AX2200S / AX1250S / AX1240S Software Manual

Message and Log Reference

For Version 2.4

AX1240S-S005X-60

■ **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 manual 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-S005X-60

■ **Copyright**

■ **History of Amendments**

Ver. 2.4 (Edition 7)

Summary of amendments

Location and title	Changes
Addition of series	● A description for the AX2200S was added.
2.5.4 Event location = POE [AX2200S] [AX1240S]	● An INFO message (item number 3) was added. ● A FATAL message (item number 1) was added. The subsequent item numbers in the table changed accordingly.
2.6.5 Event location = FAN [AX2200S] [AX1240S]	● An ERROR message (item number 1) was added. The subsequent item numbers in the table changed accordingly.

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

Ver. 2.3 (Edition 6)

Summary of amendments

Location and title	Changes
Event location = VLAN (Ring Protocol)	● Two INFO messages (item numbers 3 to 4) were added.

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

Ver. 2.3 (Edition 5)

Summary of amendments

Location and title	Changes
Event location = THERMO	● Four INFO messages (item numbers 2 to 5) were added.
Event location = SVP	● An INFO message (item number 3) has been added.

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

Ver. 2.2 (Edition 4)

Summary of amendments

Location and title	Changes
Addition of series	● A description for the AX1250S was added.
Event location = SFP	● An INFO message (item number 10) has been added. The subsequent item numbers in the table changed accordingly.
Event location = PCI	● This subsection was added.
Event location = RAM	● This subsection was added.
Event location = CPU	● This subsection was added.

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

Ver. 2.2 (Edition 3)

Summary of amendments

Location and title	Changes
Event location = VLAN (Ring Protocol)	● This subsection was added.
Event location = VLAN (CFM)	● This subsection was added.
Event location = IP	● This subsection was added.
Event location = RADIUS	● The descriptions of eight `INFO` messages (item numbers 1, 3, 5, 7, 9, 11, 13, and 15) were changed. ● Ten `INFO` messages related to the RADIUS server for authentication or the RADIUS server group (item numbers 2, 4, 6, 8,

Location and title	Changes
	10, 12, 14, 16, 17 and 18) were added. The subsequent item numbers in the table changed accordingly.
Event location = CERTIF	● WARN information was added.
Event location = FABRIC	● INFO information was added. ● Three CRITC messages (item numbers 3 to 5) were added. ● Three FATAL messages (item numbers 5 to 7) were added.
Event location = ROM	● Two ERROR messages (item numbers 3 to 4) were added. The subsequent item numbers in the table changed accordingly.
Event location = THERMO	● The event level of the Accumulation operation time was initialized message was changed from ERROR to WARN.

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

Ver. 2.1 (Edition 2)

Summary of amendments

Location and title	Changes
Event location = SESSION	● The description of the INFO message (item number 16) during local login authentication was changed. ● An INFO message (item number 17) during local login authentication was added.
Event location = VLAN	● Two INFO messages related to automatic VLAN allocation (item numbers 7 and 8) were added. The subsequent item numbers in the table changed accordingly.
Event location = KERNEL	● INFO information was added.
Event location = RADIUS	● Six INFO messages related to the RADIUS server for authentications (item numbers 3 to 8) were added.
Event location = ECO	● This subsection was added.
Event location = PORT	● Event message (Ref. Code = 1e145000) was added.
Event location = ULR	● Two INFO messages related to the MAC address updating functionality (item numbers 17 and 18) were added.
Event location = FAN	● Two INFO messages related to fan behavior through temperature monitoring (item numbers 2 and 3) were added.
Event location = SVP	● This subsection was added.
Event location = PWRSUP	● This subsection was added.

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

Preface

Applicable products and software versions

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

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

Unless otherwise noted, this manual describes functionality applicable to AX2200S, AX1250S, and AX1240S series switches. Functionality specific to a model is indicated as follows:

[*AX2200S*]:

The description applies to the AX2200S switch.

[*AX1250S*]:

The description applies to the AX1250S switch.

[*AX1240S*]:

The description applies to the AX1240S switch.

In addition, unless otherwise noted, this manual describes the functionality applicable to both OS-LT4, OS-LT3, and OS-LT2. The functionality supported by option 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

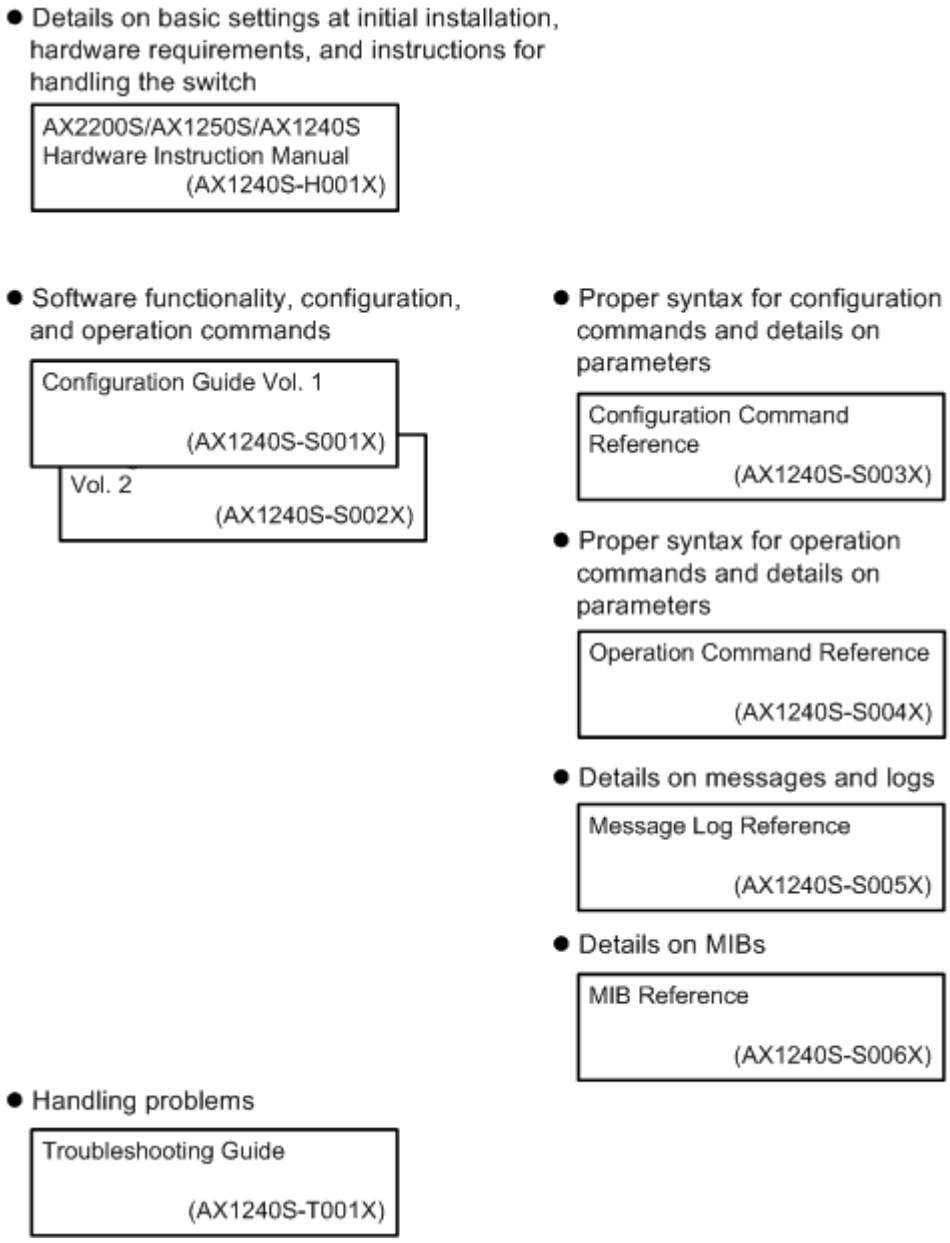
Manual URL

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.



Abbreviations used in the manual

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	Bits per second (can also appear as bps)
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface

CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU

LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations, Administration, and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	packets per second (can also appear as pps)
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PoE	Power over Ethernet
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
QoS	Quality of Service
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 1024^2 bytes.1 GB (gigabyte) is 1024^3 bytes.1 TB (terabyte) is 1024^4 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

1. Operation Log and Switch Failure Log

This chapter explains the operation log and switch failure log, which are used in the event of a failure to identify where errors have occurred.

1.1 Characteristics of the operation log and switch failure log

The Switch outputs information to be reported to the administrator, such as activity status and failure information, to an operation terminal as operation logs or switch failure logs. Switch failure logs are also stored internally.

The following table describes the characteristics of the operation log and Switch failure log.

Table 1-1 Characteristics of the operation log and error log information

Item	Operation log	Switch failure log
Description	Acquires the following information in chronological order	Records the times that events occur, from the oldest to newest.
Maintenance information that is to be acquired	Entered commands Command response messages Switch failure and event information	Switch failure information
Number of acquisitions	A total of 512 event entries can be acquired.	A total of 127 entries can be acquired.
Processing when the number of acquisitions is exceeded	If the number of acquired entries exceeds 512, the oldest event is deleted and a new event is added.	If the number of log entries exceeds 127, newly acquired logs are discarded.

1.1.1 Format of messages

(1) Format of operation logs

The figure below describes the format of the operation log.

Figure 1-1 Format of operation logs

```
EVT  LEVEL yy/mm/dd hh:mm:ss  TASK    Message
 1     2          3            4        5
```

1. Event type: Displays a three-letter identification code
2. Event level
3. Time: Displays the date and time when the event indicated in the message occurred
4. Event location or function
5. Message text

Code information such as the event level and the event location or functionality included in the message is the same as the Switch failure log. For details, see *1.1.2 Code information for operation logs and Switch failure logs*.

(2) Format of Switch failure logs

The figure below describes the format of Switch failure logs.

Figure 1-2 Format of a Switch failure log

```
*** Detailed Log Display : Recode Num.=ccc : Ref-Code = xxxxxxxx ***
                                  1                  2
  Time Stamp = yyyy/mm/dd-hh:mm:ss : SysUpTime = dday-hh:mm:ss#
                       3                     4
 *** Log Text Data ***
```

```
  (Additional information for the log: text data) 5
*** Log Binary Data ***
  (Additional information for the log: binary data) 6
```

1. Log record number
2. Switch failure log code (reference code)
3. Time: Displays the date and time when the log was acquired
4. Displays the time elapsed since the Switch started
5. Additional information for the log (text data)
6. Additional information for the log (binary data)

The elapsed time is displayed as follows:

If the elapsed time is 24 hours or less: *hh*:*mm*:*ss* (*hh* = hours, *mm* = minutes, *ss* = seconds)

If the elapsed time is more than 24 hours: *d*day-*hh*:*mm*:*ss* (*d* = number of days, *hh* = hours, *mm* = minutes, *ss* = seconds)

1.1.2 Code information for operation logs and Switch failure logs

(1) Event type

The following event log types are given to the operation log entries:

- Command operation by user and the operation's result
- Operation information output by the switch
- Error information

The table below describes the correspondence between the information acquired as operation logs and event types. Within the operation logs, an event level is assigned to Switch failure information and event information.

Table 1-2 Correspondence between event types and event levels

Information to be acquired	Event Type	Description	Event Level
Entered commands	KEY	Commands entered by an operator from an operation terminal	--
Command response messages	RSP	Messages output by Switches to respond to entered commands	--
Switch failure and event information	ERR	Error information for a Switch event location	FATAL CRITC ERROR
	EVT	Event information for a Switch event location	WARN INFO

Legend --: Not applicable

(2) Event level

Switch failure and event information is classified into five levels depending on severity. The following table describes the event levels and their contents.

Table 1-3 Event levels and their contents

Event Level	Switch failure log	Display contents (type)	Description
1	Yes	FATAL (fatal error)	This error stops the whole system. (The system might restart or operation might stop.)
2	Yes	CRITC (critical error)	This failure stops part of the Switch. ● If this error is due to a hardware error, restarting the applicable hardware is involved.
3	Yes	ERROR (software error)	This error stops part of the software.
4	No	WARN (warning)	Warning information
5	--	--	Not used
6	No	INFO (information)	Event information related to operation

Legend

Yes: Messages are displayed, or Switch failure log data is acquired.

No: Messages are displayed, but Switch failure log data is not acquired.

--: Not applicable.

(3) Event location

The location or functionality of the event that occurred is indicated by the ID.

Table 1-4 Event location

ID	Event location or functionality
CONSOLE	Console operation
SESSION	Login or logout operation for Telnet, the console, or FTP
TELNETC	Login or logout operation by a Telnet client
STP	Spanning tree functionality
GSRP	GSRP aware functionality
VLAN	VLAN control functionality
VLAN (Ring Protocol)	Ring Protocol functionality
VLAN (CFM)	Connectivity Fault Management functionality
SNOOP	IGMP/MLD snooping functionality
DHCP	Web authentication DHCP server functionality
LINKAGG	Link aggregation functionality

ID	Event location or functionality
DHCPSN	DHCP snooping functionality
IP	IP control functionality
KERNEL	Software controller
NTP	NTP client functionality
802.1X	IEEE 802.1X authentication functionality
RADIUS	RADIUS authentication functionality
CERTIF	MAC or Web authentication functionality
HTTPD	Web authentication functionality (web server)
QOS	QoS or transmission control functionality
FIELD	Filter functionality
SWOL	Secure wake on LAN functionality
ECO	Power-saving functionality
PORT	Port control functionality
SFP	SFP module control functionality
FABRIC	Switching driver controller
POE [AX2200S] [AX1240S]	PoE controller
ULR	Uplink redundancy functionality
ROM	ROM diagnosis
RTC	RTC functionality
THERMO	Temperature sensor functionality
SDCARD	SD card control functionality
FAN [AX2200S] [AX1240S]	Fan control functionality
LED	LED functionality
SVP	Service processor monitoring functionality
PWRSUP	Power supply controller
PCI	PCI bus controller
RAM	RAM diagnosis

ID	Event location or functionality
CPU	CPU (internal memory controller)

(4) Interface ID

This ID indicates the location of the interface where the event occurred. The following table describes the display formats of the interface IDs for the Switch.

Table 1-5 Display format of the interface ID

Display format of the ID	Interface
FastEthernet *<IF#>*	10BASE-T or 100BASE-TX interface
GigabitEthernet *<IF#>*	10BASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X interface [AX2200S]
	1000BASE-T, 100BASE-FX, or 1000BASE-X interface [AX1250S]
	10BASE-T or 100BASE-X interface [AX1240S]

Legend

<IF#>: Interface port number (example: `FastEthernet 0/1`)

1.2 How to read the tables in this manual

This manual uses the format shown in the table below for the descriptions in *2. Switch Failure and Event* Information.

Table 1-6 How to read the tables

No.	Event Level	Event location	Ref. Code	Message text
	Description			
1	INFO WARN ERROR CRITC FATAL#	Event location as shown in *Table 1-4*.	This item is written only for the Switch failure log shown in *Table 1-3*.	*Message*
	Meaning of the message [Action] If there is an action that can be taken, the action is described. If you do not need to take any action or if there is no action that can be taken, *None* is written.			

The `show logging` operation command cannot be used to display information in which the event level is `FATAL`.

1. Operation Log and Switch Failure Log

2. Switch Failure and Event Information

This chapter describes the contents of switch failure and event information. All messages for switch failure and event information are output to the operation terminal window. Depending on the error severity and the event contents, messages are categorized into five levels, called *event levels*.

2.1 Configuration

2.1.1 Event location = CONSOLE

The following tables describe Switch failure and event information when the event location is `CONSOLE`.

- `INFO` information

Table 2-1 Switch INFO information when the event location is CONSOLE

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	CONSOLE		Line:*<line>* Command error (No in configure mode) : [*<input command>*]
	A command entry error occurred on line *<line-number>* because the *<entered-command>* command was not a configuration command. [Action] None			
2	INFO	CONSOLE		Line:*<line>* Command error : [*<input command>*]
	A command entry error occurred due to the *<entered-command>* command on line *<line>*. [Action] Enter valid settings on the target line in the configuration displayed by executing the `show startup-config` operation command.			
3	INFO	CONSOLE		Cannot read a startup-config file
	A startup configuration file could not be read. [Action] ● The startup configuration file might have been deleted by the `erase startup-config operation` command. Reconfigure the startup configuration by using configuration commands, save the configuration into the startup configuration file, and then restart the Switch. ● The startup configuration file in the internal flash memory might be corrupted. After deleting the startup configuration file by using the `erase startup-config` operation command, reconfigure the startup configuration by using configuration commands, save the configuration into the startup configuration file, and then restart the Switch.			
4	INFO	CONSOLE		The configuration file is empty.
	The startup configuration file was empty. [Action] Execute the `copy running-config startup-config` operation command to save the configuration file, and then restart the Switch.			

- `WARN` information

Table 2-2 Switch WARN information when the event location is CONSOLE

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	WARN	CONSOLE		Cannot execute config command
	The `show running-config` operation command could not be executed. [Action] None			

- `CRITC` information

Table 2-3 Switch CRITC information when the event location is CONSOLE

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	CRITC	CONSOLE	18200001	Software error
	The semaphore ID processing failed during initialization when the Switch started. [Action] Use the `reload` operation command to restart the Switch.			

2.2 Login

2.2.1 Event location = SESSION

The following tables describe Switch failure and event information when the event location is SESSION.

- INFO information

Table 2-4 Switch INFO information when the event location is SESSION

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	SESSION		Login *xxxxxxxx* from console
	A user (*xxxxxxxx*) logged in via RS-232C (console). *xxxxxxxx*: User name [Action] None			
2	INFO	SESSION		Logout *xxxxxxxx* from console
	An RS-232C (console) user (*xxxxxxxx*) logged out. *xxxxxxxx*: User name [Action] None			
3	INFO	SESSION		Login *xxxxxxxx* from *x.x.x.x* (vty0)
	A user (*xxxxxxxx* from *x.x.x.x*) logged in via Telnet (vty0). *xxxxxxxx*: User name from *x.x.x.x*: Remote login user's IP address [Action] None			
4	INFO	SESSION		Logout *xxxxxxxx* from *x.x.x.x* (vty0)
	A Telnet (vty0) user (*xxxxxxxx* from *x.x.x.x*) was logged out. *xxxxxxxx*: User name from *x.x.x.x*: Remote login user's IP address [Action] None			
5	INFO	SESSION		Login *xxxxxxxx* from *x.x.x.x* (vty1)
	A user (*xxxxxxxx* from *x.x.x.x*) logged in via Telnet (vty1) after already logging in via Telnet. *xxxxxxxx*: User name from *x.x.x.x*: Remote login user's IP address [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
6	INFO	SESSION		Logout *xxxxxxxx* from *x.x.x.x* (vty1)
	A user (*xxxxxxxx* from *x.x.x.x*) logged out via Telnet (vty1) after logging in via Telnet. *xxxxxxxx*: User name from *x.x.x.x*: Remote login user's IP address [Action] None			
7	INFO	SESSION		Login *xxxxxxxx* from *x.x.x.x* (ftp)
	A user (*xxxxxxxx* from *x.x.x.x*) logged in via FTP. *xxxxxxxx*: User name from *x.x.x.x*: Remote login user's IP address [Action] None			
8	INFO	SESSION		Logout *xxxxxxxx* from *x.x.x.x* (ftp)
	An FTP user (*xxxxxxxx* from *x.x.x.x*) logged out. *xxxxxxxx*: User name from *x.x.x.x*: Remote login user's IP address [Action] None			
9	INFO	SESSION		Login incorrect *xxxxxxxx*
	A login attempt has failed. *xxxxxxxx*: User name [Action] None			
10	INFO	SESSION		Authentication login *xxxxxxxx* RADIUS server configuration is not defined.
	A RADIUS server has not been set for RADIUS authentication. *xxxxxxxx*: user name [Action] Configure the RADIUS server for RADIUS authentication.			
11	INFO	SESSION		Authentication login *xxxxxxxx* RADIUS accept
	RADIUS authentication succeeded. *xxxxxxxx*: User name [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
12	INFO	SESSION		Authentication login *xxxxxxxx* RADIUS reject
	RADIUS authentication failed *xxxxxxxx*: User name [Action] None			
13	INFO	SESSION		Authentication login *xxxxxxxx* RADIUS no response
	During RADIUS authentication, the RADIUS server did not respond. *xxxxxxxx*: User name [Action] None			
14	INFO	SESSION		Authentication login *xxxxxxxx* RADIUS over request
	During RADIUS authentication, the maximum number (256) of simultaneous transmissions to the RADIUS server was exceeded. *xxxxxxxx*: User name [Action] None			
15	INFO	SESSION		Authentication login *xxxxxxxx* RADIUS UDP send error
	During RADIUS authentication, an attempt to send packets to the RADIUS server failed. *xxxxxxxx*: User name [Action] None			
16	INFO	SESSION		Unknown host address *x.x.x.x*
	An attempt to connect to the Switch via Telnet or FTP from *x.x.x.x* was not permitted. *x.x.x.x*: IP address used to connect via Telnet or FTP [Action] 1. Unauthorized access (access from a remote host not authorized in the configuration) to the Switch might have been attempted. Check the remote access permissions for *x.x.x.x*. 2. If remote access from *x.x.x.x* is permitted, the configuration might be incorrect. Check the configuration settings. 3. If you want to permit remote access from "*x.x.x.x*", configure the access permissions.			
17	INFO	SESSION		Login refused for too many users logged in
	An attempt to connect via Telnet or FTP was refused because too many users are logged in. [Action] 1. Check the number of users who are currently logged in. 2. If necessary, increase the limit for the number of users who can log in for the configuration.			

- WARN information

Table 2-5 Switch WARN information when the event location is SESSION

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	WARN	SESSION		Authentication login *xxxxxxxx* RADIUS invalid server specified
	An internal error occurred during RADIUS authentication. *xxxxxxxx*: User name [Action] None			
2	WARN	SESSION		Authentication login *xxxxxxxx* RADIUS return error
	An internal error occurred during RADIUS authentication. *xxxxxxxx*: User name [Action] None			
3	WARN	SESSION		Authentication login *xxxxxxxx* RADIUS msgid use over. use = *xx*
	An internal error (message queue error) occurred during RADIUS authentication. *xxxxxxxx*: User name use=*xx*: Used for analysis by the manufacturer [Action] None			
4	WARN	SESSION		Authentication login *xxxxxxxx* RADIUS message queue time out
	An internal error (message queue error) occurred during RADIUS authentication. *xxxxxxxx*: User name [Action] None			
5	WARN	SESSION		Authentication login *xxxxxxxx* RADIUS message queue error
	An internal error (message queue error response) occurred during RADIUS authentication. *xxxxxxxx*: User name [Action] None			

2.2.2 Event location = TELNETC

The following table describes Switch failure and event information when the event location is TELNETC.

- INFO information

Table 2-6 Switch INFO information when the event location is TELNETC

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	TELNETC		Socket open error
	A connection with the host failed. [Action] Log in again.			
2	INFO	TELNETC		Socket option set errors
	A connection with the host failed. [Action] Log in again.			
3	INFO	TELNETC		Connection time out
	A connection failed due to a timeout. [Action] Check whether the remote switch permits login via Telnet, and then log in again.			
4	INFO	TELNETC		Rejection echo option of server
	An echo request was rejected. [Action] None			
5	INFO	TELNETC		Rejection full duplex option of server
	A full-duplex communication request was rejected. [Action] None			
6	INFO	TELNETC		Close session *x.x.x.x* (Serial)
	An RS-232C (Serial) user forcibly closed a session. *x.x.x.x*: Remote user's IP address [Action] None			
7	INFO	TELNETC		Close session *x.x.x.x* (Telnet)
	A Telnet user forcibly closed a session. *x.x.x.x*: Remote user's IP address [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
8	INFO	TELNETC		Disconnected logout *x.x.x.x* (Serial)
	An RS-232C (Serial) user logged out normally from a Telnet client session. *x.x.x.x*: Remote user's IP address [Action] None			
9	INFO	TELNETC		Disconnected logout *x.x.x.x* (Telnet)
	A Telnet user logged out normally from a Telnet client session. *x.x.x.x*: Remote user's IP address [Action] None			
10	INFO	TELNETC		Disconnected *x.x.x.x* (Serial)
	A RS-232C (Serial) user closed a Telnet client session. *x.x.x.x*: Remote user's IP address [Action] None			
11	INFO	TELNETC		Disconnected *x.x.x.x* (Telnet)
	A Telnet user closed a Telnet client session. *x.x.x.x*: Remote user's IP address [Action] None			
12	INFO	TELNETC		Connected to *x.x.x.x* (Serial)
	An RS-232C (Serial) user connected normally to a Telnet client login. *x.x.x.x*: Remote user's IP address [Action] None			
13	INFO	TELNETC		Connected to *x.x.x.x* (Telnet)
	A Telnet user connected normally to a Telnet client login. *x.x.x.x*: Remote user's IP address [Action] None			

2.3 Protocol

2.3.1 Event location = STP

The following tables describe Switch failure and event information when the event location is STP.

- INFO information

Table 2-7 Switch INFO information when the event location is STP

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	STP		(*<mode>*) : Port status becomes Forwarding on the port(*<IF#>*)
	The port was placed in the Forwarding status. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● CIST: Multiple Spanning Tree (CIST) ● MST Instance *<MSTI ID>*: Multiple Spanning Tree (MSTI) and MST instance ID *<IF#>*: Interface port number [Action] None			
2	INFO	STP		(*<mode>*) : Port status becomes Blocking on the port(*<IF#>*)
	The port was placed in the Blocking status. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● CIST: Multiple spanning tree (CIST) ● MST Instance *<MSTI ID>*: Multiple Spanning Tree (MSTI) and MST instance ID *<IF#>*: Interface port number [Action] None			
3	INFO	STP		(*<mode>*) : Port status becomes Down- BPDU received on the BPDU GUARD port(*<IF#>*)
	A port was placed in the Down status because it was set with the BPDU guard function and received a BPDU. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● MST: Multiple Spanning Tree *<IF#>*: Interface port number [Action] Check the line status.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
4	INFO	STP		(*<mode>*) : Port status becomes Forwarding on the port (ChGr : *<Channel group#>*)
	The port was placed in the Forwarding status. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● CIST: Multiple spanning tree (CIST) ● MST Instance *<MSTI ID>*: Multiple Spanning Tree (MSTI) and MST instance ID *<Channel group#>*: Channel group number [Action] None			
5	INFO	STP		(*<mode>*) : Port status becomes Blocking on the port (ChGr:*<Channel group#>*)
	The port was placed in the Blocking status. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● MST Instance *<MSTI ID>*: Multiple Spanning Tree (MSTI) and MST instance ID *<Channel group#>*: Channel group number [Action] None			
6	INFO	STP		(*<mode>*) : Port status becomes Down- BPDU received on the BPDU GUARD port (ChGr:*<Channel group#>*)
	A port was placed in the Down status because it was set with the BPDU guard function and received a BPDU. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● MST: Multiple Spanning Tree *<Channel group#>*: Channel group number [Action] Check the line status.			
7	INFO	STP		(*<mode>*) : Port status becomes Blocking on the port(*<IF#>*), because IEEE802.1Q Tagged BPDU was received from a port that is not a trunk port
	Even though there was a setting (using an `Untagged` frame) for an access port, protocol port, or MAC port, the Switch received a BPDU with an IEEE802.1Q tag attached. Because of this, the port was placed in the Blocking status. *<mode>*: Spanning tree type ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID *<IF#>*: Interface port number [Action] Check the settings of the remote switch.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
8	INFO	STP		(*<mode>*) : Port status becomes Blocking on the port (ChGr:*<Channel group#>*), because IEEE802.1Q Tagged BPDU was received from a port that is not a trunk port
	Even though there was a setting (using an `Untagged` frame) for an access port, protocol port, or MAC port, the Switch received a BPDU with an IEEE802.1Q tag attached. Because of this, the port was placed in the Blocking status. *<mode>*: Spanning tree type ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID *<Channel group#>*: Channel group number [Action] Check the settings of the remote switch.			
9	INFO	STP		: Exceeded the number of the maximum spanning tree
	The number of trees has exceeded the maximum capacity of the Spanning Tree Protocol. No more trees can be added. [Action] Either review the network configuration or use a Single Spanning Tree or a Multiple Spanning Tree. If two or more VLANs are used, this log might be collected during startup, but no action is required if PVST+ is used.			
10	INFO	STP		(*<mode>*) : Port status becomes Blocking - BPDU in which priority is high was received on the ROOT GUARD port(*<IF#>*)
	A port was placed in the `Blocking` status because it was set with the `route-guard` function and received a high-priority BPDU. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● CIST: Multiple spanning tree (CIST) ● MST Instance *<MSTI ID>*: Multiple Spanning Tree (MSTI) and MST instance ID *<IF#>*: Interface port number [Action] Check the settings of the remote switch.			
11	INFO	STP		(*<mode>*) : Port status becomes Blocking - BPDU in which priority is high was received on the ROOT GUARD port (ChGr:*<Channel group#>*)
	A port was placed in the `Blocking` status because it was set with the `route-guard` function and received a high-priority BPDU. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● CIST: Multiple spanning tree (CIST) ● MST Instance *<MSTI ID>*: Multiple Spanning Tree (MSTI) and MST instance ID *<Channel group#>*: Channel group number [Action] Check the settings of the remote switch.			

- `WARN` information

Table 2-8 Switch WARN information when the event location is STP

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	WARN	STP		(*<mode>*) : This bridge becomes the Root Bridge.
	The Switch has become the root bridge. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID [Action] None			
2	WARN	STP		(*<mode>*) : This bridge becomes the Designated Bridge.
	The Switch has become the designated bridge. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID [Action] None			
3	WARN	STP		(*<mode>*) : Topology change detected - BPDU Timeout detected on the root port(*<IF#>*)
	A BPDU timeout was detected on the root port. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● CIST: Multiple spanning tree (CIST) ● MST Instance *<MSTI ID>*: Multiple Spanning Tree (MSTI) and MST instance ID *<IF#>*: Interface port number [Action] Check the line status.			
4	WARN	STP		(*<mode>*) : Topology change detected - Topology Change Notification BPDU received on the port(*<IF#>*)
	A topology change BPDU has been received. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● MST: Multiple Spanning Tree *<IF#>*: Interface port number [Action] Check the line status.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
5	WARN	STP		(*<mode>*) : Spanning Tree Protocol enabled - BPDU received on the Port Fast(*<IF#>*)
	A port has become subject to the Spanning Tree Protocol because the port was set with the `PortFast` function and received a BPDU. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● MST: Multiple Spanning Tree *<IF#>*: Interface port number [Action] Check the line status.			
6	WARN	STP		(*<mode>*) : Topology change detected - BPDU Timeout detected on the root port(ChGr:*<Channel group#>*)
	A BPDU timeout was detected on the root port. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● CIST: Multiple spanning tree (CIST) ● MST: Instance *<MSTI ID>*: Multiple Spanning Tree (MSTI) and MST instance ID *<Channel group#>*: Channel group number [Action] Check the line status.			
7	WARN	STP		(*<mode>*) : Topology change detected - Topology Change Notification BPDU received on the port(ChGr:*<Channel group#>*)
	A topology change BPDU has been received. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● MST: Multiple Spanning Tree *<Channel group#>*: Channel group number [Action] Check the line status.			
8	WARN	STP		(*<mode>*) : Spanning Tree Protocol enabled - BPDU received on the Port Fast(ChGr:*<Channel group#>*)
	A port has become subject to the Spanning Tree Protocol because the port was set with the `PortFast` function and received a BPDU. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● MST: Multiple Spanning Tree *<Channel group#>*: Channel group number [Action] Check the line status.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
9	WARN	STP		: Cleared MAC Address Table entry
	A MAC address table entry was cleared because a BPDU for topology change was received. [Action] None			
10	WARN	STP		(*<mode>*) : Topology change detected - BPDU Timeout detected on the alternate port(*<IF#>*)
	A BPDU timeout was detected on the alternate port. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● CIST: Multiple spanning tree (CIST) ● MST: Instance *<MSTI ID>*: Multiple Spanning Tree (MSTI) and MST instance ID *<IF#>*: Interface port number [Action] Check the line status.			
11	WARN	STP		(*<mode>*) : Topology change detected - BPDU Timeout detected on the backup port(*<IF#>*)
	A BPDU timeout was detected on the backup port. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● CIST: Multiple spanning tree (CIST) ● MST Instance *<MSTI ID>*: Multiple Spanning Tree (MSTI) and MST instance ID *<IF#>*: Interface port number [Action] Check the line status.			
12	WARN	STP		(*<mode>*) : Topology change detected - BPDU Timeout detected on the alternate port(ChGr:*<Channel group#>*)
	A BPDU timeout was detected on the alternate port. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● CIST: Multiple spanning tree (CIST) ● MST Instance *<MSTI ID>*: Multiple Spanning Tree (MSTI) and MST instance ID *<Channel group#>*: Channel group number [Action] Check the line status.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
13	WARN	STP		(*<mode>*) : Topology change detected - BPDU Timeout detected on the backup port(ChGr:*<Channel group#>*)
	A BPDU timeout was detected on the backup port. *<mode>*: Spanning tree type ● single: Single Spanning Tree ● PVST+: VLAN *<VLAN ID>*: PVST+ Spanning Tree Protocol and VLAN ID ● CIST: Multiple spanning tree (CIST) ● MST Instance *<MSTI ID>*: Multiple Spanning Tree (MSTI) and MST instance ID *<Channel group#>*: Channel group number [Action] Check the line status.			
14	WARN	STP		(MST) : This bridge becomes the CIST Root Bridge.
	The Switch has become the CIST root bridge. [Action] None			
15	WARN	STP		(CIST) : This bridge becomes the CIST Regional Root Bridge.
	The Switch has become the CIST regional root bridge. [Action] None			
16	WARN	STP		(MST Instance *<MSTI ID>*) : This bridge becomes the MSTI Regional Root Bridge.
	The Switch has become the MSTI regional root bridge. *<MSTI ID>*: MST instance ID [Action] None			
17	WARN	STP		(CIST) : This bridge becomes the CIST Regional Designated Bridge.
	The Switch has become the CIST regional designated bridge. [Action] None			
18	WARN	STP		(MST Instance *<MSTI ID>*) : This bridge becomes the MSTI Regional Designated Bridge.
	The Switch has become the MSTI regional designated bridge. *<MSTI ID>*: MST instance ID [Action] None			

- `CRITC` information

Table 2-9 Switch CRITC information when the event location is STP

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	CRITC	STP	01200000	*<comment>*
	An unexpected error occurred in the spanning tree. *<comment>*: Cause information (information for vendor analysis) [Action] None			

- `FATAL` information

Table 2-10 Switch FATAL information when the event location is STP

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	FATAL	STP	01100000	*<comment>*
	The Switch restarted to recover from an unexpected error such as a memory acquisition failure occurring in the spanning tree. *<comment>*: Cause information (information for vendor analysis) [Action] Either review the network configuration or use a Single Spanning Tree or a Multiple Spanning Tree.			

2.3.2 Event location = GSRP

The following table describes Switch failure and event information when the event location is GSRP.

- WARN information

Table 2-11 Switch WARN information when the event location is GSRP

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	WARN	GSRP		aware : MAC Address Table entry cleared, because GSRP flush request received on port *<IF#>*, GSRP *<GSRP ID>* VLAN group *<VLAN group ID>* Source MAC address *<MAC address>*
	The MAC address table was cleared because a GSRP flush request frame was received. *<IF#>*: Interface port number *<GSRP ID>*: GSRP group number (information related to the GSRP Switch that sent a GSRP flush request frame) *<VLAN group ID>*: VLAN group number (information related to the GSRP Switch that sent a GSRP flush request frame) *<MAC address>*: MAC address (information related to the GSRP Switch that sent a GSRP flush request frame) [Action] None			

2.3.3 Event location = VLAN

The following table describes switch failure and event information when the event location is VLAN.

- INFO information

Table 2-12 Switch INFO information when the event location is VLAN

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	VLAN		VLAN (*<VLAN ID>*) Status is Up.
	The VLAN status is Up. *<VLAN ID>*: VLAN ID [Action] None			
2	INFO	VLAN		VLAN (*<VLAN ID>*) Status is Down.
	The VLAN status is Down. *<VLAN ID>*: VLAN ID [Action] Check the status of each line that belongs to VLAN.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
3	INFO	VLAN		The MAC-VLAN MAC Address entry is changed from dynamic through the configuration.
	A dynamic MAC address entry of the MAC VLAN was replaced with an address specified by the `mac-address` configuration command because the dynamic MAC address entry was the same as the address specified by the `mac-address` configuration command. [Action] None			
4	INFO	VLAN		The MAC-VLAN MAC Address Configuration can't be registered in the hardware tables.
	An address entry specified by the MAC VLAN configuration command `mac-address` could not be set in the hardware table. [Action] Review the system configuration. However, a setting to the maximum of the capacity limit might not be available due to the limit of the hash method applied to the hardware.			
5	INFO	VLAN		The MAC-VLAN MAC Address entry can't be registered in the hardware tables.
	A dynamic MAC address entry of the MAC VLAN could not be set in the hardware table. [Action] Review the system configuration. However, a setting to the maximum of the capacity limit might not be available due to the limit of the hash method applied to the hardware.			
6	INFO	VLAN		L2TABLE : Optimize mode x ->> y
	As a hash entry overflow occurred due to a hash conflict in the MAC address table, the hash algorithm will be optimized or changed to avoid this. x: Hash algorithm mode value before the change y: Hash algorithm mode value after the change [Action] None			
7	INFO	VLAN		VLAN (*<VLAN ID>*) is auto-registered on the port(*<IF#>*)
	A VLAN was automatically registered on the port by automatic VLAN allocation. *<VLAN ID>*: VLAN ID *<IF#>*: Interface port number [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
8	INFO	VLAN		VLAN (<*VLAN ID*>) is auto-unregistered on the port(<*IF#*>)
	A VLAN was automatically removed from the port by automatic VLAN de-allocation. <*VLAN ID*>: VLAN ID <*IF#*>: Interface port number [Action] None			
9	INFO	VLAN		L2LD : Port(<*IF#*>) inactivated because of loop detection from port(<*IF#*>)
	The active port has been blocked because a loop failure was detected. <*IF#*>: Interface port number [Action] Check the network configuration.			
10	INFO	VLAN		L2LD : Port(<*IF#*>) inactivated because of loop detection from ChGr(<*Channel group#*>)
	The active port has been blocked because a loop failure was detected. <*IF#*>: Interface port number <*Channel group#*>: Channel group number [Action] Check the network configuration.			
11	INFO	VLAN		L2LD : ChGr(<*Channel group#*>) inactivated because of loop detection from port(<*IF#*>)
	The active port has been blocked because a loop failure was detected. <*Channel group#*>: Channel group number <*IF#*>: Interface port number [Action] Check the network configuration.			
12	INFO	VLAN		L2LD : ChGr(<*Channel group#*>) inactivated because of loop detection from ChGr(<*Channel group#*>)
	The active port has been blocked because a loop failure was detected. <*Channel group#*>: Channel group number [Action] Check the network configuration.			
13	INFO	VLAN		L2LD : Port(<*IF#*>) loop detection from port (<*IF#*>)
	A loop failure was detected. <*IF#*>: Interface port number [Action] Check the network configuration.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
14	INFO	VLAN		L2LD : Port(*<IF#>*) loop detection from ChGr(*<Channel group#>*)
	A loop failure was detected. *<IF#>*: Interface port number *<Channel group#>*: Channel group number [Action] Check the network configuration.			
15	INFO	VLAN		L2LD : ChGr(*<Channel group#>*) loop detection from port (*<IF#>*)
	A loop failure was detected. *<Channel group#>*: Channel group number *<IF#>*: Interface port number [Action] Check the network configuration.			
16	INFO	VLAN		L2LD : ChGr(*<Channel group#>*) loop detection from ChGr(*<Channel group#>*)
	A loop failure was detected. *<Channel group#>*: Channel group number [Action] Check the network configuration.			
17	INFO	VLAN		L2LD : ChGr(*<Channel group#>*) activate by automatic restoration of the L2loop detection function
	A port will be unblocked by the automatic restoration of the L2 loop detection functionality. *<Channel group#>*: Channel group number [Action] None			
18	INFO	VLAN		L2LD : Port(*<IF#>*) activate by automatic restoration of the L2loop detection function
	A port will be unblocked by the automatic restoration of the L2 loop detection functionality. *<IF#>*: Interface port number [Action] None			
19	INFO	VLAN		L2LD : L2loop detection frame cannot be sent in the port where capacity was exceeded
	The number of ports that can send L2 loop detection frames exceeds the capacity limit. Ports exceeding the capacity limit cannot send L2 loop detection frames. [Action] Decrease the number of ports sending L2 loop detection frames. If many VLANs are used, this log might be collected during switch startup. However, there is no problem if the `show loop detection` operation command does not show that the configuration value exceeds the capacity value.			

- WARN information

Table 2-13 Switch WARN information when the event location is VLAN

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	WARN	VLAN		L2TABLE : Cannot optimize mode (config)
	A hash entry overflow occurred because a hash conflict occurred in the MAC address table. However, this cannot be avoided because the hash algorithm mode has been fixed by a configuration command. [Action] To avoid a hash conflict, set `auto` in the `system l2-table mode` configuration command to change the hash algorithm mode to auto selection mode.			
2	WARN	VLAN		L2TABLE : Cannot optimize mode (not found)
	A hash entry overflow occurred because a hash conflict occurred in the MAC address table. However, this cannot be avoided because the hash entry overflow occurs even if the hash algorithm mode is optimized or changed. [Action] Review the system configuration.			
3	WARN	VLAN		L2TABLE : Cannot optimize mode (error)
	A hash entry overflow occurred because a hash conflict occurred in the MAC address table. However, this cannot be avoided because the hash algorithm mode cannot be optimized due to the system being unable to reserve memory. [Action] Review the system configuration.			

- FATAL information

Table 2-14 Switch FATAL information when the event location is VLAN

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	FATAL	VLAN	07100201	L2LD : SendTask process VLANCallBackSetErr[*xx*]
	An error occurred when the `VLANCALLBACK` function was registered. *xx*: Cause code (information for vendor analysis) [Action] Replace the Switch.			

2.3.4 Event location = VLAN (Ring Protocol)

The following table describes switch failure and event information when the event location is `VLAN (Ring Protocol)`.

- `INFO` information

Table 2-15 Switch INFO information when the event location is VLAN (Ring Protocol)

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	VLAN		AXRP *<Ring ID>* : cleared MAC address table by receiving flush request frames
	A flush control frame was received, and the MAC address table was cleared. The Switch outputs this message when it clears a MAC address table in which the output target is a ring port. *<Ring ID>*: Ring ID [Action] None.			
2	INFO	VLAN		AXRP *<Ring ID>* : cleared MAC address table by timeout of forwarding-shift-timer
	A MAC address table was cleared due to a `forwarding-shift-time` timeout. The Switch outputs this message when a `forwarding-shift-time` timeout is detected and the MAC address table is cleared. *<Ring ID>*: Ring ID [Action] None			
3	INFO	VLAN		AXRP (virtual-link *<Link ID>*) : cleared MAC address table by receiving flush frames
	A virtual link flush control frame was received by using the `Ring Protocol`, and MAC address table entries were cleared. The Switch outputs this message when the MAC address table entries learned on all ring ports are cleared. *<Link ID>*: Virtual link ID [Action] None			
4	INFO	VLAN		AXRP (multi-fault-detection *<Ring ID>*) : cleared MAC address table by receiving flush frames
	A multi-fault flush control frame was received, and the MAC address table was cleared. The Switch outputs this message when it clears the MAC address table of a ring port that supports a ring ID that applies multi-fault monitoring. *<Ring ID>*: Ring ID [Action] None			

- `FATAL` information

Table 2-16 Switch FATAL information when the event location is VLAN (Ring Protocol)

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	FATAL	VLAN	07100701	Swd Configuration Error *<comment>*
	The Ring Protocol configuration could not be set for the hardware controller. *<comment>*: Cause code (information for vendor analysis) [Action] None (The Switch automatically restarts.)			

2.3.5 Event location = VLAN (CFM)

The following table describes switch failure and event information when the event location is `VLAN (CFM)`.

- `INFO` information

Table 2-17 Switch INFO information when the event location is VLAN (CFM)

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	VLAN		MD Level *<Level>* MA *<No.>*: detected on fault of OtherCCM in MEP *<MEPID>*
	The relevant MEP detected a fault (OtherCCM). *<Level>*: Domain level *<No.>*: MA identification number *<MEPID>*: MEP ID [Action] A partner switch is not recognized as the same MA. Check that the domain level, MA ID, domain name, and MA name match the partner switches.			
2	INFO	VLAN		MD Level *<Level>* MA *<No.>*: detected on fault of ErrorCCM in MEP *<MEPID>*
	The relevant MEP detected a fault (ErrorCCM). *<Level>*: Domain level *<No.>*: MA identification number *<MEPID>*: MEP ID [Action] A partner switch and the configuration do not match. Check whether the MEP ID is different from the partner switch, and make sure the send interval (`interval`) matches that of the partner switch.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
3	INFO	VLAN		MD Level *<Level>* MA *<No.>*: detected on fault of Timeout in MEP *<MEPID>*
	The relevant MEP detected a fault (Timeout). *<Level>*: Domain level *<No.>*: MA identification number *<MEPID>*: MEP ID [Action] The Switch is not receiving CCM from partner switches. Check the network status.			
4	INFO	VLAN		MD Level *<Level>* MA *<No.>*: detected on fault of PortState in MEP *<MEPID>*
	The relevant MEP detected a fault (PortState). *<Level>*: Domain level *<No.>*: MA identification number *<MEPID>*: MEP ID [Action] A partner switch line fault or a port blocking status was detected. Check the status of the partner switch.			
5	INFO	VLAN		MD Level *<Level>* MA *<No.>*: detected on fault of RDI in MEP *<MEPID>*
	The relevant MEP detected a fault (RDI). *<Level>*: Domain level *<No.>*: MA identification number *<MEPID>*: MEP ID [Action] A fault was detected in a partner switch. Check the status of the partner switch.			

- `CRITC` information

Table 2-18 Switch CRITC information when the event location is VLAN (CFM)

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	CRITC	VLAN	07200500	Could not start CFM function (Code=*xx*)
	The CFM functionality could not start. *xx*: Cause code (information for vendor analysis) [Action] Use the `reload` operation command to restart the Switch.			

- FATAL information

Table 2-19 Switch FATAL information when the event location is VLAN (CFM)

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	FATAL	VLAN	07100510	Swd Configuration Error (Code1=*xx* Code2=*xx*)
	The CFM configuration could not be set for the hardware controller. *xx*: Cause code (information for vendor analysis) [Action] None (The Switch automatically restarts.)			

2.3.6 Event location = SNOOP

The following tables describe Switch failure and event information when the event location is SNOOP.

- INFO information

Table 2-20 Switch INFO information when the event location is SNOOP

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	SNOOP		The number of the snooping entry exceeded the capacity of this system.
	An attempt to register an IPv4 multicast group failed because the number of learning entries used in IGMP/MLD snooping exceeds the switch capacity (maximum of 500) of the Switch. [Action] The number of entries exceeds the capacity limit. Review the system configuration and setting so that you can reduce the number of entries.			
2	INFO	SNOOP		The number of the snooping entry exceeded the capacity of this system.
	An attempt to register an IPv6 multicast group failed because the number of learning entries used in IGMP/MLD snooping exceeds the switch capacity (maximum of 500) of the Switch. [Action] Because the number of entries exceeds the capacity limit, review the system configuration and setting so that you can reduce the number of entries.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
3	INFO	SNOOP		IGMP querier changed on VLAN *<ID>* - lost IGMP querier address *<IPv4 address>*
	The availability of the IPv4 multicast group member (recipient host) cannot be confirmed. Therefore, IPv4 multicast data forwarding is not properly executed due to the following reasons: The IGMP querier information was deleted because the advertisement (IGMP Query) from the IGMP querier at *<IPv4 address >*on VLAN *<VLAN ID>* disappeared. If the Switch is the IGMP querier, the IGMP querier information was deleted because the IP address of the VLAN *<VLAN ID>* was deleted. *<VLAN ID>*: VLAN ID *<IPv4 address>*: IPv4 address [Action] 1. Check the connection with the IGMP querier at *<IPv4 address>*. 2. Check whether the IGMP querier change message (`IGMP querier changed on VLAN` *<VLAN ID>* `- new IGMP querier address` *<IPv4 address>*.) was output. 3. If the connection with the IGMP querier cannot be checked, execute the configuration command `ip igmp snooping querier` to enable the IGMP querier function of the Switch.			
4	INFO	SNOOP		MLD querier changed on VLAN *<VLAN ID>* - lost MLD querier address *<IPv6 address>*
	The availability of the IPv6 multicast group member (recipient host) cannot be confirmed. Therefore, the IPv6 multicast data forwarding is not be properly executed due to the following reasons: The MLD querier information was deleted because an advertisement (MLD Query) from the MLD querier at *<IPv6 address >*on VLAN *<VLAN ID>* disappeared. *<VLAN ID>*: VLAN ID *<IPv6 address>*: IPv6 address [Action] 1. Check the connection with the MLD querier at *<IPv6 address>*. 2. Check whether the MLD querier change message (`MLD querier changed on VLAN` *<VLAN ID>* `- new MLD querier address` *<IPv6 address>*.) was output. 3. If the connection with the MLD querier cannot be checked, execute the configuration command `ipv6 mld snooping querier` to enable the MLD querier function of the Switch.			
5	INFO	SNOOP		IGMP querier changed on VLAN *<VLAN ID>* - new IGMP querier address *<IPv4 address>*
	The IGMP querier was changed to *<IPv4 address>* because a new IGMP querier was identified on the VLAN (*<VLAN ID>*). *<VLAN ID>*: VLAN ID *<IPv4 address>*: IPv4 address [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
6	INFO	SNOOP		MLD querier changed on VLAN *<VLAN ID>* - new MLD querier address *<IPv6 address>*
	The MLD querier was changed to *<IPv6 address>* because a new MLD querier was identified on the VLAN (*<VLAN ID>*). *<VLAN ID>*: VLAN ID *<IPv6 address>*: IPv6 address [Action] None			
7	INFO	SNOOP		IPv4 address not defined on VLAN *<VLAN ID>*, IGMP querier function stopped
	The IGMP querier on the VLAN (*<VLAN ID>*) stopped because the IPv4 address is not set. *<VLAN ID>*: VLAN ID [Action] 1. Set an IPv4 address for the VLAN. 2. Execute the `show igmp-snooping` command and confirm that the IPv4 address set for the VLAN is displayed.			
8	INFO	SNOOP		MLD query source address not defined on VLAN *<VLAN ID>*, MLD querier function stopped
	The MLD querier on the VLAN *<VLAN ID>* stopped because the source IP address for MLD query messages is not set. *<VLAN ID>*: VLAN ID [Action] 1. Set an MLD snooping source IPv6 address for the VLAN. 2. Execute the `show mld-snooping` command and confirm that the IPv6 address set for the VLAN is displayed.			

- FATAL information

Table 2-21 Switch FATAL information when the event location is SNOOP

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	FATAL	SNOOP	2e113110	IGMPsnooping: set snooping enable to filter by config, error (error code) occurred on VLAN *<VLAN ID>*
	An error (*<error code>*) occurred on the VLAN *<VLAN ID>* when configuring the IGMP snooping start settings for the hardware. *<VLAN ID>*: VLAN ID [Action] None (The Switch automatically restarts.)			

No.	Event level	Event location	Ref. Code	Message text
	Description			
2	FATAL	SNOOP	2e123110	MLDsnooping: set snooping enable to filter by config, error (error code) occurred on VLAN *<VLAN ID>*
	An error (*<error code>*) occurred on the VLAN *<VLAN ID>* when configuring the MLD snooping start settings for the hardware. *<VLAN ID>*: VLAN ID [Action] None (The Switch automatically restarts.)			
3	FATAL	SNOOP	2e113100	IGMPsnooping: set snooping disable to filter by config, error (error code) occurred on VLAN*<VLAN ID>*
	An error (*<error code>*) occurred on VLAN *<VLAN ID>* when clearing the IGMP snooping settings for the hardware. *<VLAN ID>*: VLAN ID [Action] None (The Switch automatically restarts.)			
4	FATAL	SNOOP	2e123100	MLDsnooping: set snooping disable to filter by config, error (error code) occurred on VLAN*<VLAN ID>*
	An error (*<error code>*) occurred on VLAN *<VLAN ID>* when clearing the MLD snooping settings for the hardware. *<VLAN ID>*: VLAN ID [Action] None (The Switch automatically restarts.)			
5	FATAL	SNOOP	2e113200	IGMPsnooping: set snooping disable to filter by config, error (error code) occurred on VLAN*<VLAN ID>*
	An error (*<error code>*) occurred when clearing the IGMP snooping setting for the hardware because the VLAN *<VLAN ID>* for which IGMP snooping is enabled was deleted. *<VLAN ID>*: VLAN ID [Action] None (The Switch automatically restarts.)			
6	FATAL	SNOOP	2e123200	MLDsnooping: set snooping disable to filter by config, error (error code) occurred on VLAN*<VLAN ID>*
	An error (*<error code>*) occurred when the MLD snooping setting for the hardware was cleared because the VLAN *<VLAN ID>* for which MLD snooping is enabled was deleted. *<VLAN ID>*: VLAN ID [Action] None (The Switch automatically restarts.)			

No.	Event level	Event location	Ref. Code	Message text
	Description			
7	FATAL	SNOOP	2e113301	IGMPsnooping: set port*<IF#>* mrouter enable to driver by snoop start, error (error code) occurred on VLAN*<VLAN ID>*
	An error (*<error code>*) occurred on the router port *<IF#>* for the hardware when IGMP snooping started for the VLAN *<VLAN ID>*. *<VLAN ID>*: VLAN ID *<IF#>*: Interface port number [Action] None (The Switch automatically restarts.)			
8	FATAL	SNOOP	2e123301	MLDsnooping: set port*<IF#>* mrouter enable to driver by snoop start, error (error code) occurred on VLAN*<VLAN ID>*
	An error (*<error code>*) occurred on a router port *<IF#>* for the hardware when MLD snooping started for the VLAN *<VLAN ID>*. *<VLAN ID>*: VLAN ID *<IF#>*: Interface port number [Action] None (The Switch automatically restarts.)			
9	FATAL	SNOOP	2e113311	IGMPsnooping: set port*<IF#>* mrouter enable to driver by config, error (error code) occurred on VLAN*<VLAN ID>*
	An error (*<error code>*) occurred when configuring the VLAN *<VLAN ID>* router port *<IF#>* for the hardware. *<VLAN ID>*: VLAN ID *<IF#>*: Interface port number [Action] None (The Switch automatically restarts.)			
10	FATAL	SNOOP	2e123311	MLDsnooping: set port*<IF#>* mrouter enable to driver by config, error (error code) occurred on VLAN*<VLAN ID>*
	An error (*<error code>*) occurred when configuring the VLAN *<VLAN ID>* router port *<IF#>* for the hardware. *<VLAN ID>*: VLAN ID *<IF#>*: Interface port number [Action] None (The Switch automatically restarts.)			
11	FATAL	SNOOP	2e113321	IGMPsnooping: set port*<IF#>* mrouter enable to driver by accommodated to vlan, error (error code) occurred on VLAN*<VLAN ID>*
	An error (*<error code>*) occurred when the router port *<IF#>* was set for the hardware with router port settings enabled because a port not contained in VLAN *<VLAN ID>* was moved to the VLAN. *<VLAN ID>*: VLAN ID *<IF#>*: Interface port number [Action] None (The Switch automatically restarts.)			

No.	Event level	Event location	Ref. Code	Message text
	Description			
12	FATAL	SNOOP	2e123321	MLDsnooping: set port<*IF#*> mrouter enable to driver accommodated to vlan, error (error code) occurred on VLAN<*VLAN ID*>
	An error (<*error code*>) occurred when the router port <*IF#*> was set for the hardware with router port settings enabled because a port not contained in VLAN <*VLAN ID*> was moved to the VLAN. <*VLAN ID*>: VLAN ID <*IF#*>: Interface port number [Action] None (The Switch automatically restarts.)			
13	FATAL	SNOOP	2e113310	IGMPsnooping: set port<*IF#*> mrouter disable to driver by config, error (error code) occurred on VLAN<*VLAN ID*>
	An error (<*error code*>) occurred when VLAN <*VLAN ID*> router port <*IF#*> settings for the hardware were cleared by the configuration. <*VLAN ID*>: VLAN ID <*IF#*>: Interface port number [Action] None (The Switch automatically restarts.)			
14	FATAL	SNOOP	2e123310	MLDsnooping: set port<*IF#*> mrouter disable to driver by config, error (error code) occurred on VLAN<*VLAN ID*>
	An error (<*error code*>) occurred when VLAN <*VLAN ID*> router port <*IF#*> settings for the hardware were cleared by the configuration. <*VLAN ID*>: VLAN ID <*IF#*>: Interface port number [Action] None (The Switch automatically restarts.)			
15	FATAL	SNOOP	2e113320	IGMPsnooping: set port<*IF#*> mrouter disable to driver by excluded vlan, error (error code) occurred on VLAN<*VLAN ID*>
	An error (<*error code*>) occurred when IGMP snooping router port <*IF#*> settings for the hardware were released with router port settings enabled because a port (port <*IF#*>) contained in VLAN <*VLAN ID*> was detached from the VLAN. <*VLAN ID*>: VLAN ID <*IF#*>: Interface port number [Action] None (The Switch automatically restarts.)			
16	FATAL	SNOOP	2e123320	MLDsnooping: set port<*IF#*> mrouter disable to driver by excluded vlan, error (error code) occurred on VLAN<*VLAN ID*>
	An error (<*error code*>) occurred when MLD snooping router port <*IF#*> settings for the hardware were released with router port settings enabled because a port (port <*IF#*>) contained in VLAN <*VLAN ID*> was detached from the VLAN. <*VLAN ID*>: VLAN ID <*IF#*>: Interface port number [Action] None (The Switch automatically restarts.)			

2.3.7 Event location = DHCP

The following table describes Switch failure and event information when the event location is DHCP.

- INFO information

Table 2-22 Switch INFO information when the event location is DHCP

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	DHCP		The non-used IP address that a dhcp_server can lease out is not a subnet *<SUBNET_ADDRESS>*.
	The unused IP addresses leased by the DHCP server do not exist in the subnet address. *<SUBNET_ADDRESS>*: Subnet address [Action] Examine the maximum number of DHCP clients in the subnet that the DHCP server can allocate.			
2	INFO	DHCP		The dhcp_server reused the abandoned IP address *<IP_ADDRESS>*.
	The DHCP server reused a discarded IP address. *<IP_ADDRESS>*: Reused IP address [Action] None			
3	INFO	DHCP		The IP address *<IP_ADDRESS>* that the dhcp_server schedules to lease out is already used by others.
	The IP address to be leased by the DHCP server is already being used. *<IP_ADDRESS>*: IP address to be leased [Action] None			

2.3.8 Event location = LINKAGG

The following table describes Switch failure and event information when the event location is `LINKAGG`.

- `INFO` information

Table 2-23 Switch INFO information when the event location is LINKAGG

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	LINKAGG		Port *<IF#>* detached from Channel Group *<Channel group#>*
	The port *<IF#>* was detached from the channel group. *<IF#>*: Interface port number *<Channel group#>*: Channel group number [Action] 1. Check whether the connection with the remote switch is correct. 2. Check whether the remote switch is configured correctly.			
2	INFO	LINKAGG		Channel Group *<Channel group#>* is Down
	A channel group is Down. *<Channel group#>*: Channel group number [Action] 1. Make sure that the line is not Down. 2. Make sure that the line is not half duplex. 3. Make sure that the LACP setting of the remote switch is correct.			
3	INFO	LINKAGG		Port *<IF#>* attached to Channel Group *<Channel group#>*
	A port was aggregated to the channel group. *<IF#>*: Interface port number *<Channel group#>*: Channel group number [Action] None			
4	INFO	LINKAGG		Channel Group *<Channel group#>* is Up.
	A channel group is Up. *<Channel group#>*: Channel group number [Action] None			

2.3.9 Event location = DHCPSN

The following tables describe Switch failure and event information when the event location is DHCPSN.

- INFO information

Table 2-24 Switch INFO information when the event location is DHCPSN

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	DHCPSN		Binding entry created (<*MAC_ADDRESS*>/<*VLAN ID*>/<*IP_ADDRESS*>)
	A binding database was created. <*MAC_ADDRESS*>/<*VLAN ID*>/<*IP_ADDRESS*>: DHCP client terminal information <*MAC_ADDRESS*>: MAC address <*VLAN ID*>: VLAN ID <*IP_ADDRESS*>: IP address [Action] None			
2	INFO	DHCPSN		Binding entry timeout(<*MAC_ADDRESS*>/<*VLAN ID*>/<*IP_ADDRESS*>)
	The binding database was deleted because of an aging timeout. <*MAC_ADDRESS*>/<*VLAN ID*>/<*IP_ADDRESS*>: DHCP client terminal information <*MAC_ADDRESS*>: MAC address <*VLAN ID*>: VLAN ID <*IP_ADDRESS*>: IP address [Action] None			
3	INFO	DHCPSN		Binding entry was deleted by received DHCPRELEASE(<*MAC_ADDRESS*>/<*VLAN ID*>/<*IP_ADDRESS*>)
	The binding database was deleted because DHCPRELEASE was received. <*MAC_ADDRESS*>/<*VLAN ID*>/<*IP_ADDRESS*>: DHCP client terminal information <*MAC_ADDRESS*>: MAC address <*VLAN ID*>: VLAN ID <*IP_ADDRESS*>: IP address [Action] None			
4	INFO	DHCPSN		Binding entry was deleted by received DHCPDECLINE(<*MAC_ADDRESS*>/<*VLAN ID*>/<*IP_ADDRESS*>)
	The binding database was deleted because DHCPDECLINE was received. <*MAC_ADDRESS*>/<*VLAN ID*>/<*IP_ADDRESS*>: DHCP client terminal information <*MAC_ADDRESS*>: MAC address <*VLAN ID*>: VLAN ID <*IP_ADDRESS*>: IP address [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
5	INFO	DHCPSN		Binding entry changed from dynamic through the configuration(*<MAC_ADDRESS>*/*<VLAN ID>*/*<IP_ADDRESS>*)
	The contents of the binding database was changed to the settings of the `ip source binding` configuration command because the same IP address and VLAN number as those of the dynamically learned binding database had been set to the binding database using the `ip source binding` configuration command *<MAC_ADDRESS>*/*<VLAN ID>*/*<IP_ADDRESS>*: DHCP client terminal information *<MAC_ADDRESS>*: MAC address *<VLAN ID>*: VLAN ID *<IP_ADDRESS>*: IP address [Action] None			
6	INFO	DHCPSN		The binding entry was renewed (*<MAC_ADDRESS>*/*<VLAN ID>*/*< IP_ADDRESS>*).
	The binding database was updated because the changes of connection ports or MAC addresses corresponding to the IP addresses assigned to DHCP client terminals were detected by receiving `DHCPACK/BOOTPREPLY`. *<MAC_ADDRESS>*/*<VLAN ID>*/*<IP_ADDRESS>*: DHCP client terminal information *<MAC_ADDRESS>*: MAC address *<VLAN ID>*: VLAN ID *<IP_ADDRESS>*: IP address [Action] None			
7	INFO	DHCPSN		Failed to make binding entry because interface unknown(*<MAC_ADDRESS>*/*<VLAN ID>*/*<IP_ADDRESS>*)
	The creation or update of a binding database failed because the connection port for a DHCP client is unknown. *<MAC_ADDRESS>*/*<VLAN ID>*/*<IP_ADDRESS>*: DHCP client terminal information *<MAC_ADDRESS>*: MAC address *<VLAN ID>*: VLAN ID *<IP_ADDRESS>*: IP address [Action] None			
8	INFO	DHCPSN		Observed ARP flood, some packets shall be discarded (*<IF_NUMBER>*).
	The number of received ARP packets exceeded the number of the reception rate set by using the `ip arp inspection limit rate` configuration command. *<IF_NUMBER>*: Type and number of the interface for which the reception rate is exceeded ● Port=*<IF#>*: Interface port number ● ChGr=*<Channel group#>*: Channel group number [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
9	INFO	DHCPSN		ARP flood ebbed (*<IF_NUMBER>*)
	The reception rate for ARP packets has not been exceeded for 30 seconds. (After this, if the reception rate is exceeded, the events for when the reception rate is exceeded are collected again.) *<IF_NUMBER>*: Type and number of the interface in which the reception rate is exceeded ● Port=*<IF#>*: Interface port number ● ChGr=*<Channel group#>*: Channel group number [Action] None			
10	INFO	DHCPSN		Observed DHCP flood, some packets shall be discarded (*<IF_NUMBER>*).
	The number of received DHCP packets exceeded the number of the reception rate set by using the `ip dhcp snooping limit rate` configuration command. *<IF_NUMBER>*: Type and number of the interface in which the reception rate is exceeded ● Port=*<IF#>*: Interface port number ● ChGr=*<Channel group#>*: Channel group number [Action] None			
11	INFO	DHCPSN		DHCP flood ebbed (*<IF_NUMBER>*)
	The reception rate for DHCP packets has not been exceeded for 30 seconds. (After this, if the reception rate is exceeded, the events for when the reception rate is exceeded are collected again.) *<IF_NUMBER>*: Type and number of the interface in which the reception rate is exceeded ● Port=*<IF#>*: Interface port number ● ChGr=*<Channel group#>*: Channel group number [Action] None			
12	INFO	DHCPSN		Failed to make binding entry exceeded (*<MAC_ADDRESS>*/*<VLAN ID>*/*<IP_ADDRESS>*)
	The generation of the binding database failed because of insufficient database entries. *<MAC_ADDRESS>*/*<VLAN ID>*/*<IP_ADDRESS>*: DHCP client terminal information *<MAC_ADDRESS>*: MAC address *<VLAN ID>*: VLAN ID *<IP_ADDRESS>*: IP address [Action] The capacity limit of the Switch was exceeded. Review the system configuration.			
13	INFO	DHCPSN		Succeeded in the restored binding database from *<url>* [retry]
	The binding database was restored from the specified storage destination. *<url>*: Specified storage destination ● `flash`: Indicates internal flash memory ● mc: SD memory card [retry]: Number of retries [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
14	INFO	DHCPSN		Succeeded in the restored binding database from *<url>* [retry] (*<reason>*)
	The binding database was restored from the specified storage destination. *<url>*: Specified storage destination ● `flash`: Indicates internal flash memory ● mc: SD memory card [retry]: Number of retries *<reason>*: Reason The number of the dynamic entries is zero. (The number of dynamic entries was zero.) [Action] None			
15	INFO	DHCPSN		DHCP server packets were received at an untrusted port (*<IF_NUMBER>*/*<VLAN ID>*/*<MAC_ADDRESS>*/*<IP_ADDRESS>*).
	An invalid DHCP server was detected. This message is output once every five minutes on a port-by-port basis. *<IF_NUMBER>*: Type and number of the interface that received the DHCP packets ● *<IF#>*: Interface port number ● ChGr: *<Channel group#>*: Channel group number *<VLAN ID>*/*<MAC_ADDRESS>*/*<IP_ADDRESS>*: DHCP server information *<VLAN ID>*: VLAN ID *<MAC_ADDRESS>*: MAC address *<IP_ADDRESS>*: IP address [Action] Check the connected switch.			

- WARN information

Table 2-25 Switch WARN information when the event location is DHCPSN

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	WARN	DHCPSN		It was not able to restore the binding database from <*url*>. [retry] (<*reason*>)
	The binding database could not be restored from the specified storage destination. <*url*>: Specified storage destination ● flash: Internal flash memory ● mc: SD memory card [retry]: Number of retries <*reason*>: Reason for the failure ● An MC is not inserted. (No MC is inserted.) ● The MC file is not found. (No file is found in the MC.) ● It accessed the MC through another process. (The MC is being used by another process.) ● It is accessed Flash by other processing. (The internal flash memory is being used by another process.) ● MC file is not reading. (A file in the MC cannot be loaded.) ● May be broken. (The storage destination specified in the configuration might be corrupted.) ● The data is not saved. (There is no restorable data.) Any <*reason*> other than the above is for vendor analysis. [Action] Take appropriate action according to the indicated reason.			
2	WARN	DHCPSN		It cannot store a binding database (<*reason*>).
	The binding database could not be stored. <*reason*>: Reason for the failure An MC is not inserted. (No MC is inserted.) Can't access to MC by write protection. (The MC is read-only.) [Action] Take appropriate action according to the indicated reason.			
3	WARN	DHCPSN		It was not able to store a binding database in <*url*>. [retry] (<*reason*>)
	The binding database could not be saved to the specified storage destination. <*url*>: Specified storage destination ● mc: SD memory card [retry]: Number of retries <*reason*>: Reason for the failure ● MC is not inserted. (No MC is inserted.) ● Can't access to MC by write protection. (The MC is read-only.) ● It is accessed MC by other processing. (The MC is being used by another process.) ● MC file is not writing. (A file in the MC cannot be written to.) Any <*reason*> other than the above is for vendor analysis. [Action] Take appropriate action according to the indicated reason.			

- ERROR information

Table 2-26 Switch ERROR information when the event location is DHCPSN

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	ERROR	DHCPSN	31300016	It was not able to store a binding database in <*url*>. [retry] (<*reason*>)
	The binding database could not be saved to the specified storage destination. <*url*>: Specified storage destination ● flash: Indicates internal flash memory [retry]: Number of retries <*reason*>: Reason for the failure It is accessed Flash by other processing. (The internal flash memory is being used by another process.) Any <*reason*> other than the above is for vendor analysis. [Action] Take appropriate action according to the indicated reason.			

2.3.10 Event location = IP

The following table describes switch failure and event information when the event location is IP.

- INFO information

Table 2-27 Switch INFO information when the event location is IP

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	IP		Duplicate IP address *x.x.x.x* (VLAN<*VLAN ID*>) on *xxxx.xxxx.xxxx*
	A duplicate IP address was detected on the VLAN <*VLAN ID*> interface. *x.x.x.x*: IP address in which duplication was detected VLAN<*VLAN ID*>: Interface number of the VLAN on which the duplicate IP address was detected *xxxx.xxxx.xxxx*: MAC address of the remote switch with the duplicate IP address (Source MAC address during ARP payload) [Action] Change the IP address of the VLAN interface for the Switch. Alternatively, change the duplicate IP address of the remote switch.			

2.4 Switch parts

2.4.1 Event location = KERNEL

The following tables describe switch failure and event information when the event location is `KERNEL.INFO` information

Table 2-28 Switch INFO information when the event location is KERNEL

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	KERNEL		Boot cause is system fault
	An error occurred, and then the Switch restarted. [Action] None			
2	INFO	KERNEL		Boot cause is exception
	An unexpected interruption occurred, and then the Switch restarted. [Action] None			
3	INFO	KERNEL		Boot cause is watchdog timeout
	A hardware watchdog timeout occurred, and then the Switch restarted. [Action] None			
4	INFO	KERNEL		Boot cause is reset button
	The Switch restarted because the RESET button was pressed. [Action] None			
5	INFO	KERNEL		Boot cause is expired sleep time
	The Switch restarted because the switch sleep period expired. [Action] None			
6	INFO	KERNEL		Boot cause is wake up from sleep by force
	The Switch restarted because the switch's sleep state was forcibly released. [Action] None			

- `ERROR` information

Table 2-29 Switch ERROR information when the event location is KERNEL

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	ERROR	KERNEL	1F336000	*<xxxxxxxx>* WDT Error !!
	A software watchdog timeout occurred. *<xxxxxxxx>*: Location where the error occurred (information for vendor analysis) [Action] Check the log by executing the `show critical-logging` operation command. If another problem is indicated in the log, take appropriate action according to the error message.			
2	ERROR	KERNEL	1F337000	WDT is detected (by HW)
	A hardware watchdog timeout occurred. [Action] Check the log by executing the `show critical-logging` operation command. If another problem is indicated in the log, take appropriate action according to the error message.			
3	ERROR	KERNEL	1F338000	The reboot of another origin is detected. (Register information)
	The kernel detected a software anomaly and restarted the system. [Action] Check the log by executing the `show critical-logging` operation command. If another problem is indicated in the log, take appropriate action according to the error message.			
4	ERROR	KERNEL	1F*xxxxxx* other than the above ref. codes	All other cases
	An internal error was detected in the kernel. [Action] Check the log by executing the `show critical-logging` operation command. If another problem is indicated in the log, take appropriate action according to the error message.			

2.4.2 Event location = NTP

The following table describes Switch failure and event information when the event location is NTP.

- INFO information

Table 2-30 Switch INFO information when the event location is NTP

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	NTP		NTPC: Fixation time not notified!
	The periodic monitoring report stopped because the periodic update time came during command execution. [Action] None			
2	INFO	NTP		NTPC: Time set up (Difference of 5 sec or more!)
	The time was configured, but the time lag is five seconds or more. [Action] None			

2.4.3 Event location = 802.1X

The following tables describe Switch failure and event information when the event location is 802.1X.

- ERROR information

Table 2-31 Switch ERROR information when the event location is 802.1X

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	ERROR	802.1X	08330011	There is a possibility that 802.1X (port) was not set in some interfaces.
	For some interfaces, 802.1X (port-based authentication) might not be configured. [Action] Delete settings for 802.1X by using the no command, and then reconfigure 802.1X.			
2	ERROR	802.1X	08330012	There is a possibility that 802.1X (port) was not unset in some interfaces.
	For some interfaces, 802.1X (port-based authentication) might not be unset. [Action] Configure the settings by using the commands again, and then delete settings for 802.1X by using the no command.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
3	ERROR	802.1X	08330013	There is a possibility that 802.1X (vlan(dynamic) was not set in some interfaces.
	For some interfaces, 802.1X (VLAN-based authentication [dynamic]) might not be configured. [Action] Delete settings for 802.1X by using the no command, and then reconfigure 802.1X.			
4	ERROR	802.1X	08330014	There is a possibility that 802.1X (vlan(dynamic) was not unset in some interfaces.
	In some interfaces, 802.1X (VLAN-based authentication [dynamic]) might not be cleared. [Action] Configure the settings by using the commands, and then delete settings for 802.1X by using the no command again.			

- CRITC information

Table 2-32 Switch CRITC information when the event location is 802.1X

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	CRITC	802.1X	08220001 08220002 08220003 08220004 08220005 08220006 08220007 08220008	Could not start the L2-authentication function
	Layer-2 authentication functionality could not start when the Switch started. [Action] Use the reload operation command to restart the Switch.			
2	CRITC	802.1X	08220011	Could not start the 802.1X Authenticator function
	The 802.1X functionality could not start. [Action] Use the reload operation command to restart the Switch.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
3	CRITC	802.1X	08220021 08220022 08220031 08220032 08220041	Internal error occurred (code=*xx*)
	An internal processing error occurred. *xx*: Cause code (information for vendor analysis) [Action] Use the `reload` operation command to restart the Switch.			

2.4.4 Event location = RADIUS

The following tables describe Switch failure and event information when the event location is `RADIUS`.

- `INFO` information

Table 2-33 Switch INFO information when the event location is RADIUS

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	RADIUS		Authentication dead-interval timer start
	The monitoring timer started according to the setting of the `radius-server dead-interval` configuration command because the secondary RADIUS server became the RADIUS authentication request destination due to the failure of the primary RADIUS server. [Action] None			
2	INFO	RADIUS		Accounting dead-interval timer start
	The monitoring timer started according to the setting of the `radius-server dead-interval` configuration command because the secondary RADIUS server became the RADIUS accounting destination due to the failure of the primary RADIUS server. [Action] None			
3	INFO	RADIUS		Authentication dead-interval timer stop
	The monitoring timer configured by using the `mac-authentication radius-server dead-interval` configuration command stopped due to one of the following reasons: - The monitoring timer configured by using the `radius-server dead-interval` configuration command expired. - The RADIUS authentication request destination changed from the secondary RADIUS server to the restored primary RADIUS server. [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
4	INFO	RADIUS		Accounting dead-interval timer stop
	The monitoring timer configured by using the `mac-authentication radius-server dead-interval` configuration command stopped due to one of the following reasons: ● The monitoring timer configured by using the `radius-server dead-interval` configuration command expired. ● The RADIUS accounting destination changed from the secondary RADIUS server to the restored primary RADIUS server. [Action] None			
5	INFO	RADIUS		MAC authentication dead-interval timer start
	The monitoring timer started according to the setting of the `mac-authentication radius-server dead-interval` configuration command because the secondary RADIUS server for MAC authentication became the RADIUS authentication request destination due to the failure of the primary RADIUS server for MAC authentication. [Action] None			
6	INFO	RADIUS		MAC accounting dead-interval timer start
	The monitoring timer started according to the setting of the `mac-authentication radius-server dead-interval` configuration command because the secondary RADIUS server for MAC authentication became the RADIUS accounting destination due to the failure of the primary RADIUS server for MAC authentication. [Action] None			
7	INFO	RADIUS		MAC authentication dead-interval timer stop
	The monitoring timer configured by using the `mac-authentication radius-server dead-interval` configuration command stopped due to one of the following reasons: ● The monitoring timer configured by using the `mac-authentication radius-server dead-interval` configuration command expired. ● The RADIUS authentication request destination changed from the secondary RADIUS server for MAC authentication to the restored primary RADIUS server for MAC authentication. [Action] None			
8	INFO	RADIUS		MAC accounting dead-interval timer stop
	The monitoring timer configured by using the `mac-authentication radius-server dead-interval` configuration command stopped due to one of the following reasons: ● The monitoring timer configured by using the `mac-authentication radius-server dead-interval` configuration command expired. ● The RADIUS accounting destination changed from the secondary RADIUS server for MAC authentication to the restored primary RADIUS server for MAC authentication. [Action] None			
9	INFO	RADIUS		Web authentication dead-interval timer start

No.	Event level	Event location	Ref. Code	Message text
	Description			
	The monitoring timer started according to the setting of the `web-authentication radius-server dead-interval` configuration command because the secondary RADIUS server for Web authentication became the RADIUS authentication request destination due to the failure of the primary RADIUS server for Web authentication. [Action] None			
10	INFO	RADIUS		Web accounting dead-interval timer start
	The monitoring timer started according to the setting of the `web-authentication radius-server dead-interval` configuration command because the secondary RADIUS server for Web authentication became the RADIUS accounting destination due to the failure of the primary RADIUS server for Web authentication. [Action] None			
11	INFO	RADIUS		Web authentication dead-interval timer stop
	The monitoring timer configured by using the `web-authentication radius-server dead-interval` configuration command stopped due to one of the following reasons: ● The monitoring timer configured by using the `web-authentication radius-server dead-interval` configuration command expired. ● The RADIUS authentication request destination changed from the secondary RADIUS server for Web authentication to the restored primary RADIUS server for Web authentication. [Action] None			
12	INFO	RADIUS		Web accounting dead-interval timer stop
	The monitoring timer configured by using the `web-authentication radius-server dead-interval` configuration command stopped due to one of the following reasons: ● The monitoring timer configured by using the `web-authentication radius-server dead-interval` configuration command expired. ● The RADIUS accounting destination changed from the secondary RADIUS server for Web authentication to the restored primary RADIUS server for Web authentication. [Action] None			
13	INFO	RADIUS		802.1X authentication dead-interval timer start
	The monitoring timer started according to the setting of the `dot1x radius-server dead-interval` configuration command because the secondary RADIUS server for IEEE 802.1X authentication became the RADIUS authentication request destination due to the failure of the primary RADIUS server for IEEE 802.1X authentication. [Action] None.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
14	INFO	RADIUS		802.1X accounting dead-interval timer start
	The monitoring timer started according to the setting of the `dot1x radius-server dead-interval` configuration command because the secondary RADIUS server for IEEE 802.1X authentication became the RADIUS accounting destination due to the failure of the primary RADIUS server for IEEE 802.1X authentication. [Action] None			
15	INFO	RADIUS		802.1X authentication dead-interval timer stop
	The monitoring timer configured by using the `dot1x radius-server dead-interval` configuration command stopped due to one of the following reasons: ● The monitoring timer configured by using the `dot1x radius-server dead-interval` configuration command expired. ● The RADIUS authentication request destination changed from the secondary RADIUS server for IEEE 802.1X authentication to the restored primary RADIUS server for IEEE 802.1X authentication. [Action] None			
16	INFO	RADIUS		802.1X accounting dead-interval timer stop
	The monitoring timer configured by using the `dot1x radius-server dead-interval` configuration command stopped due to one of the following reasons: ● The monitoring timer configured by using the `dot1x radius-server dead-interval` configuration command expired. ● The RADIUS accounting destination changed from the secondary RADIUS server for IEEE 802.1X authentication to the restored primary RADIUS server for IEEE 802.1X authentication. [Action] None			
17	INFO	RADIUS		Group[x] authentication dead-interval timer start
	The monitoring timer started according to the setting of the `radius-server dead-interval` configuration command because the secondary RADIUS server in RADIUS server group *x* became the RADIUS authentication request destination due to the failure of the primary RADIUS server in the same group. x: RADIUS server group name [Action] None			
18	INFO	RADIUS		Group[x] authentication dead-interval timer stop
	The monitoring timer configured by using the `mac-authentication radius-server dead-interval` configuration command stopped due to one of the following reasons: ● The monitoring timer configured by using the `radius-server dead-interval` configuration command expired. ● The RADIUS authentication request destination changed from the secondary RADIUS server in RADIUS server group *x* to the restored primary RADIUS server in the same group. x: RADIUS server group name [Action] None			

- `ERROR` information

Table 2-34 Switch ERROR information when the event location is RADIUS

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	ERROR	RADIUS	10330001	Cannot set radius-server(host=*x.x.x.x*) because of internal error
	The `radius-server` configuration command (for the host in which the IP address is *x.x.x.x*) could not be configured. Usually, an error caused by executing the `radius-server` configuration command is handled as a command error. However, this event is caused by consecutively executing the `radius-server` configuration command, as internal settings are performed after the command is accepted.) [Action] Execute the `no` command to delete the settings for the `radius-server host` or `radius-server key` configuration command, and then set the configuration command again.			

- `CRITC` information

Table 2-35 Switch CRITC information when the event location is RADIUS

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	CRITC	RADIUS	10220012	Could not start the RADIUS Client function
	The RADIUS client functionality could not start. [Action] Use the `reload` operation command to restart the Switch.			

2.4.5 Event location = CERTIF

The following tables describe Switch failure and event information when the event location is `CERTIF`.

- `WARN` information

Table 2-36 Switch WARN information when the event location is CERTIF

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	WARN	CERTIF		File name '*<html-file>*' is reserved.
	A file with the same name as the name of the management file was detected in the files configured by using the Web authentication window replacement functionality. The file was restored successfully, but the following functionality may not operate normally. ● Port-based authentication window replacement functionality ● Secure Wake-on-LAN *<html-file>*: Name of the file that has the same name as the management file [Action] To recover the file: 1. Retrieving registered files Execute the `store web-authentication html-files` operation command to retrieve the files registered on the RAMDISK. 2. Copying a registered file Execute the `copy ramdisk` *<File name>* `mc` *<File name>* operation command to copy a file registered on the RAMDISK to a memory card. 3. Editing a registered file Use a PC to edit the contents and name of the file copied to the memory card to resolve the duplicate file names. 4. Deleting registered files Execute the `clear web-authentication html-files -all` operation command to delete all registered files. 5. Re-registering edited files Execute the `set web-authentication html-files` operation command to re-register the file edited in step 3.			
2	WARN	CERTIF		Directory size over
	The directory capacity exceeds the maximum capacity (256 KB) that is set by using the Web authentication window replacement functionality. [Action] To recover the file: 1. Retrieving registered files Execute the `store web-authentication html-files` operation command to retrieve the files registered on the RAMDISK. 2. Copying a registered file Execute the `copy ramdisk` *<File name>* `mc` *<File name>* operation command to copy a file registered on the RAMDISK to a memory card. 3. Editing a registered file Edit the contents of the file copied to the memory card to decrease the directory capacity to the limit value or lower. 4. Deleting registered files Execute the `clear web-authentication html-files -all` operation command to delete all registered files. 5. Re-registering edited files Execute the `set web-authentication html-files` operation command to re-register the file edited in step 3.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
3	WARN	CERTIF		Too many files
	The number of files exceeds the maximum number of files (64 files) that is set by using the Web authentication window replacement functionality. [Action] To recover the file: 1. Retrieving registered files Execute the `store web-authentication html-files` operation command to retrieve the files registered on the RAMDISK. 2. Copying a registered file Execute the `copy ramdisk` <*File name*> `mc` <*File name*> operation command to copy a file registered on the RAMDISK to a memory card. 3. Editing a registered file Edit the contents of the file copied to the memory to decrease the number of files to the limit value or lower. 4. Deleting registered files Execute the `clear web-authentication html-files -all` operation command to delete all registered files. 5. Re-registering edited files Execute the `set web-authentication html-files` operation command to re-register the file edited in step 3.			

- `CRITC` information

Table 2-37 Switch CRITC information when the event location is CERTIF

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	CRITC	CERTIF	0f212006	Could not start MAC Authentication function (Code=*xx*)
	The MAC authentication functionality could not start. *xx*: Cause code (information for vendor analysis) [Action] Use the `reload` operation command to restart the Switch.			
2	CRITC	CERTIF	0f222006	Could not start Web Authentication function (Code=*xx*)
	The Web authentication functionality could not start. *xx*: Cause code (information for vendor analysis) [Action] Use the `reload` operation command to restart the Switch.			

- FATAL information

Table 2-38 Switch FATAL information when the event location is CERTIF

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	FATAL	CERTIF	0f111011	Internal error occurred (Code=*xx*)
	When using the MAC authentication functionality, an internal error occurred. *xx*: Cause code (information for vendor analysis) [Action] None (The Switch automatically restarts.)			
2	FATAL	CERTIF	0f111014	Failed to *<xxxx>* driver's filter (Code=x, ethernet *<IF#>*)
	When using the MAC authentication functionality, the driver filter control failed. *<xxxx>*: Set or unset x: Cause code (information for vendor analysis) *<IF#>*: Interface port number [Action] None (The Switch automatically restarts.)			
3	FATAL	CERTIF	0f111021	Failed to control timer function (Code=*xx*)
	When using the MAC authentication functionality, the timer functionality control failed. *xx*: Cause code (information for vendor analysis) [Action] None (The Switch automatically restarts.)			
4	FATAL	CERTIF	0f121011	Internal error occurred (Code=*xx*)
	When using the RADIUS authentication functionality, an internal error occurred. *xx*: Cause code (information for vendor analysis) [Action] None (The Switch automatically restarts.)			
5	FATAL	CERTIF	0f121021	Failed to control timer function (Code=*xx*)
	When using the Web authentication functionality, the timer functionality control failed. *xx*: Cause code (information for vendor analysis) [Action] None (The Switch automatically restarts.)			

2.4.6 Event location = HTTPD

The following tables describe Switch failure and event information when the event location is HTTPD.

- ERROR information

Table 2-39 Switch ERROR information when the event location is HTTPD

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	ERROR	HTTPD	32300001	HTTP server initialization failed
	The HTTP server failed to be initialized. [Action] The SSL certificate and private key are incorrect. Obtain the correct SSL certificate and private key, and then reinstall them to the Switch.			

- FATAL information

Table 2-40 Switch FATAL information when the event location is HTTPD

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	FATAL	HTTPD	32100002	HTTP server task Suspended: *xxxxxxxx*
	Tasks are suspended on the HTTP server. *xxxxxxxx*: Cause information (information for vendor analysis) [Action] None (The Switch automatically restarts.)			

2.4.7 Event location = QOS

The following tables describe Switch failure and event information when the event location is `QOS`.

- `WARN` information

Table 2-41 Switch WARN information when the event location is QOS

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	WARN	QOS		Port *<IF#>* Unable to use traffic-shape rate feature because a value-exceeding setting range was specified
	Port bandwidth control is not available because a value outside the valid setting range (usable line-speed) was specified. *<IF#>*: Interface port number [Action] Change the bandwidth to inside the setting range. For details about the valid setting range, see the descriptions of the `rate` parameter under traffic-shape rate in *Configuration Command Reference*.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
2	WARN	QOS		Port <*IF#*> Port half duplex does not support the traffic-shape rate feature.
	Port bandwidth control is not available for half-duplex lines. <*IF#*>: Interface port number [Action] Do either of the following: 1. If port bandwidth control is to be used, switch to a full-duplex line. 2. If a half-duplex line is to be used, delete port bandwidth control by using the configuration command `no traffic-shape rate`.			
3	WARN	QOS		Port <*IF#*> Unable to use WFQ feature because the total value of minimum rate exceeds the maximum rate of the port.
	Scheduling modes that include WFQ are not available because the total value of the minimum guaranteed bandwidths (min-rate) exceeds the maximum send bandwidth. <*IF#*>: Interface port number [Action] Use the `qos-queue-list` configuration command to adjust the total value of the minimum guaranteed bandwidths so that the total is equal to or lower than the maximum send bandwidth.			
4	WARN	QOS		Port <*IF#*> Port half duplex does not support the WFQ feature
	The scheduling mode that includes WFQ is not available for half-duplex lines. <*IF#*>: Interface port number [Action] Do either of the following: 1. If WFQ is to be used in the scheduling mode, switch to a full-duplex line. 2. If a half-duplex line is to be used, switch to a scheduling mode that does not include WFQ by using the configuration commands `qos-queue-group` and `qos-queue-list`.			
5	WARN	QOS		Port <*IF#*> Relations between traffic-shape rate and scheduling mode are inconsistent.
	The port bandwidth control settings do not match the scheduling mode settings. When using port bandwidth control, you can only specify PQ for scheduling mode. <*IF#*>: Interface port number [Action] Do either of the following: 1. To use port bandwidth control, change the scheduling mode to PQ by using the `qos-queue-group` and `qos-queue-list` configuration commands. 2. To use a scheduling mode other than PQ, delete the port bandwidth control setting by using the `no traffic-shape rate` configuration command.			

- `CRITC` information

Table 2-42 Switch CRITC information when the event location is QOS

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	CRITC	QOS	09200001	Software error
	Software error (semaphore ID error) ● The creation of the semaphore ID failed when initializing during Switch startup. ● The acquisition of the semaphore ID failed when creating switch operation configurations. [Action] Use the `reload` operation command to restart the Switch.			

- FATAL information

Table 2-43 Switch FATAL information when the event location is QOS

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	FATAL	QOS	09100000	Swd Configuration Error *<comment>*
	The QoS configuration could not be set for the hardware controller. *<comment>*: Cause information (information for vendor analysis) [Action] None (The Switch automatically restarts.)			
2	FATAL	QOS	09100010 09100011	Internal error occurred *<IF#>* (code=*xxxx*)
	The QoS configuration could not be set for the hardware controller. ● 0910010: For legacy shaping ● 0910011: For port shaping *<IF#>*: Interface port number *xxxx*: Error code (information for vendor analysis) [Action] None (The Switch automatically restarts.)			

2.4.8 Event location = FIELD

The following table describes Switch failure and event information when the event location is FIELD.

- FATAL information

Table 2-44 Switch FATAL information when the event location is FIELD

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	FATAL	FIELD	0c100000	Swd Configuration Error *<comment>*
	The configuration of a filter could not be set for the hardware controller. *<comment>*: Cause information (information for vendor analysis) [Action] None (The Switch automatically restarts.)			

2.4.9 Event location = SWOL

The following table describes Switch failure and event information when the event location is SWOL.

- INFO information

Table 2-45 Switch INFO information when the event location is SWOL

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	SWOL		Login incorrect [User reject] USER=*xxxx*
	User authentication for Secure Wake on LAN failed due to an invalid user name and password. USER=*xxxx*: User name [Action] None			
2	INFO	SWOL		Login incorrect [Server busy] USER=*xxxx*
	User authentication for Secure Wake on LAN failed because the user management area does not have sufficient capacity. USER=*xxxx*: User name [Action] Wait a moment, and then retry the operation.			
3	INFO	SWOL		Device not found DEVICENAME=*xxxx*
	The terminal selected by a request is not registered in the database. DEVICENAME=*xxxx*: Terminal name [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
4	INFO	SWOL		User entry expired USER=*xxxx*
	A user entry shifted to the expiration phase because a user timed out during user authentication on Secure Wake on LAN. USER=*xxxx*: User name [Action] None			
5	INFO	SWOL		Magic packet processing was completed USER=*xxxx* MAC=*xxxx.xxxx.xxxx*
	Start command sending succeeded USER=*xxxx*: User name MAC=*xxxx.xxxx.xxxx*: Terminal MAC address [Action] None			
6	INFO	SWOL		Configuration of DHCP snooping is not set.
	The DHCP snooping configuration is not set. [Action] To monitor the status of terminals to which DHCP assigns IP addresses, set the DHCP snooping configuration.			

2.4.10 Event location = ECO

The following table describes Switch failure and event information when the event location is `ECO`.

- `INFO` information

Table 2-46 Switch INFO information when the event location is ECO

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	ECO		The system changes to the schedule power control because it became the schedule time.
	The scheduled time for power-control has been reached. [Action] None			
2	INFO	ECO		The system changes from the schedule power control because it ended the schedule time.
	The scheduled time for power-control has ended. [Action] None			

2.5 Port

2.5.1 Event location = PORT

The following table describes switch failure and event information when the event location is PORT.

- INFO information

Table 2-47 Switch INFO information when the event location is PORT

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	PORT		GigabitEthernet <IF#> Link Up/Speed 1000M-Full (auto)
	Gigabit Ethernet port <IF#> is in the link-up state at 1000 Mbps full duplex (by automatic negotiation). <IF#>: : Interface port number [Action] None			
2	INFO	PORT		GigabitEthernet <IF#> Link Up/Speed 1000M-Full
	Gigabit Ethernet port <IF#> is in the link-up state at 1000 Mbps full duplex (by fixed settings). <IF#>: : Interface port number [Action] None			
3	INFO	PORT		GigabitEthernet <IF#> Link Up/Speed 100M-Full (auto)
	Gigabit Ethernet port <IF#> is in the link-up state at 100 Mbps full duplex (by automatic negotiation settings). <IF#>: : Interface port number [Action] None			
4	INFO	PORT		GigabitEthernet <IF#> Link Up/Speed 100M-Full
	Gigabit Ethernet port <IF#> is in the link-up state at 100 Mbps full duplex (by fixed settings). <IF#>: : Interface port number [Action] None			
5	INFO	PORT		GigabitEthernet <IF#> Link Up/Speed 100M-Half (auto)
	Gigabit Ethernet port <IF#> is in the link-up state at 100 Mbps half duplex (by automatic negotiation settings). <IF#>: Interface port number [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
6	INFO	PORT		GigabitEthernet <*IF#*> Link Up/Speed 100M-Half
	Gigabit Ethernet port <*IF#*> is in the link-up state at 100 Mbps half duplex (by fixed settings). <*IF#*>: Interface port number [Action] None			
7	INFO	PORT		GigabitEthernet <*IF#*> Link Up/Speed 10M-Full (auto)
	Gigabit Ethernet port <*IF#*> is in the link-up state at 10 Mbps full duplex (by automatic negotiation settings). <*IF#*>: Interface port number [Action] None			
8	INFO	PORT		GigabitEthernet <*IF#*> Link Up/Speed 10M-Full
	Gigabit Ethernet port <*IF#*> is in the link-up state at 10 Mbps full duplex (by fixed settings). <*IF#*>: Interface port number [Action] None			
9	INFO	PORT		GigabitEthernet <*IF#*> Link Up/Speed 10M-Half (auto)
	Gigabit Ethernet port <*IF#*> is in the link-up state at 10 Mbps half duplex (by automatic negotiation settings). <*IF#*>: Interface port number [Action] None			
10	INFO	PORT		GigabitEthernet <*IF#*> Link Up/Speed 10M-Half
	Gigabit Ethernet port <*IF#*> is in the link-up state at 10 Mbps half duplex (by fixed settings). <*IF#*>: Interface port number [Action] None			
11	INFO	PORT		FastEthernet <*IF#*> Link Up/Speed 100M-Full (auto) [AX1250S][AX1240S]
	Fast Ethernet port <*IF#*> is in the link-up state at 100 Mbps full duplex (by automatic negotiation settings). <*IF#*>: Interface port number [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
12	INFO	PORT		FastEthernet <*IF#*> Link Up/Speed 100M-Full [AX1250S] [AX1240S]
	Fast Ethernet port <*IF#*> is in the link-up state at 100 Mbps full duplex (by fixed settings). <*IF#*>: Interface port number [Action] None.			
13	INFO	PORT		FastEthernet <*IF#*> Link Up/Speed 100M-Half(auto) [AX1250S][AX1240S]
	Fast Ethernet port <*IF#*> is in the link-up state at 100 Mbps half duplex (by automatic negotiation settings). <*IF#*>: Interface port number [Action] None			
14	INFO	PORT		FastEthernet <*IF#*> Link Up/Speed 100M-Half [AX1250S][AX1240S]
	Fast Ethernet port <*IF#*> is in the link-up state at 100 Mbps half duplex (by fixed settings). <*IF#*>: Interface port number [Action] None			
15	INFO	PORT		FastEthernet <*IF#*> Link Up/Speed 10M-Full (auto) [AX1250S] [AX1240S]
	Fast Ethernet port <*IF#*> is in the link-up state at 10 Mbps full duplex (by automatic negotiation settings). <*IF#*>: Interface port number [Action] None			
16	INFO	PORT		FastEthernet <*IF#*> Link Up/Speed 10M-Full [AX1250S] [AX1240S]
	Gigabit Ethernet port <*IF#*> is in the link-up state at 10 Mbps full duplex (by fixed settings). <*IF#*>: Interface port number [Action] None			
17	INFO	PORT		FastEthernet <*IF#*> Link Up/Speed 10M-Half(auto) [AX1250S] [AX1240S]
	Fast Ethernet port <*IF#*> is in the link-up state at 10 Mbps half duplex (by automatic negotiation settings). <*IF#*>: Interface port number [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
18	INFO	PORT		FastEthernet <*IF#*> Link Up/Speed 10M-Half [AX1250S] [AX1240S]
	Fast Ethernet port <*IF#*> is in the link-up state at 10 Mbps half duplex (by fixed settings). <*IF#*>: Interface port number [Action] None			
19	INFO	PORT		GigabitEthernet <*IF#*> Link Up/Speed UnKnown
	The speed of gigabit Ethernet port <*IF#*> could not be identified. <*IF#*>: Interface port number [Action] None			
20	INFO	PORT		FastEthernet <*IF#*> Link Up/Speed UnKnown [AX1250S] [AX1240S]
	The speed of Fast Ethernet port <*IF#*> could not be identified. <*IF#*>: Interface port number [Action] None			
21	INFO	PORT		GigabitEthernet <*IF#*> Link Down
	Gigabit Ethernet port <*IF#*> is in the link-down state. <*IF#*>: Interface port number [Action] None			
22	INFO	PORT		FastEthernet <*IF#*> Link Down [AX1250S] [AX1240S]
	Fast Ethernet port <*IF#*> is in the link-down state. <*IF#*>: Interface port number [Action] None			
23	INFO	PORT		<*IF#*> is enabled.
	A port is enabled. <*IF#*>: Interface port number [Action] None			
24	INFO	PORT		<*IF#*> is disabled.
	A port is disabled. <*IF#*>: Interface port number [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
25	INFO	PORT		Port <*IF#*> activated
	A port was specified to be active. <*IF#*>: Interface port number [Action] None			
26	INFO	PORT		Port <*IF#*> inactivated
	A port was specified to be inactive. <*IF#*>: Interface port number [Action] None			
27	INFO	PORT		Active Medium Change Notification (<*IF#*>, RJ45)
	The media type for the interface port was switched to RJ45. <*IF#*>: Interface port number [Action] None			
28	INFO	PORT		Active Medium Change Notification (<*IF#*>, SFP)
	The media type for the interface port was switched to SFP. <*IF#*>: Interface port number [Action] None			

- WARN information

Table 2-48 Switch WARN information when the event location is PORT

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	WARN	PORT		<*IF#*> speed setting failed
	An attempt to set the speed failed. <*IF#*>: Interface port number [Action] Retry the operation.			
2	WARN	PORT		<*IF#*> duplex setting failed
	An attempt to set the duplex failed. <*IF#*>: Interface port number [Action] Retry the operation.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
3	WARN	PORT		<IF#> flowcontrol setting failed
	An attempt to set the flow control failed. <IF#>: Interface port number [Action] Retry the operation.			
4	WARN	PORT		<IF#> mdix setting failed
	An attempt to set MDIX failed. <IF#>: Interface port number [Action] Retry the operation.			
5	WARN	PORT		Media-type setting failed
	An attempt to set the media-type configuration failed. [Action] Retry the operation.			
6	WARN	PORT		Failed Interface MTU setting
	An attempt to set the MTU specified in the interface failed. [Action] Retry the operation.			
7	WARN	PORT		Failed System MTU setting
	An attempt to set the system MTU failed. [Action] Retry the operation.			
8	WARN	PORT		Failed setting Medium Type
	An attempt to set the media type failed. [Action] Retry the operation.			
9	WARN	PORT		PLM : Config setting Error
	An attempt to set the port failed. [Action] Retry the operation.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
10	WARN	PORT		<*xxxxxxxx*> Message Queue Receive Error Errno: *xxxx*
	An error occurred when receiving a message between tasks. <*xxxxxxxx*>: Location where the error was detected (information for vendor analysis) *xxxx*: Cause code (information for vendor analysis) [Action] Use the `reload` operation command to restart the Switch.			
11	WARN	PORT		<*xxxxxxxx*> Message Queue Send Error Errno: *xxxx*
	An error occurred when sending a message between tasks. <*xxxxxxxx*>: Location where the error was detected (information for vendor analysis) *xxxx*: Cause code (information for vendor analysis) [Action] Use the `reload` operation command to restart the Switch.			
12	WARN	PORT		<*xxxxxxxx*> : Failed SFP *xx* Tx Enable <*xxxxxxxx*> : Failed SFP *xx* Tx Disable
	SFP transmission control failed <*xxxxxxxx*>: Location where the error was detected (information for vendor analysis) [Action] Use the `reload` operation command to restart the Switch.			
13	WARN	PORT		Failed Register medium report
	An attempt to register a report functionality for a media type failed. [Action] Use the `reload` operation command to restart the Switch.			
14	WARN	PORT		<*xxxxxxxx*> Failed Register a handler <*xxxxxxxx*> Failed Register a handler (Linkdeb)
	An attempt to register a report functionality failed. <*xxxxxxxx*>: Location where the error was detected (information for vendor analysis) [Action] Use the `reload` operation command to restart the Switch.			
15	WARN	PORT		STORM : Port <*IF#*> inactivated because of broadcast storm detection
	A port was deactivated because a broadcast storm was detected. <*IF#*>: Interface port number [Action] After recovering from the storm, use the `activate` operation command to change the port status to active.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
16	WARN	PORT		STORM : Port <*IF#*> broadcast storm detected
	A broadcast storm was detected. <*IF#*>: Interface port number [Action] None			
17	WARN	PORT		STORM : Port <*IF#*> broadcast storm recovered
	The system has recovered from a broadcast storm. <*IF#*>: Interface port number [Action] None			
18	WARN	PORT		STORM : Port <*IF#*> inactivated because of multicast storm detection
	A port was deactivated because a multicast storm was detected. <*IF#*>: Interface port number [Action] After recovering from the storm, use the `activate` operation command to change the port status to active.			
19	WARN	PORT		STORM : Port <*IF#*> multicast storm detected
	A multicast storm was detected. <*IF#*>: Interface port number [Action] None			
20	WARN	PORT		STORM : Port <*IF#*> multicast storm recovered
	The system has recovered from a multicast storm. <*IF#*>: Interface port number [Action] None			
21	WARN	PORT		STORM : Port <*IF#*> inactivated because of unicast storm detection
	A port was deactivated because a unicast storm was detected. <*IF#*>: Interface port number [Action] After recovering from the storm, use the `activate` operation command to change the port status to active.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
22	WARN	PORT		STORM : Port <*IF#*> unicast storm detected
	A unicast storm was detected. <*IF#*>: Interface port number [Action] None			
23	WARN	PORT		STORM : Port <*IF#*> unicast storm recovered
	The system has recovered from a unicast storm. <*IF#*>: Interface port number [Action] None			

- `ERROR` information

Table 2-49 Switch ERROR information when the event location is PORT

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	ERROR	PORT	1e331000	Failed Pause MAC Address setting
	An attempt to set a MAC address for a pause failed. [Action] Use the `reload` operation command to restart the Switch.			

- FATAL information

Table 2-50 Switch FATAL information when the event location is PORT

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	FATAL	PORT	1e115000 1e125000 1e135000 1e135001 1e145000	<*xxxxxxxx*> WDT Time Out
	A watchdog timeout occurred. <*xxxxxxxx*>: Location where the error was detected (information for vendor analysis) [Action] None (The Switch automatically restarts.)			

2.5.2 Event location = SFP

The following table describes Switch failure and event information when the event location is SFP.

- INFO information

Table 2-51 Switch INFO information when the event location is SFP

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	SFP		Detect to mount transceiver module [UNKNOWN] on the port (<*IF#*>)
	An SFP module [Unknown] is inserted in the port. <*IF#*>: Interface port number [Action] Make sure that the SFP module is valid, and then insert it again. The valid SFP module might not be recognized due to a loose connection. In this case, re-insert it.			
2	INFO	SFP		Detect to mount transceiver module [1000BASE-SX] on the port (<*IF#*>)
	An SFP module [1000BASE-SX] is inserted in the port. <*IF#*>: Interface port number [Action] None			
3	INFO	SFP		Detect to mount transceiver module [1000BASE-LX] on the port (<*IF#*>)
	An SFP module [1000BASE-LX] is inserted in the port. <*IF#*>: Interface port number [Action] None			
4	INFO	SFP		Detect to mount transceiver module [1000BASE-LH] on the port (<*IF#*>)
	An SFP module [1000BASE-LH] is inserted in the port. <*IF#*>: Interface port number [Action] None			
5	INFO	SFP		Detect to mount transceiver module [1000BASE-SX2] on the port (<*IF#*>)
	An SFP module [1000BASE-SX2] is inserted in the port. <*IF#*>: Interface port number [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
6	INFO	SFP		Detect to mount transceiver module [1000BASE-BX10-D] on the port (<*IF#*>)
	An SFP module [1000BASE-BX10-D] is inserted in the port. <*IF#*>: Interface port number [Action] None			
7	INFO	SFP		Detect to mount transceiver module [1000BASE-BX10-U] on the port (<*IF#*>)
	An SFP module [1000BASE-BX10-U] is inserted in the port. <*IF#*>: Interface port number [Action] None			
8	INFO	SFP		Detect to mount transceiver module [1000BASE-BX40-D] on the port (<*IF#*>)
	An SFP module [1000BASE-BX40-D] is inserted in the port. <*IF#*>: Interface port number [Action] None			
9	INFO	SFP		Detect to mount transceiver module [1000BASE-BX40-U] on the port (<*IF#*>)
	An SFP module [1000BASE-BX40-U] is inserted in the port. <*IF#*>: Interface port number [Action] None			
10	INFO	SFP		Detect to mount transceiver module [100BASE-FX] on the port (<*IF#*>)
	An SFP module [100BASE-FX] is inserted in the port. <*IF#*>: Interface port number [Action] None			
11	INFO	SFP		Detect to unmount transceiver module on the port (<*IF#*>)
	An SFP module was removed from a port. <*IF#*>: Interface port number [Action] None			

2.5.3 Event location = FABRIC

The following tables describe Switch failure and event information when the event location is `FABRIC`.

- `INFO` information

Table 2-52 Switch INFO information when the event location is FABRIC

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	FABRIC		b-driver: Switch device driver succeeded in memory restoration (*<type>*)
	Recovery from a parity error succeeded *<type>*: "L2_ENTRY," "L2MC" [Action] None			
2	INFO	FABRIC		Switch device driver detected a fault (*<IF#>*) [*<code>*]
	An error was detected in the device driver, and recovery processing was performed. *<IF#>*: Interface port number *<code>*: Error code (information for vendor analysis) [Action] If an error is detected repeatedly, check the following: ● Check and reconnect the cable. ● If the cable is normal, check the destination device.			

- `WARN` information

Table 2-53 Switch WARN information when the event location is FABRIC

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	WARN	FABRIC		b-driver: *xxxx*
	An error was detected in the device driver. *xxxx*: Error message (information for vendor analysis) [Action] Use the `reload` operation command to restart the Switch.			

- `ERROR` information

Table 2-54 Switch ERROR information when the event location is FABRIC

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	ERROR	FABRIC	1d3f0010	b-driver: *xxxx*
	An error was detected in the device driver. *xxxx*: Error message (information for vendor analysis) [Action] Replace the Switch.			

- `CRITC` information

Table 2-55 Switch CRITC information when the event location is FABRIC

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	CRITC	FABRIC	1d200000	Switch Device Configuration Unmatch
	The Switch type definition does not match the number of recognized switches. [Action] Use the `reload` operation command to restart the Switch.			
2	CRITC	FABRIC	1d2f0000	Switch Device Driver Startup Sequence Failure
	An attempt to start the device driver failed. [Action] Use the `reload` operation command to restart the Switch.			
3	CRITC	FABRIC	1d290000	Failed to set STG *<STG#>* (rv=*xx*)
	Configuration for the hardware failed. *<STG#>*: Used for analysis by the manufacturer *xx*: Used for analysis by the manufacturer [Action] Restart the Switch by executing the `reload` operation command, or by turning it off and then on.			

- FATAL information

Table 2-56 Switch FATAL information when the event location is FABRIC

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	FATAL	FABRIC	1d100000	Switch Device Configuration Unmatch
	The Switch type definition does not match the number of recognized switches. [Action] None (The Switch automatically restarts.)			
2	FATAL	FABRIC	1d100001	Switch Device Driver Error (returned by BCMX attach x: ...)
	The API cannot be controlled because an error occurred when attaching the device driver. [Action] None (The Switch automatically restarts.)			
3	FATAL	FABRIC	1d100002	Switch Device Driver Startup Sequence Failure
	The device driver failed to start. [Action] None (The Switch automatically restarts.)			
4	FATAL	FABRIC	1d100003	Switch Device Driver Startup Sequence Time-Out
	A timeout occurred during device driver startup. [Action] None (The Switch automatically restarts.)			
5	FATAL	FABRIC	1d100004	b-driver: Switch device driver detected a fault.(*<type>*) *<code>*
	A failure was detected when the threshold was exceeded. *<type>*: "L2_ENTRY", "L2MC" "IPIPE", or "MMU" *<code>*: Error code (information for vendor analysis) [Action] None (The Switch automatically restarts.)			
6	FATAL	FABRIC	1d100005	b-driver: Parity error occurred (*<type>*)
	A parity error was detected (not "L2_ENTRY", "L2MC", or "CELLCRCERROR"). *<type>*: "IPIPE," "MMU" [Action] None (The Switch automatically restarts.)			
7	FATAL	FABRIC	1d100006	b-driver: Switch device driver failed in memory restoration (*<type>*)*<code>*
	Recovery from the parity error failed *<type>*: "L2_ENTRY" *<code>*: Error code (information for vendor analysis) [Action] None (The Switch automatically restarts.)			

2.5.4 Event location = POE [AX2200S] [AX1240S]

The following tables describe Switch failure and event information when the event location is POE.

- INFO information

Table 2-57 Switch INFO information when the event location is POE

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	POE		Initialization PoE configuration
	The PoE configuration will be set. [Action] None			
2	INFO	POE		<*IF#*> Unable to supply power by the power shortage [AX1240S]
	Power cannot be supplied because there is not enough power to power all the switches. [Action] To supply power to the port, check Threshold and Allocate by using the show power inline operation command, and then decrease the number of switches receiving the power so that Allocate goes below Threshold. Alternatively, change the priority by using the power inline configuration command.			
3	INFO	POE		PoE Firmware Download Successful (X) [AX2200S]
	The PoE controller download ended normally. (X): 1 (controller 1), 2 (controller 2) [Action] None			

- WARN information

Table 2-58 Switch WARN information when the event location is POE

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	WARN	POE		<*IF#*> Supplying power was stopped by the overload detection.
	The power supply was stopped because a power overload was detected. <*IF#*>: Interface port number [Action] Check the devices receiving the power. If devices to which PoE power can be supplied are connected, use the power inline configuration command to disable PoE on the port.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
2	WARN	POE		*<IF#>* Supplying power was stopped by the thermal shutdown.
	The power supply was stopped because a temperature anomaly was detected on a PoE controller. *<IF#>*: Interface port number [Action] Check the installation environment of the switch, and then connect it again.			
3	WARN	POE		*<IF#>* Supplying power was stopped by the PD disorder. (*xxxx*)
	The power supply was stopped because a failure was detected on a Switch receiving power. *<IF#>*: Interface port number *xxxx*: Cause for stopping power supply [Action] Try to execute the `activate power inline` operation command. If the power supply does not restart, check the Switch receiving the power and the cables, and then reconnect the cables to the Switch.			

- `CRITC` information

Table 2-59 Switch CRITC information when the event location is POE

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	CRITC	POE	2C200201	PoE controller not found
	The PoE controller could not be found. The PoE functionality cannot be used. [Action] Use the `reload` operation command to restart the Switch.			

- FATAL information

Table 2-60 Switch FATAL information when the event location is POE

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	FATAL	POE	2C100301	PoE controller wake up failed (X) [AX2200S]
	The PoE controller failed to start. (X): 1 (controller 1), 2 (controller 2) [Action] None (The Switch automatically restarts.)			
2	FATAL	POE	2C100301	PoE controller wake up failed [AX1240S]
	The PoE controller failed to start. [Action] None (The Switch automatically restarts.)			
3	FATAL	POE	2C100302	Init controller failed
	An attempt to set up the PoE configuration failed. [Action] None (The Switch automatically restarts.)			
4	FATAL	POE	2C100303	PoE controller access failed (*xxxx*)
	An attempt to access to the PoE controller failed. (*xxxx*): Cause code (information for vendor analysis) [Action] None (The Switch automatically restarts.)			

2.5.5 Event location = ULR

The following table describes switch failure and event information when the event location is ULR.

- INFO information

Table 2-61 Switch INFO information when the event location is ULR

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	ULR		: Change to secondary Port <*IF#*> from primary port <*IF#*>
	The secondary port became an active port because a link failure occurred on the primary port. <*IF#*>: Interface port number [Action] Check the failure in the primary port.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
2	INFO	ULR		: Change to secondary port *<IF#>* from primary ChGr *<Channel group#>*
	The secondary port became an active port because a link failure occurred on the primary port. *<IF#>*: Interface port number *<Channel group#>*: Channel group number [Action] Check the failure in the primary port.			
3	INFO	ULR		: Change to secondary ChGr *<Channel group#>* from primary port *<IF#>*
	The secondary port became an active port because a link failure occurred on the primary port. *<Channel group#>*: Channel group number *<IF#>*: Interface port number [Action] Check the failure in the primary port.			
4	INFO	ULR		: Change to secondary ChGr *<Channel group#>* from primary ChGr *<Channel group#>*
	The secondary port became an active port because a link failure occurred on the primary port. *<Channel group#>*: Channel group number [Action] Check the failure in the primary port.			
5	INFO	ULR		: Change to primary port *<IF#>* from secondary port *<IF#>*.
	The primary port became an active port because a link failure occurred on the secondary port. *<IF#>*: Interface port number [Action] Check the failure in the secondary port.			
6	INFO	ULR		: Change to primary port *<IF#>* from secondary ChGr *<Channel group#>*
	The primary port became an active port because a link failure occurred on the secondary port. *<IF#>*: Interface port number *<Channel group#>*: Channel group number [Action] Check the failure in the secondary port.			
7	INFO	ULR		: Change to primary ChGr *<Channel group#>* from secondary port *<IF#>*.
	The primary port became an active port because a link failure occurred on the secondary port. *<Channel group#>*: Channel group number *<IF#>*: Interface port number [Action] Check the failure in the secondary port.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
8	INFO	ULR		: Change to primary ChGr *<Channel group#>* from secondary ChGr *<Channel group#>*
	The primary port became an active port because a link failure occurred on the secondary port. *<Channel group#>*: Channel group number [Action] Check the failure in the secondary port.			
9	INFO	ULR		: Change to secondary port *<IF#>* from primary port *<IF#>* forced
	Manual switching from the primary port to the secondary port was executed. *<IF#>*: Interface port number [Action] None			
10	INFO	ULR		: Change to secondary port *<IF#>* from primary ChGr *<Channel group#>* forced
	Manual switching from the primary port to the secondary port was executed. *<IF#>*: Interface port number *<Channel group#>*: Channel group number [Action] None			
11	INFO	ULR		: Change to secondary ChGr *<Channel group#>* from primary port *<IF#>* forced.
	Manual switching from the primary port to the secondary port was executed. *<Channel group#>*: Channel group number *<IF#>*: Interface port number [Action] None			
12	INFO	ULR		: Change to secondary ChGr *<Channel group#>* from primary ChGr *<Channel group#>* forced.
	Manual switching from the primary port to the secondary port was executed. *<Channel group#>*: Channel group number [Action] None			
13	INFO	ULR		: Change to primary port *<IF#>* from secondary port *<IF#>* forced
	Manual switching from the secondary port to the primary port was executed. *<IF#>*: Interface port number [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
14	INFO	ULR		: Change to primary port <*IF#*> from secondary ChGr <*Channel group#*> forced
	Manual switching from the secondary port to the primary port was executed. <*IF#*>: Interface port number <*Channel group#*>: Channel group number [Action] None			
15	INFO	ULR		: Change to primary ChGr <*Channel group#*> from secondary port <*IF#*> forced
	Manual switching from the secondary port to the primary port was executed. <*Channel group#*>: Channel group number <*IF#*>: Interface port number [Action] None			
16	INFO	ULR		: Change to primary ChGr <*Channel group#*> from secondary ChGr <*Channel group#*> forced
	Manual switching from the secondary port to the primary port was executed. <*Channel group#*>: Channel group number [Action] None			
17	INFO	ULR		: Mac-address-table update frame cannot be sent on the port <*IF#*> because capacity was exceeded.
	A MAC address update frame cannot be sent because the number of MAC addresses that were sent exceeds the maximum (1,024). <*IF#*>: Interface port number [Action] None			
18	INFO	ULR		: Mac-address-table update frame cannot be sent on the ChGr <*Channel group#*> because capacity was exceeded.
	A MAC address update frame cannot be sent because the number of MAC addresses that were sent exceeds the maximum (1,024). <*Channel group#*>: Channel group number [Action] None.			

- WARN information

Table 2-62 Switch WARN information when the event location is ULR

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	WARN	ULR		: Cleared MAC Address Table entry
	The MAC address table was cleared because a flush control frame was received. [Action] None			

2.6 Switch

2.6.1 Event location = ROM

The following tables describe Switch failure and event information when the event location is `ROM`.

- `WARN` information

Table 2-63 Switch WARN information when the event location is ROM

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	WARN	ROM		FROM write timeout Addr=*xxxxxxxx*, getData=*xx*
	An error occurred in an attempt to write to flash memory. Addr=*xxxxxxxx*,getData=*xx*: Location where the error was detected (information for vendor analysis) [Action] Re-execute the command.			
2	WARN	ROM		FROM erase timeout Addr=*xxxxxxxx*
	An error occurred in an attempt to erase the flash memory. Addr=*xxxxxxxx*: Location where the error was detected (information for vendor analysis) [Action] Re-execute the command.			
3	WARN	ROM		Flash format complete
	Initialization of the flash memory file system succeeded (This information is collected even if the `format flash` operation command succeeded.) [Action] None			
4	WARN	ROM		Flash format error detail=*xxxx*
	Initialization of the flash memory file system failed detail=*xxxx*: Cause code (information for vendor analysis) [Action] Re-execute the `format flash` operation command. If this message is still seen, the flash memory might be corrupted.			
5	WARN	ROM		Flash format task not ended detail=*xxxx*
	The initialization of the flash memory file system was not completed. detail=*xxxx*: Cause code (information for vendor analysis) [Action] Re-execute the `format flash` operation command. If this message is still seen, the flash memory might be corrupted.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
6	WARN	ROM		Flash format system error(1) detail=*xxxx*
	An error occurred during the initialization of the flash memory file system. detail=*xxxx*: Cause code (information for vendor analysis) [Action] Re-execute the `format flash` operation command. If this message is still collected, the flash memory might be corrupted.			
7	WARN	ROM		Flash format system error(2) detail=*xxxx*
	An error occurred during the initialization of the flash memory file system. detail=*xxxx*: Cause code (information for vendor analysis) [Action] Re-execute the `format flash` operation command. If this message is still collected, the flash memory might be corrupted.			

- `ERROR` information

Table 2-64 Switch ERROR information when the event location is ROM

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	ERROR	ROM	29300001	Boot program check sum error
	A checksum error was detected by the boot program. [Action] Replace the Switch.			
2	ERROR	ROM	29300004	SMP Main (bootA) program check sum error
	A main program sum check error occurred. [Action] Replace the Switch.			
3	ERROR	ROM	29300007	Flash write error. addr=*xxxxxxxxxx* size=*xxxx*
	An error occurred in an attempt to write to flash memory. addr=*xxxxxxx* size=*xxxx*: Location where the error was detected (information for vendor analysis) [Action] Re-execute the command. If the error still occurs, replace the Switch.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
4	ERROR	ROM	29300008	Flash erase error. addr=*xxxxxxxxxx* size=*xxxx*
	An error occurred in an attempt to erase the flash memory. addr=*xxxxxxx* size=*xxxx*: Location where the error was detected (information for vendor analysis) [Action] Re-execute the command. If the error still occurs, replace the Switch.			
5	ERROR	ROM	29300010	The model type is not set as ROM.
	The model type is not set. [Action] Replace the Switch.			
6	ERROR	ROM	29300013	File system error
	The storage area for the flash memory configuration cannot be used. [Action] Try to execute the `format flash` operation command. If the error still occurs, the flash memory might be corrupted.			
7	ERROR	ROM	29300100	FROM write fail [cnt=*xxxxxxxx*,size=*xxxxxxxx*,err=*xxxxxxxx*]
	Writing to flash memory failed when executing the `ppupdate` or `restore` operation command. cnt=*xxxxxxxx*: Cause code (information for vendor analysis) size=*xxxxxxxx*: Cause code (information for vendor analysis) err=*xxxxxxxx*: Cause code (information for vendor analysis) [Action] Re-execute the `ppupdate` command (or, if the `restore` command was executed, re-execute the `restore` operation command). If the error still occurs, replace the Switch.			

2.6.2 Event location = RTC

The following tables describe Switch failure and event information when the event location is `RTC`.

- `WARN` information

Table 2-65 Switch WARN information when the event location is RTC

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	WARN	RTC		Battery EMPTY
	The Switch started when the RTC battery was 0 V (if the Switch started 10 or more days after the Switch power was turned off). [Action] Reset the time.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
2	WARN	RTC		Retry failure
	An attempt to access the RTC failed. [Action] None			

- `ERROR` information

Table 2-66 Switch ERROR information when the event location is RTC

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	ERROR	RTC	22300201	Initialize Failure
	An attempt to initialize the RTC failed. [Action] Use the `reload` operation command to restart the Switch.			

2.6.3 Event location = THERMO

The following tables describe Switch failure and event information when the event location is `THERMO`.

- `INFO` information

Table 2-67 Switch INFO information when the event location is THERMO

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	THERMO		An environmental level became normal.
	The external temperature that was exceeding the threshold returned to normal. [Action] None			
2	INFO	THERMO		The temperature of hardware reached the warning level (*<temperature threshold>* degree).
	The hardware temperature has exceeded the temperature set with the `system temperature-warning-level` configuration command. *<temperature threshold>*: Temperature set with the `system temperature-warning-level` configuration command (in Celsius) [Action] The temperature of the Switch has reached the specified temperature. Check the environment surrounding the Switch (condition of the fan, ventilation, existence of heat sources, etc.).			

No.	Event level	Event location	Ref. Code	Message text
	Description			
3	INFO	THERMO		The temperature of the hardware came down from the warning level.
	The hardware temperature fell 3°C below the temperature set using the `system temperature-warning-level` configuration command. [Action] None			
4	INFO	THERMO		The temperature logging can't be written.
	Writing the temperature logging information failed. [Action] None.			
5	INFO	THERMO		The average temperature of the hardware reached the warning level. (*<temperature>* degree/*<temperature threshold>* degree *<days>* day(s))
	The average hardware temperature has exceeded the temperature set using the `system temperature-warning-level average` configuration command. *<temperature>*: Average switch temperature (in Celsius) *<temperature threshold>*: Temperature set using the `system temperature-warning-average average` configuration command (in Celsius) *<days>*: Average temperature calculation period [Action] The average temperature of the switch has reached the specified average temperature. Check the environment surrounding the switch (condition of the fan, ventilation, possible heat sources, etc.).			

- `WARN` information

Table 2-68 Switch WARN information when the event location is THERMO

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	WARN	THERMO		Data of accumulation operation time fail
	The data for the accumulation operation time is corrupted. [Action] None			
2	WARN	THERMO		Accumulation operation time was initialized
	The accumulation operation time was reset to zero because the accumulated operation time was corrupted. [Action] None			

- `ERROR` information

Table 2-69 Switch ERROR information when the event location is THERMO

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	ERROR	THERMO	23300301	Temperature exceeds the threshold
	The external temperature exceeds the threshold. [Action] Check and, if necessary, improve the environment, such as the room temperature around the Switches.			
2	ERROR	THERMO	23300303	Temperature sensor re-try failure
	The temperature sensor's attempt to retry failed. [Action] Use the `reload` operation command to restart the Switch.			
3	ERROR	THERMO	23300305	Set Configuration Failure
	Verification failed when setting the configuration to the temperature sensor register at Switch startup. [Action] Use the `reload` operation command to restart the Switch.			

2.6.4 Event location = SDCARD

The following tables describe Switch failure and event information when the event location is `SDCARD`.

- `INFO` information

Table 2-70 Switch INFO information when the event location is SDCARD

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	SDCARD		Can't update software [Hardware rev.*xx*]
	The update cannot be performed using this software. The hardware revision number of the Switch is *xx*. [Action] Check the hardware revision number of the target Switch by using the `show version` operation command.			

- `WARN` information

Table 2-71 Switch WARN information when the event location is SDCARD

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	WARN	SDCARD		Non-supported File System
	The file system of the inserted medium is neither FAT12 nor FAT16. [Action] Reformat the media in either FAT12 or FAT16.			

- `ERROR` information

Table 2-72 Switch ERROR information when the event location is SDCARD

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	ERROR	SDCARD	26300201	Create Device Fail
	The generation of a memory card access device failed when initializing during Switch startup. [Action] Use the `reload` operation command to restart the Switch.			
2	ERROR	SDCARD	26300202	Could Not Create Semaphore
	The generation of a semaphore failed when initializing during Switch startup. [Action] Use the `reload` operation command to restart the Switch.			
3	ERROR	SDCARD	26300203	Could Not Create Message Que
	The generation of a message queue failed when initializing during Switch startup. [Action] Use the `reload` operation command to restart the Switch.			
4	ERROR	SDCARD	26300204	Could not Create Task
	The generation of a task failed when initializing during Switch startup. [Action] Use the `reload` operation command to restart the Switch.			

2.6.5 Event location = FAN [AX2200S] [AX1240S]

The following table describes switch failure and event information when the event location is FAN.

- INFO information

Table 2-73 Switch INFO information when the event location is FAN

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	FAN		Recover of FAN Alarm
	The fans recovered from a stop, and both FAN1 and FAN2 work normally. [Action] None			
2	INFO	FAN		FAN stopped by the system FAN control
	The fans were stopped by temperature monitoring. [Action] None			
3	INFO	FAN		FAN started by the system FAN control
	The fans were started by temperature monitoring. [Action] None			

- ERROR information

Table 2-74 Switch ERROR information when the event location is FAN

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	ERROR	FAN	2b340001	Alarm of FAN detected [AX2200S]
	A FAN stop was detected. [Action] Replace the switch.			
2	ERROR	FAN	2b340001	Alarm of FAN1 detected [AX1240S]
	A FAN1 stop was detected. [Action] Replace the Switch.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
3	ERROR	FAN	2b341001	Alarm of FAN2 detected
	A FAN2 stop was detected. [Action] Replace the Switch.			

2.6.6 Event location = LED

The following table describes Switch failure and event information when the event location is LED.

- INFO information

Table 2-75 Switch INFO information when the event location is LED

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	LED		Changed LED brightness : *xxxx*
	The LED behavior changed. *xxxx*: LED behavior setting (normal, economy, or off) [Action] None			

2.6.7 Event location = SVP

The following tables describe Switch failure and event information when the event location is SVP.

- INFO information

Table 2-76 Switch INFO information when the event location is SVP

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	INFO	SVP		SVP controller download succeeded
	The SVP controller was successfully updated. [Action] None			

No.	Event level	Event location	Ref. Code	Message text
	Description			
2	INFO	SVP		SVP started
	The SVP started. [Action] None			
3	INFO	SVP		This machine is going to sleep ... in a few seconds.
	The switch will sleep in a few seconds. [Action] None			

- `ERROR` information

Table 2-77 Switch ERROR information when the event location is SVP

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	ERROR	SVP	39339101	Error in SVP detected
	An SVP error was detected. [Action] Replace the Switch.			

- `CRITC` information

Table 2-78 Switch CRITC information when the event location is SVP

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	CRITC	SVP	39239000	SVP controller Version write error!!
	An attempt to write the SVP controller version failed. [Action] Replace the Switch.			
2	CRITC	SVP	39239001	SVP controller download(SPI Tx) error!!
	An SVP error was detected. [Action] Replace the Switch.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
3	CRITC	SVP	39239002	SVP controller download(SPI Write) error!!
	An SVP error was detected. [Action] Replace the Switch.			
4	CRITC	SVP	39239003	SVP controller download(Health Check) error!!
	An SVP error was detected. [Action] Replace the Switch.			
5	CRITC	SVP	39239004	SVP controller download(Unknown) error!!
	An SVP error was detected. [Action] Replace the Switch.			

2.6.8 Event location = PWRSUP

The following table describes Switch failure and event information when the event location is `PWRSUP`.

- `CRITC` information

Table 2-79 Switch CRITC information when the event location is PWRSUP

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	CRITC	PWRSUP	3C239201 3C239202 3C239203 3C239204 3C239205 3C239206 3C239207 3C239208 3C239209 3C23920A 3C23920B 3C23920C 3C23920D 3C23920E 3C23920F	Error of the power supply detected
	A power supply failure was detected. [Action] Replace the Switch.			

2.6.9 Event location = PCI

The following table describes Switch failure and event information when the event location is `PCI`.

- `FATAL` information

Table 2-80 Switch FATAL information when the event location is PCI

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	FATAL	PCI	1C100001	Detected parity error(cfg=*xx*,sum=*xx*)
	A parity error was detected (PCI bus failure). If the `system recovery` configuration command is set, the Switch restarts. *xx*: Location where the error was detected (information for vendor analysis) [Action] Replace the Switch.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
2	FATAL	PCI	1C100002	Signaled system error(cfg=*xx*,sum=*xx*)
	A system error was signaled (PCI bus failure). If the `system recovery` configuration command is set, the Switch restarts. *xx*: Location where the error was detected (information for vendor analysis) [Action] Replace the Switch.			
3	FATAL	PCI	1C100003	Received master abort(cfg=*xx*,sum=*xx*)
	A master abort was received when the CPU was a target (PCI bus failure). If the `system recovery` configuration command is set, the Switch restarts. *xx*: Location where the error was detected (information for vendor analysis) [Action] Replace the Switch.			
4	FATAL	PCI	1C100004	Received target abort(cfg=*xx*,sum=*xx*)
	A target abort was received when the CPU was the master (PCI bus failure). If the `system recovery` configuration command is set, the Switch restarts. *xx*: Location where the error was detected (information for vendor analysis) [Action] Replace the Switch.			
5	FATAL	PCI	1C100005	Signaled target abort(cfg=*xx*,sum=*xx*)
	A target abort was received when the CPU was a target (PCI bus failure). If the `system recovery` configuration command is set, the Switch restarts. *xx*: Location where the error was detected (information for vendor analysis) [Action] Replace the Switch.			
6	FATAL	PCI	1C100006	Master data parity error(cfg=*xx*,sum=*xx*)
	A parity error was asserted or detected (PCI bus failure). If the `system recovery` configuration command is set, the Switch restarts. *xx*: Location where the error was detected (information for vendor analysis) [Action] Replace the Switch.			
7	FATAL	PCI	1C100007	System Error(cfg=*xx*,sum=*xx*)
	The CPU detected a PCI error (PCI bus failure). If the `system recovery` configuration command is set, the Switch restarts. *xx*: Location where the error was detected (information for vendor analysis) [Action] Replace the Switch.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
8	FATAL	PCI	1C100008	PCI fatal error(Command Status=*xx*)
	SW-LSI detected a PCI error (PCI bus failure). If the `system recovery` configuration command is set, the Switch restarts. *xx*: Location where the error was detected (information for vendor analysis) [Action] Replace the Switch.			
9	FATAL	PCI	1C100009	PCI parity error(Command Status=*xx*)
	A parity error was detected on SW-LSI (PCI bus failure). If the `system recovery` configuration command is set, the Switch restarts. *xx*: Location where the error was detected (information for vendor analysis) [Action] Replace the Switch.			

2.6.10 Event location = RAM

The following table describes Switch failure and event information when the event location is `RAM`.

- `FATAL` information

Table 2-81 Switch FATAL information when the event location is RAM

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	FATAL	RAM	2A100001	Double bit error in DDR2(FADR=*xx*,SYND=*xx*)
	A 2-bit error occurred on DDR2 (ECC error). If the `system recovery` configuration command is set, the Switch restarts. *xx*: Location where the error was detected (information for vendor analysis) [Action] Replace the Switch.			
2	FATAL	RAM	2A100002	Double bit error in L2D(FADR=*xx*, SYND0=*xx*,SYND1=*xx*)
	A 2-bit error occurred in L2 Cache data (ECC error). If the `system recovery` configuration command is set, the Switch restarts. *xx*: Location where the error was detected (information for vendor analysis) [Action] Replace the Switch.			

No.	Event level	Event location	Ref. Code	Message text
	Description			
3	FATAL	RAM	2A100003	Double bit error in L2T(FADR=*xx*,SYND=*xx*)
	A 2-bit error occurred in L2 Cache Tag (ECC error). If the `system recovery` configuration command is set, the Switch restarts. *xx*: Location where the error was detected (information for vendor analysis) [Action] Replace the Switch.			

2.6.11 Event location = CPU

The following table describes Switch failure and event information when the event location is `CPU`.

- `CRITC` information

Table 2-82 Switch CRITC information when the event location is CPU

No.	Event level	Event location	Ref. Code	Message text
	Description			
1	CRITC	CPU	2D202000	CPU BIST Fatal Detect *xx*[*xx*](mask=*xx*) expect: *xx* -> rdata: *xx*
	BIST detected an error for FIFO in the CPU. *xx*: Location where the error was detected (information for vendor analysis) [Action] Replace the Switch.			

Index