |      | IGMP: Version 1 and 2<br>MLD: Version 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<br>MLD querier                     |      | Querier operation is performed according to the IGMPv2, MLDv1, or MLDv2 specifications | --                         |
| Settings for multicast router connection ports  |      | Static settings by configuration                                                       | --                         |

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.

When IGMP snooping is used, the MAC address control method is used to control forwarding for multicast traffic.

### 24.3.1 MAC address control method

#### (1) MAC address learning

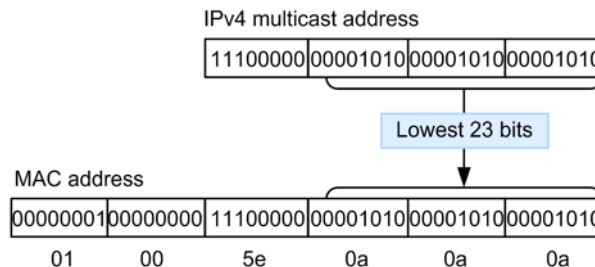
For VLANs for which IGMP snooping is set, multicast MAC addresses are dynamically learned when IGMP messages are received. The learned multicast MAC addresses are registered to the MAC address table.

##### (a) Registering entries

When an IGMP Report 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 IGMP Report messages have been received.

Destination MAC addresses for IPv4 multicast data are generated by copying the lowest 23 bits of the IP address to the MAC address. Therefore, MAC addresses will be redundant for IP addresses for which the lower 23 bits are the same. For example, the multicast MAC address for both 224.10.10.10 and 225.10.10.10 is 0100.5E0A.0A0A. These addresses are treated as packets bound for the same MAC address by Layer 2 forwarding. The following figure shows the correspondence between IPv4 multicast addresses and MAC addresses.

**Figure 24-3** Correspondence between IPv4 multicast addresses and MAC addresses



##### (b) Deleting entries

Learned multicast MAC addresses are deleted in either 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 only sent when a querier is set and are sent from a representative querier otherwise). If there is no response, only that port is deleted from the entries (forwarding of multicast traffic to this port is suppressed). If no group members are left in all ports in the VLAN, the entry itself is deleted.

- A set time elapses after an IGMP 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 IGMP Report (membership request) message within 260 seconds, it deletes the corresponding entries.

## (2) Layer 2 forwarding for IPv4 multicast packet

Layer 2 forwarding within VLANs receiving IPv4 multicast packets is performed based on MAC address. Layer 2 forwarding is performed based on IGMP snooping results for all ports that receive IGMP Report (membership request) messages with IP multicast addresses that are mapped to the same MAC address.

Because the multicast MAC address for both 224.10.10.10 and 225.10.10.10 as shown in the example for (a) *Registering entries* in (1) *MAC address learning* is 0100.5E0A.0A0A, when Layer 2 forwarding is performed for multicast data bound for 224.10.10.10, that multicast data is also forwarded to the 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 router 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 IGMP messages

| 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.<br>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 IGMP Report (membership request) message receives an IGMP Leave message, the IGMP Leave 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.

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.

## 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.

When MLD snooping is used, the MAC address control method is used to control forwarding for multicast traffic.

### 24.4.1 MAC address control method

#### (1) MAC address learning

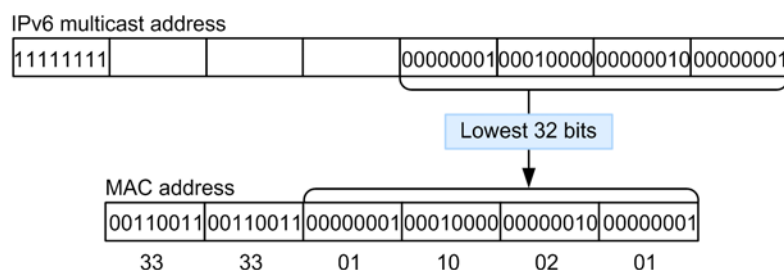
For VLANs for which MLD snooping is set, multicast MAC addresses are dynamically learned when MLD messages are received. The learned multicast MAC addresses are registered to the MAC address table.

##### (a) Registering entries

When an MLDv1 Report message or 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 only sent when a querier is set and are sent from a representative querier otherwise). If there is no response, only that port is deleted from the entries (forwarding of multicast traffic to this port is suppressed). If no group members are left in all ports in the VLAN, the entry itself is deleted.
- An MLDv2 Report (detachment request) message is received.  
Group-Specific Query messages are sent from the Switch to the port that received MLDv2 Report (detachment request) messages, twice every second (Group-Specific Query messages are only sent when a querier is set and are sent from a

representative querier otherwise). If there is no response, only that port is deleted from the entries (forwarding of multicast traffic to this port is suppressed). If no group members are left in all ports in the VLAN, the entry itself is deleted. However, when an MLDv2 Report message whose multicast address record type is BLOCK\_OLD\_SOURCES is received, Group-Specific Query messages are sent and entry deletion processing is performed only when a querier has been set for the local device.

- A set time elapses after an MLDv1 or MLDv2 Report (membership request) message is received.

Multicast routers regularly send MLD Query messages to check that group members exist in directly connected interfaces. When the Switch receives an MLD Query message from a router, it forwards it to all ports in the VLAN. If there is no response to the MLD Query message, only that port is deleted from the entries. When no response is received from any port, the entry itself is deleted.

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 address, just as for IPv4 multicast packets. Layer 2 forwarding based on MLD snooping results is performed for all ports that receive MLD Report (membership request) messages whose IPv6 multicast address is mapped to the same MAC address.

### 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 24-4** 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.<br>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 24-5** 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.                                                                                                                     |         |
|                                    | Detachment Request Report | Not forwarded to any port when group members still exist for other ports.<br>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 (detachment request) message, the MLDv2 Report (detachment 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 an MLD Query message every 125 seconds.

In order to use the MLD querier functionality, the source IP address of the 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 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 *15.3 Compatibility between Layer 2 switch functionality and other functionality*.

### (2) Control packet flooding

Because multicast traffic that is subject to suppression by IGMP snooping or MLD snooping is data traffic, flooding needs to be performed within a VLAN so that the routing protocol and other control packets can be received by all routers and all hosts. Therefore, the Switch forwards packets with destination IP addresses contained in the address ranges shown in the table below to all ports on the VLAN. Packets with destination IP addresses outside the address ranges shown in the following table are forwarded according to learning results for multicast MAC addresses.

**Table 24-6** 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 lists multicast group addresses that cannot be used for addresses outside the address ranges shown in the above table.

**Table 24-7** 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) Configuring 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 such a configuration, enable the IGMP snooping and MLD snooping functionality on each Layer 2 switch (connect to the switches that support snooping).

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 Switch does not support IGMP version 3 (abbreviated hereafter to *IGMPv3*). If the IGMP snooping functionality is used, data packets are not forwarded because the Switch does not recognize a membership request for joining to an IGMPv3 group. When connecting to an IGMPv3 host, disable the IGMP snooping functionality on the host.

**(5) Connections with MLD version 2 hosts**

When connecting an MLDv2 host to the Switch, make sure that you connect an MLDv2 router and set an IP address so that the router becomes the representative querier. If the representative querier is an MLDv1 router, the network will operate in MLDv1 mode.

Use a configuration in which MLDv2 messages from MLDv2 hosts are not split into fragments.





---

## 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 explains 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 commands used to configure IGMP snooping.

**Table 25-1** List of configuration commands

| Command name                 | Description                                                                     |
|------------------------------|---------------------------------------------------------------------------------|
| ip igmp snooping (global)    | Suppresses IGMP snooping for the Switch when <b>no ip igmp snooping</b> is set. |
| ip igmp snooping (interface) | Sets IGMP snooping functionality for the specified interface.                   |
| ip igmp snooping mrouter     | Sets IGMP multicast router ports.                                               |
| ip igmp snooping querier     | 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 for 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 corresponding 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 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)# ip igmp snooping mrouter interface fastethernet 0/1
(config-if)# exit
```

Specifies the multicast router port for the corresponding interface.

### Notes

If you set 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                           |
|---------------------|---------------------------------------|
| show igmp-snooping  | Displays IGMP snooping information.   |
| clear igmp-snooping | Clears all IGMP snooping information. |

### 25.2.2 Checking IGMP snooping

The following describes the IGMP snooping contents to be checked when IGMP snooping functionality is used.

#### (1) Checking the setting status of IGMP snooping

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 2008/11/14 15:56:12 UTC
VLAN counts: 3
VLAN 3253:
 IP Address: 192.168.53.100/24 Querier: enable
 IGMP querying system: 192.168.53.100
 Port (4): 0/13-16
 Mrouter-port: 0/13-16
 Group counts: 5
VLAN 3254:
 IP Address: 192.168.54.100/24 Querier: disable
 IGMP querying system:
 Port (4): 0/17-20
 Mrouter-port: 0/17-20
 Group counts: 5
VLAN 3255:
 IP Address: 192.168.55.100/24 Querier: disable
 IGMP querying system:
 Port (4): 0/21-24
 Mrouter-port: 0/21-24
 Group counts: 5

>
```

#### (2) 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 the statuses of learned MAC addresses, IPv4 multicast addresses forwarded within a VLAN, and a list of forwarding destination ports.

**Figure 25-2** Results of executing the show igmp-snooping group command

```
> show igmp-snooping group
```

```

Date 2008/11/14 15:59:41 UTC
Total Groups: 15
VLAN counts: 3
VLAN 3253 Group counts: 5
 Group Address MAC Address
 230.0.0.11 0100.5e00.000b
 Port-list: 0/13
 230.0.0.10 0100.5e00.000a
 Port-list: 0/13
 230.0.0.14 0100.5e00.000e
 Port-list: 0/13
 230.0.0.13 0100.5e00.000d
 Port-list: 0/13
 230.0.0.12 0100.5e00.000c
 Port-list: 0/13
VLAN 3254 Group counts: 5
 Group Address MAC Address
 230.0.0.34 0100.5e00.0022
 Port-list: 0/18
 230.0.0.33 0100.5e00.0021
 Port-list: 0/18
 230.0.0.32 0100.5e00.0020
 Port-list: 0/18
 230.0.0.31 0100.5e00.001f
 Port-list: 0/18
 230.0.0.30 0100.5e00.001e
 Port-list: 0/18
VLAN 3255 Group counts: 5
 Group Address MAC Address
 230.0.0.24 0100.5e00.0018
 Port-list: 0/21
 230.0.0.23 0100.5e00.0017
 Port-list: 0/21
 230.0.0.22 0100.5e00.0016
 Port-list: 0/21
 230.0.0.21 0100.5e00.0015
 Port-list: 0/21
 230.0.0.20 0100.5e00.0014
 Port-list: 0/21

```

>

- Use the `show igmp-snooping port` operation command to check the participation group display example for individual ports.

**Figure 25-3** Result of executing the `show igmp-snooping port` command

```
> show igmp-snooping port 0/13
```

```

Date 2008/11/14 16:03:28 UTC
Port 0/13 VLAN counts: 1
VLAN 3253 Group counts: 5
 Group Address Last Reporter Uptime Expires
 230.0.0.11 192.168.53.17 19:20 04:19
 230.0.0.10 192.168.53.16 19:20 04:20
 230.0.0.14 192.168.53.20 19:20 04:19
 230.0.0.13 192.168.53.19 19:20 04:19
 230.0.0.12 192.168.53.18 19:20 04:19

```

>

## 25.3 Configuration of MLD snooping

### 25.3.1 List of configuration commands

The following table describes the commands used to configure MLD snooping.

**Table 25-3** List of configuration commands

| Command name                  | Description                                                                     |
|-------------------------------|---------------------------------------------------------------------------------|
| ipv6 mld snooping (global)    | Suppresses MLD snooping for the Switch when <b>no ipv6 mld snooping</b> is set. |
| ipv6 mld snooping (interface) | Sets MLD snooping for the specified interface.                                  |
| ipv6 mld snooping mrouter     | Sets MLD multicast router ports.                                                |
| ipv6 mld snooping querier     | Sets MLD querier functionality.                                                 |
| ipv6 mld snooping source      | Sets the source IP address of the MLD Query message sent from the Switch.       |

### 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 the MLD querier functionality

#### Points to note

When no multicast router exists within a VLAN for which MLD snooping is set, MLD querier functionality needs to be run. The following sets the VLAN interface configuration mode for the corresponding VLAN.

#### Command examples

1. 

```
(config)# interface vlan 2
(config-if)# ipv6 mld snooping querier
(config-if)# exit
```

Enables MLD querier functionality.

#### Notes

This setting is enabled only when the source IP address of the MLD Query message is set on the relevant 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 fastethernet 0/1
(config-if)# exit
```

Specifies the multicast router port for the corresponding interface.

#### Notes

If you set a port number belonging to a port channel interface for a multicast router port, no operation is performed.

### 25.3.5 Setting the source IP address of an MLD Query message

#### Points to note

When using the MLD querier functionality, you must specify the source IP address of a Query message sent from the Switch. Specify the following settings in VLAN interface configuration mode for the VLAN for 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 the source IP address of the MLD Query message for the target interface to `fe80::1`.

#### Notes

1. This command is applied to the source IP address of the MLD Query message.
2. Set 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                          |
|--------------------|--------------------------------------|
| show mld-snooping  | Displays MLD snooping information.   |
| clear mld-snooping | Clears all MLD snooping information. |

### 25.4.2 Checking MLD snooping

The following describes the MLD snooping contents to be checked when MLD snooping functionality is used.

#### (1) Checking the setting status of MLD snooping

Execute the `show mld-snooping` operation command to check that the settings related to MLD snooping are correct.

**Figure 25-4** Displayed status for MLD snooping settings

```
> show mld-snooping

Date 2008/11/14 17:21:37 UTC
VLAN counts: 3
VLAN 3001:
 IP Address: Querier: enable
 MLD querying system:
 Querier version: v1
 Port (1): 0/12
 Mrouter-port: 0/12
 Group counts: 1
VLAN 3002:
 IP Address: Querier: enable
 MLD querying system:
 Querier version: v1
 Port (1): 0/12
 Mrouter-port: 0/12
 Group counts: 1
VLAN 3003:
 IP Address: Querier: enable
 MLD querying system:
 Querier version: v1
 Port (1): 0/12
 Mrouter-port: 0/12
 Group counts: 1

>
>
```

#### (2) During operation

Execute the following command to check the status of MLD snooping during operation.

- Use the `show mld-snooping group` operation command to check the statuses of learned MAC addresses, IPv6 multicast addresses forwarded within a VLAN, and a



list of forwarding destination ports.

**Figure 25-5** Results of executing the show mld-snooping group command

```
> show mld-snooping group

Date 2008/11/14 17:22:05 UTC
Total Groups: 3
VLAN counts: 3
VLAN 3001 Group counts: 1
 Group Address MAC Address Version Mode
 ff80:0:0:0:0:99:a0a 3333.0099.0a0a v1 -
 Port-list: 0/12
VLAN 3002 Group counts: 1
 Group Address MAC Address Version Mode
 ff80:0:0:0:0:99:a0a 3333.0099.0a0a v1 -
 Port-list: 0/12
VLAN 3003 Group counts: 1
 Group Address MAC Address Version Mode
 ff80:0:0:0:0:99:a0a 3333.0099.0a0a v1 -
 Port-list: 0/12

>
```

- Use the `show mld-snooping port` operation command to check the participation group display example for individual ports.

**Figure 25-6** Results of executing the show mld-snooping port command

```
> show mld-snooping port 0/12

Date 2008/11/14 17:22:45 UTC
Port 0/12 VLAN counts: 3
VLAN 3001 Group counts: 1
 Group Address Last Reporter Uptime Expires
 ff80:0:0:0:0:99:a0a fe:80:0:0:0:0:fe00 07:10 04:20
VLAN 3002 Group counts: 1
 Group Address Last Reporter Uptime Expires
 ff80:0:0:0:0:99:a0a fe:80:0:0:0:0:fe00 05:02 04:20
VLAN 3003 Group counts: 1
 Group Address Last Reporter Uptime Expires
 ff80:0:0:0:0:99:a0a fe:80:0:0:0:0:fe00 05:02 04:20

>
```



## 26. IPv4 Interfaces

This chapter describes IPv4 interfaces and explains how to use them.

|      |               |
|------|---------------|
| 26.1 | Description   |
| 26.2 | Configuration |
| 26.3 | Operation     |

## 26.1 Description

You can set IPv4 addresses for VLANs so that the Switch can use SNMP, Telnet, and FTP communications for management use. To allow the Switch to communicate to other subnets, static routes must be configured for the subnets.

Also, the Switch detects duplication of IPv4 addresses set for VLAN interfaces. There is no configuration for enabling duplication detection. Setting IPv4 addresses for VLAN interfaces automatically enables duplication detection for the VLAN interfaces.

### (1) Detecting duplication of IP addresses

The Switch checks for the duplication of IP addresses set for the VLAN interfaces on the Switch. The Switch sends a gratuitous ARP for each VLAN interface, and checks whether the source IP addresses in the received ARP packets are duplicated.

#### (a) Gratuitous ARPs sent from the Switch

The Switch sends a gratuitous ARP in which the IP address set for the VLAN interface on the Switch is set in the Target Protocol Address field. Each time a VLAN interface goes up, one gratuitous ARP packet is sent.

#### (b) ARP packets checked for duplication

All ARP packets (not only gratuitous ARP response packets) that are received normally are checked for duplication as long as the following conditions are met:

- The destination MAC address is the unicast address for a VLAN on the Switch, or a broadcast address.
- The packet is not discarded by a Spanning Tree Protocol, access lists, dynamic ARP inspection, or authentication method on the Switch.
- An IP address has been set for the VLAN interface that receives the packet.

#### (c) Detection conditions

A duplicate IP address is detected when all the following conditions are met:

- The source MAC address in the ARP payload is other than the unicast MAC address for the Switch (common to all VLANs).
- The source IP address is the IP address set for the Switch.

#### (d) Operation when a duplication is detected

When the duplication of an IP address is detected, the Switch outputs an operation log containing the following information.

**Table 26-1** Operation log information output when a duplication of an IP address is detected

| Information included in a log | 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 that has a duplicate IP address (source MAC address in the ARP payload) |

However, if an operation log was output for the same IP address within the past 10 minutes, a new operation log will not be output.

## 26.2 Configuration

### 26.2.1 List of configuration commands

The following table shows the configuration commands used to configure IPv4 interfaces.

**Table 26-2** List of configuration commands

| Command name | Description                                 |
|--------------|---------------------------------------------|
| ip address   | Specifies an IPv4 address for an interface. |
| ip route     | Specifies IPv4 static routes.               |

### 26.2.2 Configures an interface.

Points to note

The example below shows how to set an IPv4 address for a VLAN. To do so, switch to interface configuration mode.

Command examples

1. `(config)# interface vlan 100`  
Switches to interface configuration mode for VLAN ID 100.
2. `(config-if)# ip address 192.168.1.1 255.255.255.0`  
`(config-if)# exit`  
Sets IPv4 address 192.168.1.1 and subnet mask 255.255.255.0 for VLAN ID 100.

### 26.2.3 Setting static routes

Points to note

The Switch does not support the setting of routing protocols. To enable communication to subnets outside the VLANs, you must set static routes.

Command examples

1. `(config)# ip route 192.168.2.0 255.255.255.0 192.168.1.254`  
Specifies 192.168.1.254 as the forwarding route to the destination subnet 192.168.2.0/24.

## 26.3 Operation

### 26.3.1 List of operation commands

The following table shows the operation commands related to the IPv4 interface.

**Table 26-3** List of operation commands

| Command name      | Description                                  |
|-------------------|----------------------------------------------|
| show ip interface | Displays the status of IPv4 interfaces.      |
| show ip arp       | Displays the information in the ARP entries. |
| show ip route     | Displays the routing table.                  |
| ping              | Performs an echo test.                       |
| tracert           | Displays the route.                          |

### 26.3.2 Checking the up/down state of an IPv4 interface

After setting an IPv4 address for a line or a port on a line of the Switch connected to an IPv4 network, execute the `show ip interface` operation command to confirm that the up/down state of the IPv4 interface is **UP**.

**Figure 26-1** Example of displaying the IPv4 interface status

```
>show ip interface summary

Date 2008/11/14 17:47:34 UTC
VLAN0001: Up 192.168.0.100/24
VLAN0010: Down 192.168.10.100/24
VLAN3005: Up 192.168.5.10/24
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 reachability to the destination

Execute the `ping` operation command for an interface in the Switch connected to the IPv4 network to determine whether the destination device is reachable.

**Figure 26-2** Results of executing the ping command (when the destination is reachable)

```
> ping 192.168.0.1
Pinging 192.168.0.1 with 46 bytes of data:
Reply from 192.168.0.1: count=1, bytes=46
Reply from 192.168.0.1: count=2, bytes=46
Reply from 192.168.0.1: count=3, bytes=46
Reply from 192.168.0.1: count=4, bytes=46

--- 192.168.0.1 PING Statistics ---
 Packets: sent 4, received 4, lost 0 (0% loss)
>
```

**Figure 26-3** Results of executing the ping command (when the destination is unreachable)

```
> ping 192.168.0.1
Pinging 192.168.0.1 with 46 bytes of data:
Request Timeout
Request Timeout
Request Timeout
Request Timeout

--- 192.168.0.1 Ping Statistics ---
 Packets: sent 4, received 0, lost 4 (100.% loss)
>
```

### 26.3.4 Checking the route to the destination

Execute the `tracert` operation command to check the relay devices between the interface of the Switch connected to the IPv4 network and a destination.

**Figure 26-4** Results of executing the traceroute command

```
> traceroute -m 3 192.168.0.1
traceroute to 192.168.0.1 over a maximum 3 hops:
 1 <10 ms 20 ms 10 ms x.x.x.x
 2 <10 ms 10 ms <10 ms x.x.x.x
 3 x.x.x.x reports: Destination host unreachable.
>
```

### 26.3.5 Checking ARP information

After setting an IPv4 address for a line or a port on a line in the Switch connected to an IPv4 network, execute the `show ip arp` operation command to check whether the addresses are resolved between the Switch and the neighboring device (that is, whether ARP entries exist).

**Figure 26-5** Results of executing the show ip arp command

```
> show ip arp

Date 2008/11/14 22:04:23 UTC
Total: 8

```

| IP Address    | Linklayer Address | Interface | Expire | Type |
|---------------|-------------------|-----------|--------|------|
| 10.0.0.55     | 0013.20ad.0155    | VLAN2048  | 20min  | arpa |
| 10.0.0.56     | 0013.20ad.0156    | VLAN2048  | 20min  | arpa |
| 10.0.0.57     | 0013.20ad.0157    | VLAN2048  | 20min  | arpa |
| 10.0.0.58     | 0013.20ad.0158    | VLAN2048  | 20min  | arpa |
| 10.0.0.59     | 0013.20ad.0159    | VLAN2048  | 20min  | arpa |
| 10.10.10.1    | incomplete        | VLAN2048  | --     | arpa |
| 192.20.0.2    | 0080.452d.9701    | VLAN2000  | 12min  | arpa |
| 192.168.0.200 | incomplete        | VLAN3333  | --     | arpa |

```
>
```

### 26.3.6 Checking the routing table

You can display the IPv4 routing table. Execute the `show ip route` operation command to check whether the routes between the Switch and the devices on other subnets are set.

**Figure 26-6** Results of executing the show ip route command

```
> show ip route

Date 2008/11/14 17:32:39 UTC
Total: 5

```

| Destination    | Nexthop       | Interface | Protocol  |
|----------------|---------------|-----------|-----------|
| 192.168.0.0/24 | 192.168.0.100 | VLAN0001  | Connected |

## 26 IPv4 Interfaces

|                 |                |          |           |
|-----------------|----------------|----------|-----------|
| 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 |

>



## Appendix

---

### A. Relevant standards

---

## A. Relevant standards

### A.1 TELNET/FTP

**Table A-1** Relevant standards and recommendations for TELNET/FTP

| Name (month and year issued) | Title                         |
|------------------------------|-------------------------------|
| RFC 854 (May 1983)           | TELNET PROTOCOL SPECIFICATION |
| RFC 855 (May 1983)           | TELNET OPTION SPECIFICATIONS  |
| RFC 959 (October 1985)       | FILE TRANSFER PROTOCOL (FTP)  |

### A.2 RADIUS

**Table A-2** Relevant standard and recommendation for RADIUS

| Name (month and year issued) | Title                                               |
|------------------------------|-----------------------------------------------------|
| RFC 2865 (June 2000)         | Remote Authentication Dial In User Service (RADIUS) |

### A.3 NTP

**Table A-3** Relevant standard and recommendation for NTP

| Name (month and year issued) | Title                                                               |
|------------------------------|---------------------------------------------------------------------|
| RFC 2030 (October 1996)      | Simple Network Time Protocol (SNTP) Version4 for IPv4, IPv6 and OSI |

### A.4 Ethernet

**Table A-4** Relevant standards for Ethernet interfaces

| Type                                                                 | Standards              | Model name                                                                                                                                                                                           |
|----------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10BASE-T,<br>100BASE-TX,<br>100BASE-FX,<br>1000BASE-T,<br>1000BASE-X | IEEE802.2 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 |
|                                                                      | IEEE802.3 2000 Edition | Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer Specifications                                                                                     |
|                                                                      | IEEE802.3ah 2004       | Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks                                                                                |

| Type | Standards                       | Model name                                                                                                                                                                                          |
|------|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PoE  | IEEE802.3af<br>IEEE802.3at/D3.1 | Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Data Terminal Equipment (DTE)Power via Media Dependent Interface (MDI). |

## A.5 Link aggregation

**Table A-5** Relevant standard for link aggregation

| Standards                              | Model name                            |
|----------------------------------------|---------------------------------------|
| IEEE802.3ad<br>(IEEE Std 802.3ad-2000) | Aggregation of Multiple Link Segments |

## A.6 VLAN

**Table A-6** Relevant standard and recommendation for VLANs

| Standards                            | Model name                                       |
|--------------------------------------|--------------------------------------------------|
| IEEE802.1Q<br>(IEEE Std 802.1Q-2003) | Virtual Bridged Local Area Networks <sup>#</sup> |

#

GVRP/GMRP is not supported.

## A.7 Spanning Tree Protocol

**Table A-7** Relevant standards and recommendation for Spanning Tree Protocols

| Standards                                         | Model name                                                                       |
|---------------------------------------------------|----------------------------------------------------------------------------------|
| IEEE802.1D<br>(ANSI/IEEE Std 802.1D-1998 Edition) | Media Access Control (MAC) Bridges<br>(The Spanning Tree Algorithm and Protocol) |
| IEEE802.1t<br>(IEEE Std 802.1t-2001)              | Media Access Control (MAC) Bridges -<br>Amendment 1                              |
| IEEE802.1w<br>(IEEE Std 802.1w-2001)              | Media Access Control (MAC) Bridges -<br>Amendment 2: Rapid Reconfiguration       |
| IEEE802.1s<br>(IEEE Std 802.1s-2002)              | Virtual Bridged Local Area Networks -<br>Amendment 3: Multiple Spanning Trees    |

## A.8 IGMP snooping and MLD snooping

**Table A-8** Relevant standards and recommendation for IGMP snooping and MLD snooping

| Name (month and year issued)                   | Title                          |
|------------------------------------------------|--------------------------------|
| draft-ietf-magma-snoop-12.txt<br>(August 2005) | IGMP and MLD snooping switches |

## A.9 IPv4 interface

**Table A-9** Relevant standards and recommendations for IP version 4

| Name (month and year issued) | Title                                                                                                                                              |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 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                                                                                               |

# Index

## A

- abbreviated-command execution, 51
- access ports and trunk ports, 261
- adding, changing, and deleting configuration entries, 69
- aging and MAC address learning, 242
- allocating power supplied by PoE [AX1240S], 200
- allocating power that can be supplied to each port, 211
- allocating the power supplied by PoE [AX2200S], 197
- application functionality and scope of RADIUS authentication, 86
- assigning an IP address to the Switch, 77
- authentication using RADIUS, 88
- automatic MDIX functionality settings, 162, 173, 184
- automatic SFP recognition (selection of media type) [AX1250S] [AX1240S], 182

## B

- backing up and restoring device information, 113
- basic configuration (when DHCP snooping is performed via a Layer 3 switch), 420
- basic configuration for the multi-fault monitoring functionality, 373
- basic Ring Protocol principles, 356
- BPDU filter, 340

## C

- capacity limit, 19
- changing blocked ports, 291
- changing the login user, 83
- checking ARP information, 461
- checking DHCP snooping, 429
- checking dynamic ARP inspection, 430
- checking IGMP snooping, 450
- checking MLD snooping, 454
- checking PVST+ statuses, 315
- checking Ring Protocol statuses, 395
- checking the Ethernet operating status, 165
- checking the MAC address learning count, 248
- checking the Multiple Spanning Tree status, 337
- checking the PoE power supply status, 212
- checking the reachability to the destination, 460
- checking the route to the destination, 461
- checking the routing table, 461
- checking the Single Spanning Tree status, 323
- checking the software version, 109
- checking the status of common Spanning Tree functionality, 349
- checking the status of MAC address learning, 248

- checking the switch status, 110
- checking the time, 105
- checking the up/down state of an IPv4 interface, 460
- checking VLAN extended functionality, 292
- checking VLAN status, 281
- clearing the MAC address table, 243
- command input mode, 48
- command operations, 47
- commands
  - operations, 47
- compatibility between AX2200S and AX1200S series switches, 115
- compatibility between Layer 2 switch functionality and other functionality, 236
- compatibility of device information between AX1250S series switches and AX1240S series switches, 117
- compatibility of device information between AX1250S/AX1240S series switches and AX1230S series switches, 118
- compatibility of input commands between AX1250S/AX1240S series switches and AX1230S series switches, 115
- compatibility with other Spanning Tree Protocols, 329
- configuration, 61
- configuration at startup, 62
- configuration common to all Ethernet interfaces, 159
- configuration components for Spanning Tree topologies, 299
- configuration during operation, 62
- configuration editing procedures, 66
- configuration of a port channel interface, 221
- configuration of DHCP snooping, 419
- configuration of FastEthernet [AX1250S] [AX1240S], 172
- configuration of GigabitEthernet (RJ45), 183, 195
- configuration of IGMP snooping, 448
- configuration of LACP link aggregation, 220
- configuration of MAC VLANs, 275
- configuration of MLD snooping, 452
- configuration of Multiple Spanning Tree, 331
- configuration of PoE [AX2200S] [AX1240S], 209
- configuration of protocol VLANs, 267
- configuration of Single Spanning Tree, 318
- configuration of the basic link aggregation functionality, 219
- configuration of the basic VLAN functionality, 258
- configuration of the common Spanning Tree functionality, 345
- configuration of the inter-port relay blocking functionality, 290
- configuration of the link aggregation extended functionality, 228
- configuration of the Spanning Tree operating

- mode, 304
- configuration of the standby link functionality, 228
- configuration operations, 72
- configuration procedure for DHCP snooping, 419
- configures an interface., 459
- configuring
  - L2 protocol frame transparency functionality, 287
  - port VLANs, 262
- configuring a port VLAN, 262
- configuring a RADIUS server group, 95
- configuring a VLAN group, 389
- configuring IGMP snooping, 448
- configuring link types, 348
- configuring loop guards, 347
- configuring MAC VLANs, 275
- configuring MLD snooping, 452
- configuring modes and ring ports (for multi-ring configurations with shared links), 390
- configuring multicast router ports, 448, 453
- configuring multiple ports at one time, 160
- configuring Multiple Spanning Tree, 331, 334
- configuring Multiple Spanning Tree parameters, 334
- configuring native VLAN for protocol ports, 269
- configuring native VLANs for MAC ports, 278
- configuring native VLANs for trunk ports, 263
- configuring port VLANs, 262
- configuring ports, 172, 183, 259
- configuring PVST+, 310, 311, 312
- configuring PVST+ parameters, 312
- configuring PVST+ topologies, 311
- configuring RADIUS, 93
- configuring ring IDs, 387
- configuring Single Spanning Tree, 318
- configuring Single Spanning Tree parameters, 320
- configuring static entries, 246
- configuring static link aggregation, 219
- configuring the IGMP querier functionality, 448
- configuring the inter-port relay blocking functionality, 290
- configuring the L2 protocol frame transparency functionality, 287
- configuring the MLD querier functionality, 452
- configuring the operating mode, 304
- configuring topologies for Multiple Spanning Tree, 332
- configuring topologies for Single Spanning Tree, 319
- configuring VLANs, 258
- connecting to RADIUS servers, 91
- connection characteristics, 41
- connections between switches and MAC address settings, 271
- connections with multicast routers, 438, 441
- control on the MAC and LLC sublayers, 155
- cooling fan control (Semi-fanless operation)

- [AX1240S], 134
- creating protocol VLANs, 267

## D

- deleting a channel group, 224
- description of common Spanning Tree functionality, 339
- description of Fastethernet [AX1250S] [AX1240S], 166
- description of Gigabitethernet (RJ45), 174, 186
- description of IGMP Snooping and MLD Snooping, 433
- description of L2 protocol frame transparency functionality, 286
- description of MAC address learning, 242
- description of MAC VLANs, 271
- description of Multiple Spanning Tree, 325
- description of PoE [AX2200S] [AX1240S], 197
- description of port VLANs, 261
- description of protocol VLANs, 265
- description of PVST+, 307
- description of RADIUS, 86
- description of Single Spanning Tree, 316
- description of the basic link aggregation functionality, 216
- description of the basic VLAN functionality, 252
- description of the DHCP snooping functionality, 404
- description of the inter-port relay blocking functionality, 288
- description of the link aggregation extended functionality, 226
- description of the power saving functionality, 124
- description of the Ring Protocol, 351
- designing networks for Multiple Spanning Tree, 327
- designing Spanning Tree topologies, 300
- Device Management, 107
- DHCP snooping, 403
- DHCP snooping operation, 429
- displaying and checking configuration entries (show command), 67
- displaying and stopping display of the operation log on the monitor, 112
- displaying link aggregation information, 230
- displaying the effective RADIUS server information, 97
- displaying the LED behavior, 147
- displaying the NTP client information, 105
- displaying the operating status of the schedule, 148
- displaying the status of cooling fan control [AX1240S], 147
- displaying the status of port power saving control, 147
- distinguishing protocols, 265
- ending configuration editing (exit command), 71
- dynamic ARP inspection functionality, 412

**E**

Entry-error detection functionality, 51  
 error locations and recovery processing, 121  
 Ethernet, 153, 464  
     configurations common to all interfaces, 159  
     information common to all interfaces, 154  
     operations common to all interfaces, 165  
 extended VLAN functionality, 285

**F**

fault monitoring methods, 358  
 faults and restoration other than for shared links  
     in a shared link monitoring ring, 369  
 features of the Switch, 3  
 flow control settings, 162, 173, 184, 196  
 flow of Ring Protocol settings, 386  
 forwarding DHCP packets with Option 82, 411, 415  
 functionality supported for IGMP snooping and MLD snooping, 436  
 functions that use system function resources  
     [AX1250S] [AX1240S], 112

**G**

GSRP  
     using with the Ring Protocol, 397

**H**

hardware, 12  
 history functionality, 52

**I**

IGMP querier functionality, 438  
 IGMP snooping, 437  
     MAC address control method, 437  
     notes on usage, 443  
     overview, 434  
 IGMP snooping and MLD snooping, 466  
 IGMP snooping operation, 450  
 information common to all Ethernet interfaces, 154  
 IPv4 interfaces, 457  
 IPv5 interface, 466

**K**

Keyboard command functionality, 53

**L**

L2 protocol frame transparency functionality  
     configuring, 287  
 Layer 2 switching  
     overview, 233  
 Layer 2 switching by MAC address, 242  
 Layer 2 Switching overview, 233  
 LED behavior, 125  
 LED behavior setting, 144

limiting the rate of DHCP packet reception, 411  
 line and module capacities, 20  
 link aggregation, 215, 465  
 link aggregation configuration, 216  
 linkage with the Layer 2 authentication  
     functionality, 272  
 list of configuration commands, 77, 93, 103, 143, 159, 209, 219, 228, 246, 258, 262, 267, 275, 287, 290, 304, 310, 318, 331, 345, 386, 419, 448, 452, 459  
 list of operation commands, 48, 79, 97, 105, 113, 147, 150, 165, 230, 248, 281, 292, 315, 323, 337, 349, 395, 429, 450, 454, 460  
 lists of configuration commands and operation commands, 66, 82, 108  
 logging in  
     procedures, 39  
 login and logout, 45  
 login security and RADIUS, 81  
 Loop guard, 340

**M**

MAC address control method, 437, 440  
 MAC address learning, 234, 241, 246  
 MAC address learning configuration, 246  
 MAC address learning operation, 248  
 MAC address of the channel group, 217  
 MAC address of the Switch, 156  
 maximum number of concurrent users  
     setting, 84  
 maximum number of lines, 20  
 MLD querier functionality, 442  
 MLD snooping, 440  
     MAC address control method, 440  
     notes on usage, 443  
     overview, 434  
 MLD snooping operation, 454  
 mode transitions when entering configuration commands, 64  
 monitoring DHCP packets, 406  
 multi-fault monitoring functionality for the Ring Protocol, 372

**N**

native VLANs for protocol ports, 266  
 network configuration, 356  
 network configuration example, 154  
 normal ring operation, 359, 363  
 note on changing the time, 102  
 notes common to Spanning Tree Protocols, 303  
 notes on applying a backup configuration file, 74  
 notes on CLI operation, 55  
 notes on configuration editing, 71  
 notes on IGMP snooping and MLD snooping usage, 443  
 notes on Multiple Spanning Tree usage, 330  
 notes on PoE usage, 207  
 notes on PVST+ usage, 309

- notes on regarding port VLAN usage, 261
- notes on Ring Protocol usage, 382
- notes on Single Spanning Tree usage, 317
- notes on updating the software, 151
- notes on using DHCP snooping, 417
- notes on using link aggregation, 217
- notes on using SFP, 193
- notes on using the inter-port relay blocking functionality, 288
- notes on VLAN usage, 257
- notes when the power saving functionality is used, 141
- NTP, 464

## O

- operation during multi-fault recovery, 377
- operation for common Spanning Tree functionality, 349
- operation for faults and restoration other than for shared links in a shared link non-monitoring ring, 367
- operation for link aggregation, 230
- operation for Multiple Spanning Tree, 337
- operation for shared link faults and restoration, 365
- operation for Single Spanning Tree, 323
- operation for the VLAN extended functionality, 292
- operation of PoE [AX2200S] [AX1240S], 212
- operation terminals, 40
- operation when a fault is detected, 359
- operation when multi-faults occur, 374
- operation when recovery is detected, 361
- operational overview, 400
- operations common to all Ethernet interfaces, 165
- optional functionality of MAC ports, 273
- order of Ethernet frames, 157
- overview of editing a running configuration, 63
- overview of IGMP snooping and MLD snooping, 434
- overview of login control, 82
- overview of multicast, 434
- overview of multi-ring operation, 363
- overview of operation for multi-fault monitoring, 373
- overview of operation management functionality, 42
- overview of PoE, 197
- overview of RADIUS, 86
- overview of single ring operation, 359
- overview of Spanning Tree Protocols, 296
- overview of the Ring Protocol, 352
- overview of the Switch, 1, 2

## P

- paging, 53
- permitting login by using FTP, 78
- permitting login by using the Telnet protocol, 78

- permitting login from a remote operation terminal, 83
- physical interfaces, 154
- port allocation for sending frames, 217
- port power saving, 132
- port VLANs
  - configuring, 262
- power control configuration, 143
- power control operation, 147
- power saving functionality, 123
- power saving scheduling, 134
- prohibited configurations for the multi-fault monitoring functionality, 381
- prohibited Ring Protocol configurations, 381
- protocol ports and trunk ports, 266
- PVST + operation, 315
- PVST+
  - description, 307
- PVST+ configuration, 310
- PVST+ for access ports, 307

## R

- RADIUS, 464
- RADIUS operations, 97
- range of Switch models, 8
- registering static entries, 242
- regularly obtaining time information from the NTP server, 104
- relevant standards, 464
- remote login, 75
- remote terminal
  - verifying communication between the Switch, 79
- restricting login from remote operation terminals, 84
- resuming and stopping power supply, and the port status, 204
- Ring Protocol
  - using with GSRP, 397
  - using with Spanning Tree Protocols, 397
- ring protocol network design, 380
- Root guard, 343

## S

- saving a binding database, 415
- saving to the configuration file, 70
- setting
  - maximum number of concurrent users, 84
- setting 100BASE-FX ports [AX1250S], 195
- setting a 1000BASE-X port, 195
- setting and checking the time, 100
- setting authentication methods, 93
- setting behavior of when the maximum power supply is exceeded, 201
- setting BPDU filters, 346
- setting control VLANs, 387
- setting cooling fan control (Semi-fanless operation) [AX1240S], 144
- setting Ethernet interface ports [AX1250S]



- [AX1240S], 160
- setting Ethernet interface ports [AX2200S], 160
- setting forwarding of tagged frames on a MAC port, 278
- setting how to save the binding database, 427
- setting login security, 82
- setting port priority, 210
- setting PortFast, 345
- setting power saving based on scheduling, 145
- setting power saving for ports in link-down status, 144
- setting root guards, 347
- setting so that priority is given to powered ports, 210
- setting static routes, 459
- setting the aging time, 246
- setting the dynamic ARP inspection functionality, 425
- setting the link-down detection timer, 161
- setting the maximum amount of power that can be supplied for system 1 [AX2200S], 209
- setting the media type [AX1250S] [AX1240S], 184, 196
- setting the multi-fault monitoring functionality, 393
- setting the password for switching to administrator mode, 83
- setting the rate of DHCP packet reception, 425
- setting the source IP address of an MLD Query message, 453
- setting the system clock, 103
- setting trunk ports, 259
- setting various parameters, 393
- setting VLAN mappings, 388
- settings and operation for IGMP Snooping and MLD Snooping, 447
- settings and operation for the Ring Protocol, 385
- settings for modes and ring ports (for single rings and multi-ring configurations without shared links), 389
- settings related to status display and system operation, 108
- shutting down a port, 161
- single ring operation
  - overview, 359
- sleep mode [AX1250S] [AX1240S], 133
- software, 17
- software Management, 149
- software update, 151
- source MAC address learning, 242
- Spanning Tree Protocol, 295, 465
- Spanning Tree Protocols
  - using with the Ring Protocol, 397
- Spanning Tree Protocols and rapid Spanning Tree Protocols, 297
- standby link functionality, 226
- starting a switch, 44

- starting configuration editing (configure command and configure terminal command), 67
- starting the switch, 43
- STP compatibility mode, 301
- supported functionality, 124
- supported functions, 235
- supported specifications, 100, 216, 355
- Switch
  - assigning IP address to, 77
  - components, 12
  - configuration, 7
  - verifying communication between a remote terminal, 79
- switch components, 12
- switch configuration, 7
- switching communication paths, 358

## T

- target information to be backed up and restored, 113
- TELNET/FTP, 464
- terminal filtering, 409
- terminal-based management, 40
- time settings and NTP, 99
- transferring files using a memory card, 73
- transferring files using FTP, 72
- types of Spanning Tree Protocols, 296

## U

- using forwarding-delay-time for control VLANs, 380
- using jumbo frames, 163, 173, 184, 196
- using PVST+ to balance load, 307
- using the Ring Protocol with GSRP, 400
- using the Ring Protocol with Spanning Tree Protocols, 398
- using the Ring Protocol with Spanning Tree Protocols/GSRP, 397
- using VLAN mappings, 380

## V

- verifying
  - communication between a remote terminal and the Switch, 79
- viewing logged data, 112
- VLAN, 234, 251, 465
- VLAN operation, 281

## W

- when connecting a DHCP relay agent to the Switch, 423
- workflow from starting to stopping the Switch, 43