AX2340S Software Manual

Message Log Reference

For Version 2.5

AX23S-S005X-60

■ Relevant products

This manual applies to the models in the AX2340S series of switches. It also describes the function of OS-L2N version 2.5 of the software.

■ Precautions in exporting

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. If you require more information, please contact an Alaxala sales representative.

■ Trademarks

■ Reading and storing this manual

Before you use the device, 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.

■ Note

Information in this document is subject to change without notice.

■ Editions history

June 2024 (Edition 1) AX23S-S005X-60

■ Copyright

Preface

■ Applicable products and software versions

This manual applies to the models in the AX2340S series of switches. It also describes the functions supported by the software OS-L2N Ver. 2.5 and optional licenses.

Before you operate the Switch, 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.

■ 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:

https://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.

● To check the hardware equipment conditions and how to handle the hardware

Hardware Instruction Manual (AX23S-H001X)

Transceiver Hardware Instruction Manual (AX-COM-H001X)

● To learn the software functions, commands, and configuration settings

Configuration Guide Vol.1 (AX23S-S001X)

Vol.2 (AX23S-S002X)

● To learn the entry syntax of configuration commands and the details of command parameters

Configuration Command Reference (AX23S-S003X)

● To learn the entry syntax of operation commands and the details of command parameters

Operation Command Reference (AX23S-S004X)

● To check messages and logs

Message Log Reference (AX23S-S005X)

● To learn how to troubleshoot a problem

Troubleshooting Guide (AX23S-T001X)

■ Conventions: The terms "Switch" and "switch"

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

- AX2340S series switch

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

■ Abbreviations used in the manual

AC	Alternating Current
ACK	ACKnowledge
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
bit/s	bits per second (can also appear as bps)
BPDU	Bridge Protocol Data Unit
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Continuity Check
CFM	Connectivity Fault Management

CIST	Common and Internal Spanning Tree
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRR	Deficit Round Robin
DSA	Digital Signature Algorithm
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DSS	Digital Signature Standard
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
ECDHE	Elliptic Curve Diffie-Hellman key exchange, Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EEE	Energy Efficient Ethernet
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
GCM	Galois/Counter Mode
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
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
MLD	Multicast Listener Discovery
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NDP	Neighbor Discovery Protocol
NTP	Network Time Protocol
OAM	Operations,Administration,and Maintenance
OUI	Organizationally Unique Identifier
packet/s	packets per second (can also appear as pps)
PAD	PADding

PAE	Port Access Entity
PC	Personal Computer
PDU	Protocol Data Unit
PGP	Pretty Good Privacy
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PoE	Power over Ethernet
PQ	Priority Queueing
PS	Power Supply
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RMON	Remote Network Monitoring MIB
RQ	ReQuest
RSA	Rivest, Shamir, Adleman
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SFP+	enhanced Small Form-factor Pluggable
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SSAP	Source Service Access Point
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
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
USB	Universal Serial Bus
VLAN	Virtual LAN
WAN	Wide Area Network
WWW	World-Wide Web

■ Conventions: KB, MB, GB, and TB

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

Contents

1. Operation Message 9

1.1 Operation message 10

1.1.1 Type of message 10

1.1.2 Message type 10

1.1.3 Outputting message 11

1.1.4 Operation log and reference log 11

1.1.5 Output to remote servers 13

1.1.6 System message trap 14

1.2 Event location format 15

1.2.1 Format for screen output 15

1.2.2 Format of operation logs 15

1.2.3 Format of reference logs 16

1.2.4 Event level 16

1.2.5 Event location 17

1.2.6 Event interface ID 18

2. Event Location Format 19

2.1 EQUIPMENT 20

2.2 PS 23

2.3 FAN 24

2.4 SOFTWARE 25

2.4.1 0000XXXX 25

2.4.2 01XXXXXX 26

2.4.3 02XXXXXX 28

2.4.4 06XXXXXX-09XXXXXX 31

2.4.5 0dXXXXXX 32

2.4.6 1eXXXXXX 33

2.4.7 20XXXXXX-2aXXXXXX 34

2.4.8 30XXXXXX-3fXXXXXX 42

2.5 CONFIG 48

2.6 ACCESS 49

2.7 SCRIPT 55

2.8 PORT 56

2.9 POE 61

2.10 MAC 63

2.11 VLAN 68

2.11.1 2011XXXX 68

2.11.2 2013XXXX (GSRP aware) 75

2.11.3 2017XXXX (Ring Protocol) 76

2.11.4 2080XXXX (L2 loop detection) 77

2.11.5 2090XXXX (CFM) 79
2.11.6 2110XXXX-2120XXXX 80
2.11.7 2510XXXX 84
2.12 ULR 86
2.13 IP 93

1 Operation Message

1.1 Operation message

Information output by the Switch, such as changes in running status or failure information, which is intended to notify the administrator is called an operation message. Operation messages can be saved in the device as logs and output to an operation terminal or syslog server. Using this log data, you can manage the switch operating status.

1.1.1 Type of message

The table below describes the types of output messages and gives references for those messages. Among these messages, information on devices and functions output by the Switch is called an operation message.

Table 1-1: Type of message and reference

Type of message		Reference
Configuration Error Messages		"Error Messages Displayed When Editing the Configuration" in the manual "Configuration Command Reference"
Command response messages		"Response Messages" of "Operation Command Reference"
Operation message	Event location format	"2 Event Location Format"
	Action log message format	Action log messages for the following commands in the manual "Operation Command Reference" • show dot1x logging • show web-authentication logging • show mac-authentication logging • show ip dhcp snooping logging

1.1.2 Message type

Message types are the information that categorizes messages such as operation messages, user command operations, configuration error messages, and command response messages based on the contents. Additionally, operation messages can be categorized by the format of the information to be output. The following table shows a list of message types.

Table 1-2: Message type list

Message type	Description	Classification of operation messages by format
KEY	Command operations entered from an operation terminal	—
RSP	Messages output by the device in response to input commands	—
SKY	Command information input by script	—
SRS	Messages output by the device in response to commands input by script	—
ERR	Error information for each switch event location	Event location format
EVT	Event information for each switch event location	

Message type	Description	Classification of operation messages by format
AUT	The information that is collected with the Layer 2 authentication functions for each program. Indicated as corresponding operation commands. • show dot1x logging • show web-authentication logging • show mac-authentication logging	Action log message format
DSN	Information to be collected with DHCP snooping. Indicated as corresponding operation commands. • show ip dhcp snooping logging	

Legend —: Not applicable

1.1.3 Outputting message

Supported output methods for operation messages and other messages vary depending on the message type. The following table shows the output method for each message type.

Table 1-3: Output method for each message type

Message type	Output to operation terminals	Operation log	Reference log	Output to remote servers (syslog, E-Mail)	System message traps
KEY, RSP	Y	Y	N	Y	N
SKY, SRS	N	Y	N	Y	N
ERR, EVT	Y	Y	Y	Y	Y
AUT, DSN	N	N	N	Y	N

Legend:

Y: Supported

N: Not supported

1.1.4 Operation log and reference log

The following information is saved in the operation log in the order of occurrence and can be viewed by using the "show logging" command.

- Input command (message type KEY)
- Messages output by the device in response to input commands (message type RSP)
- Input command by script (message type SKY)
- Messages output by the device in response to input commands by script (message type SRS)
- Operation message (excluding message types AUT and DSN)

For operation messages of message type ERR and EVT, reference logs categorize the information by message ID, and then records the event time of the first and last occurrences, and total number of occurrences. You can display them by specifying the reference parameter with the "show logging" command.

(1) Log specifications

The following table shows the specifications of the operation log and reference log.

Table 1-4: Specifications of the operation log and reference log

Item	Operation log	Reference log
Log contents	• Acquires events that occurred in chronological order.	• Records statistics for each event, such as the time of the first and last occurrences, and the total number of occurrences.
Target message type	• KEY, RSP, SKY, SRS • ERR, EVT	• ERR#1 • EVT#1, #2
Number of acquired entries	• 12000 entries can be acquired. Within those, the first 6000 log entries are saved chronologically. • The next 3000 entries save logs in chronological order from the old logs overflowing from the above 6000 entries, excluding logs with message types SKY and SRS. • Of the remaining 3000 entries, out of the old logs overflowing from the 9000 entries above, only logs with message types KEY, RSP, ERR, and EVT are saved in chronological order. • One entry contains 80 characters. If an acquired entry contains 100 characters, it is divided between two entries.	• 500 entries can be acquired.
Overflow processing when the log size is exceeded	• If the number of logs acquired exceeds 6000 entries, logs with message types SKY and SRS among the overflowing old logs will be deleted. Among the overflowing old logs, logs with message types other than SKY and SRS are saved in entries 6001 to 9000. • If the number of logs acquired exceeds 9000 entries, logs with message types KEY, RSP, ERR, and EVT among the overflowing old logs will be saved in entries 9001 to 12000. • If the number of logs acquired exceeds 12000 entries, overflowing old logs will be deleted.	• If the number of log entries exceeds 500 entries, entries that have a lower event level are deleted and the new entries are acquired. Note that new entries that have an event level of E3 or E4 are not acquired.

#1

Not retrieved if the event location is SCRIPT.

#2

Not retrieved for event levels R8 to R5.

(2) Automatically save logs

This section describes the occasions when the operation logs and reference logs are automatically saved to internal flash memory and the destination to which they are saved. Note that if the "no logging syslog-dump" configuration command is set, logs are automatically saved for occasion 1 only.

Occasions when logs are automatically saved:

1.When the Switch is started

2.When a critical error with an event level from E9 to E5 occurs

3.When the device is restarted by using the "reload" operation command

4.When the device is restarted accompanying ppupdate

Table 1-5: Location of saved logs

Log type	Location of internal memory
Operation log	Logs are saved to /usr/var/log/system.log
Reference log	Logs are saved to /usr/var/log/error.log

(3) How to create a log file

Operation logs and reference logs can be extracted as files. Specify the redirection to create a file when executing the "show logging" command. If you want to output command output results to a file for a command other than the "show logging" command, you also must specify redirection. The following table describes the directory for storing the created files when redirection is specified for a command.

Table 1-6: Storage directory

Item	Storage directory	Remarks
Home directory for the user	/usr/home/<user-account-name>/	Stored in internal memory
Temporary directory	/tmp/	When the switch stops due to power discontinuity or the "reload" command, stored files will be deleted.

The following shows an example of creating a backup of log information by executing the "show logging" command.

Backing up the operation log in internal memory:

```
> show logging > /usr/home/<user-account-name>/<file name>
>
```

1.1.5 Output to remote servers

The Switch can output not only operation messages but also various messages classified by the message type to remote servers by using the syslog output function or the E-Mail sending function. For details, see "Configuration Guide Vol. 1, 17 Log Data Output Function".

- syslog output function

  You can use the syslog output function to output various messages to remote servers. However, the syslog output function might lose information due to reasons such as frame-loss.

- E-Mail sending function

  You can use the E-Mail sending function to send various messages as emails. This function cannot receive emails. If a user replies to an email sent by this function, a transmission error occurs.

1.1.6 System message trap

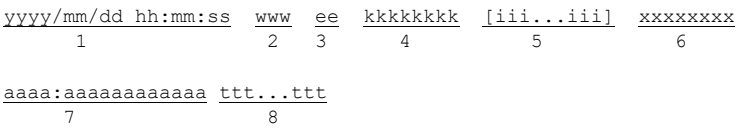
Operation messages of message type ERR or EVT can be sent as private SNMP notifications. This is called a system message trap. You can use the "snmp-server traps" configuration command to specify the importance of the operation message sent as an SNMP notification.

1.2 Event location format

1.2.1 Format for screen output

The following figure shows the format when outputting to the screen.

Figure 1-1: Format for screen output



1.Time: Displays the date and time when the event indicated in the message occurred.

2.The switch number (two digits) and the switch status (next one character):

- S: Indicates the standalone status (fixed).

3.Event level

4.Event location

5.Event interface ID. Whether this information is displayed depends on the event location.

6.Message ID

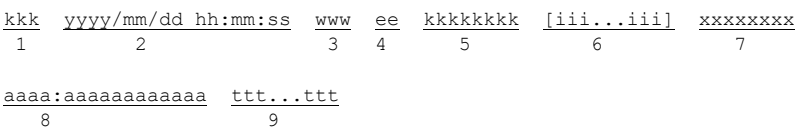
7.Added info

8.Message text

1.2.2 Format of operation logs

The following figure shows the format for saving operation logs. This is a format in which the message type is added to the information to be output on the screen.

Figure 1-2: Format of operation logs



1.Message type

2.Time: Sampling year, month, day, hour, minute, and second in text

3.The switch number (two digits) and the switch status (next one character):

- S: Indicates the standalone status (fixed).

4.Event level

5.Event location

6.Event interface ID

It may not be displayed depending on the event location.

7.Message ID

This is the code that corresponds to the message.

8.Added info

This information contains a code that indicates the detailed information about the event.

9.Message text

1.2.3 Format of reference logs

The figure below describes the format of the reference log.

Figure 1-3: Format of reference logs

```
ee   kkkkkkkk   [iii...iii]   xxxxxxxx   aaaa:aaaaaaaaaaaa
1       2            3             4           5

  yyyy/mm/dd hh:mm:ss    yyyy/mm/dd hh:mm:ss   ccc
         6                       7              8
```

1.Event level

2.Event location

3.Event interface ID

It may not be displayed depending on the event location.

4.Message ID

This is the code that corresponds to the message.

5.Added info

This information contains a code that indicates the detailed information about the event.

6.Occurrence date and time of the last applicable error.

7.Occurrence date and time of the first applicable error.

8.Number of occurrences of the applicable error.

This is the number of events that have occurred from the start of log acquisition to the present. If the applicable event occurs 255 times or more, the number of occurrences will be indicated as 255.

1.2.4 Event level

Events are classified into seven levels depending on their severity. The table below describes the event levels and their contents.

Table 1-7: Event levels and their contents

Event level	Displayed information	Description
9	E9	Indicates that a fatal failure has occurred. This is a failure that causes the entire device to stop, resulting in either re-starting the device or stopping the device operation.
8	E8	Indicates that a severe failure has occurred. If the failure causes a fan, power supply, or part of the device to stop, and the failure is a partial hardware failure, restart or stop the target hardware.
	R8	Indicates the recover from critical error.
7	E7	Indicates that a software error has occurred. Or, it indicates a temperature abnormality in the device that does not cause the device to stop.
	R7	Indicates the recover from software error.
6	E6	Not used
	R6	Not used

Event level	Displayed information	Description
5	E5	Not used
	R5	Not used
4	E4	Indicates information on network failure detection and line.
3	E3	Warning

The following table shows the correspondence between message types and event levels.

Table 1-8: Correspondence between message types and event levels

Message type	Event level
ERR	E9 to E5
EVT	E4, E3, R8 to R5

If you specify the event level by using the "set logging console" command, you can limit the output of messages to the specified level or lower.

1.2.5 Event location

Uses an ID to indicate the location or the function of the event that occurred. The following table describes the event locations.

Table 1-9: Event location

ID	Location or function of the event that occurred
EQUIPMENT	Switch control function
PS	Power control function
FAN	Fan control function
SOFTWARE	Software control function
CONFIG	Configuration
ACCESS	Switch access permissions
SCRIPT	User-created scripts
PORT	Port control function
POE	PoE function
MAC	MAC control function
VLAN	VLAN control function
ULR	Uplink redundancy control function
IP	IP control function

1.2.6 Event interface ID

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

Table 1-10: Display format of the interface ID

Display format of the ID	Interface
PORT:<switch no.>/<nif no.>/<port no.>	Ethernet interface

Legend:

<switch no.>: Switch number (fixed as 1)

<nif no.>: Indicates the NIF number (fixed as 0)

<port no.>: Indicates the port number.

2 Event Location Format

2.1 EQUIPMENT

This section shows the operation messages for the event location EQUIPMENT.

Table 2-1: Operation message of event location EQUIPMENT

Message ID	Event level	Message text
	Contents and actions	
00000003	E3	Failed in accumulated running time access to main.
	Failed to access the total operating time of the device. [Action] This event does not affect communication and usual operation. However, the total operating time management function cannot be used, so if you want to use it, replace the device.	
00020102	E7	Hardware exceeded tolerance level of low temperature(<temperature> degree). Check room temperature.
	The hardware temperature went below the permissible temperature range (<temperature> °C or lower). <temperature>: 5 [Action] 1. Check and, if necessary, improve the environment such as the room temperature around the devices. 2. Check the fan inside the device and replace the device if necessary.	
	R7	The temperature of hardware returned to normal level (<temperature> degree).
	The hardware temperature returned to normal (<temperature> °C). <temperature>: 8 [Action] None.	
00020103	E7	Hardware exceeded tolerance level of high temperature (<temperature> degree). Check that room temperature and the fan is operating normally.
	The hardware temperature rose above the permissible temperature range (<temperature> °C or higher). <temperature>: 75 [Action] 1. Check and improve the environment such as ventilation and heat sources around the devices. 2. Check the fan inside the device and replace the device if necessary.	
	R7	The temperature of hardware returned to normal level (<temperature> degree).
	The hardware temperature returned to normal (<temperature> °C). <temperature>: 72 [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
00020105	E9	Hardware is becoming high temperature which give damage to this system (<temperature> degree).
	The hardware temperature has reached a temperature (<temperature> °C or higher) that is likely to critically damage device operation. <temperature>: Detected temperature (80°C or higher) [Action] 1. Check and improve the environment such as ventilation and heat sources around the devices. 2. Check the fan inside the device and replace the device if necessary.	
00020106	E3	The temperature of hardware reached the warning level (<temperature> degree).
	The hardware has reached the temperature that is set with the "system temperature-warning-level" configuration command. <temperature>: Internal temperature of the device (in Celsius) [Action] The temperature of the device has reached the specified temperature. Check the environment surrounding the device (condition of the fan, ventilation, existence of the heat sources, etc.).	
00020107	E3	The temperature of hardware came down from the warning level.
	The hardware temperature has been 3°C or lower than the temperature that is set with the "system temperature-warning-level" configuration command. [Action] None.	
01200190 01200212 25040202	E9	System will restart due to hardware error detected.
	Due to a hardware error, the device will be restarted. [Action] Replace the device.	
01200191	E9	System will restart to correct a transient error. When the system corrects the error, there is no need to change the system.
	The device will be restarted to repair a temporary failure. [Action] Continue using the device as-is after rebooting. There is no need to replace the device. If this error occurs frequently, replace the device.	
01200211 2600000d 3900000b	E9	The temperature of the device on this system is too high.
	The temperature of the devices that configures the Switch is extremely high. [Action] Replace the device.	

Message ID	Event level	Message text
	Contents and actions	
01200214	E7	Failed in hardware temperature monitoring.
	The hardware temperature could not be obtained correctly. [Action] If it recovers automatically, continue using it. If this failure continues, replace the device.	
	R7	Hardware temperature monitoring is recoverd.
	The hardware temperature can now be obtained normally. [Action] None.	
25040200	R8	Hardware initialized.
	The hardware has been initialized. [Action] None.	
25040201	E8	Hardware restarted because of its failure.
	The switch was restarted because a hardware failure occurred at the device. [Action] Check subsequent failure recovery log entries or failure recovery failure log entries. If the recovery was successful, operations can resume. If the recovery failed, replace the device.	
	R8	Hardware recovered.
	The device recovered from a hardware failure. [Action] None.	
25040400	E8	Hardware restarted, but not recovered.
	The device restarted, but it has not recovered from a hardware failure. [Action] Replace the device.	
25040c01	E3	Corrected memory soft errors.
	The system has recovered from a memory software error. Some frames may be discarded because of the software error. [Action] None. This indicates that the memory data bits inside a switch processor might have been abruptly altered (for example by cosmic rays from a solar flare) and a software error is issued temporarily. This is not a hardware failure.	

2.2 PS

This section shows event location PS operation messages.

Table 2-2: Operation message for the event location PS

Message ID	Event level	Message text
	Contents and actions	
0000000a	E4	The speed of the fan on <ps> is high.
	The power FAN is rotating at high speed. <ps> displays the target power supply. <ps>: PS 1, PS 2 [Action] Check the environment such as ventilation and heat sources around the devices.	
0000000b	E4	The speed of the fan on <ps> is normal.
	The power FAN has returned to normal rotation. <ps> displays the target power supply. <ps>: PS 1, PS 2 [Action] None.	

2.3 FAN

This section shows event location FAN operation messages.

Table 2-3: Operation message for the event location FAN

Message ID	Event level	Message text
	Contents and actions	
00000008	E7	<fan> speed is high.
	The fan is rotating at an abnormally high speed. <fan> displays the target fan. <fan>: FAN 3 (1), FAN 3 (2) [Action] Replace the device.	
	R7	<fan> is normal.
	The fan is in a normal state. <fan> displays the target fan. <fan>: FAN 3 (1), FAN 3 (2) [Action] None.	
00000009	E7	<fan> stopped.
	The fan has stopped. <fan> displays the target fan. <fan>: FAN 3 (1), FAN 3 (2) [Action] Replace the device.	
	R7	<fan> is normal.
	The fan is in a normal state. <fan> displays the target fan. <fan>: FAN 3 (1), FAN 3 (2) [Action] None.	

2.4 SOFTWARE

This section shows event location SOFTWARE operation messages.

2.4.1 0000XXXX

This section shows operation messages where the first four digits of message ID are 0000.

Table 2-4: Operation message for the event location SOFTWARE (0000XXXX)

Message ID	Event level	Message text
	Contents and actions	
00003003	E3	System restarted due to fatal error detected by software.
	The software detected a fatal error and restarted the device. [Action] Check the log by executing the "show logging" command. If another problem is indicated in the log, take appropriate action according to the error message.	
00003004	E3	System restarted due to user operation.
	The device restarted due to either of the following causes. • Execute the "reload" command • Restart the network interface management program [Action] Check the log using the "show logging" command to determine the cause of the device restart.	
00003303	E3	Received many packets and loaded into the queue to CPU.
	Numerous received packets have accumulated in CPU queues. [Action] None. If this message is output frequently, check the following. • Check if the device has received a large quantity of packets for the local device (such as for ping or telnet), in broadcast packets, or in a multicast. If there is too much access from the network management device, limit the amount of access to the minimum necessary. • The network configuration may be too complex. Revise the network configuration.	
00003304	E3	Processed the packets in the queue to CPU.
	Packets that had been accumulating in CPU queues have been processed. [Action] None.	
00008601	E3	NTP lost synchronization with <ip address>.
	Synchronization was lost with the NTP server at <ip address>. <ip address>: IPv4 address of NTP server [Action] Use the "show ntp associations" command to check the NTP status. If the non-synchronized state continues, check the NTP configuration, NTP server running status, and availability of communication.	

Message ID	Event level	Message text
	Contents and actions	
00008602	E3	NTP detected an invalid packet from <ip address>.
	An invalid packet from the NTP server at <ip address> was detected. <ip address>: IPv4 address of NTP server [Action] Check the NTP server.	
00008603	E3	NTP could not find the server which synchronize with.
	There is no NTP server for which synchronization is possible. [Action] Check the NTP configuration, NTP server running status, and availability of communication.	

2.4.2 01XXXXXX

This section shows operation messages where the first two digits of message ID are 01.

Table 2-5: Operation message for the event location SOFTWARE (01XXXXXX)

Message ID	Event level	Message text
	Contents and actions	
01100001 01100002 01100004 01200001 01200002 01200004 01300001 01300002 01300004 01400001 01400002 01400004 01600001 01600002 01600004 01700001 01700002 01700004 01800001 01800002 01800004 01900001 01900002 01900004 01910001	E7	Software failure occurred during operation.
	An error occurred in the software during operation. [Action] Normal operation might not be possible. Take the following actions: 1. Check the log by executing the "show logging" command. If another problem is indicated in the log, take appropriate action according to the error message. 2. Use the "reload" command to restart the device. 3. After you use the "reload" command to restart the system, if the same problem occurs, replace the device.	

Message ID	Event level	Message text
	Contents and actions	
01910002 01910004		
01100003 01200003 01300003 01400003 01600003 01700003 01800003 01900003 01910003	E9	System will restart due to software failure occurred during initialization.
	Due to an error occurred in the software during initialization, the device will be restarted. [Action] Check the log by executing the "show logging" command. If another problem is indicated in the log, take appropriate action according to the error message.	
01100005 01200005 01300005 01400005 01600005 01700005 01800005 01900005 01910005	E9	System will restart due to software failure occurred during operation.
	Due to an error occurred in the software during operation, the device will be restarted. [Action] Check the log by executing the "show logging" command. If another problem is indicated in the log, take appropriate action according to the error message.	
01200187	E3	The temperature logging file can't be written.
	Writing of temperature logging information failed. [Action] 1. Check the user area of the internal flash memory. 2. If the free space is lacking, delete unnecessary files to ensure free space (approximately 8 KB).	
01200213	E7	The CPU memory is insufficient.
	There is not enough CPU memory. [Action] 1. If many users are logged in, log out all but the most essential users. 2. If there is a lot of use from ftp, disconnect all but the most essential connections. 3. If there is too much access from the network management device, limit the amount of access to the minimum necessary. 4. If the system does not recover after any one of three methods above, the capacity limit of the Switch might not be satisfied. Review the network configuration with reference to "Configuration Guide Vol. 1, 3 Capacity Limit".	
	R7	The CPU has recovered from insufficient memory.
	The CPU has recovered from a lack of memory. [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
01200220	E9	System will restart due to WDT timeout.
	The device will be restarted because of a WDT (watchdog timer) timeout. [Action] Check the log by executing the "show logging" command after restarting the device. If another problem is indicated in the log, take appropriate action according to the error message.	
01700501	E3	Statistics table initialized.
	The device time has been changed by the "set clock" command, and the statistics table that holds the CPU usage statistics has been initialized. [Action] None.	
01700502	E3	CPU overloaded. There is the possibility of software failure in responding to user command input or sending notification to SNMP agent.
	The response to a user-entered command might have failed or a notification to an SNMP agent might have failed. The CPU might be overloaded. [Action] If necessary, reenter command or retrieve MIB.	
01700503	E3	There is the possibility of software failure in responding to user command input or sending notification to SNMP agent.
	The response to a user-entered command might have failed or a notification to an SNMP agent might have failed. [Action] If necessary, reenter command or retrieve MIB.	
01900250	E3	Software started up.
	The software has started. This log data is collected in UTC time. [Action] None.	
01910201	E3	System started collecting new "error.log".
	The system has started collecting data into a new reference log. [Action] None.	
01910202	E3	System restarted by user operation.
	The system was restarted by a user operation. [Action] None.	

2.4.3 02XXXXXX

This section shows operation messages where the first two digits of message ID are 02.

Table 2-6: Operation message for the event location SOFTWARE (02XXXXXX)

Message ID	Event level	Message text
	Contents and actions	
02002001	E7	snmpd aborted.
	The SNMP agent program (snmpd) was forced to stop. [Action] Collect the error save information (snmpd.core file under /usr/var/core), log information, and the configuration of the SNMP agent program. For details about how to collect the information, see the "Troubleshooting Guide". The SNMP agent program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	snmpd restarted.
	The SNMP agent program (snmpd) has restarted. The switch outputs this message after the SNMP agent program is forced to stop and is then re-started automatically. [Action] None.	
02002003	E7	rmon aborted.
	The RMON program (rmon) was forced to stop. [Action] Collect the error save information (rmon.core file under /usr/var/core), log information, and the configuration of the RMON program. For details about how to collect the information, see the "Troubleshooting Guide". The RMON program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	rmon restarted.
	The RMON program (rmon) has restarted. The switch outputs this message after the RMON program is forced to stop and is then restarted automatically. [Action] None.	
02002010	E3	System failed switching to admin mode.
	The change to the admin mode during MIB setup has failed. [Action] Another administrator has become admin. Using the "show sessions" command, check the login users and admin users.	
02002012	E3	Specified MIB doesn't exist, or it does not have read/write attribute.
	Either the set MIB does not exist, or the MIB does not have read and write attributes. [Action] Make sure that the configured MIB has read/write attributes.	

Message ID	Event level	Message text
	Contents and actions	
02002013	E3	Incorrect instance value specified.
	The instance value set during MIB setup is not correct. [Action] Check and set the instance value.	
02002014	E3	MIB value specified was out of range.
	You are attempting to set a MIB value that is outside the setting range during MIB setup. [Action] For the range of MIB values, see "Configuration Command Reference, 12. SNMP".	
02002015	E3	Data length of the MIB value was too long.
	The entry for the MIB value set during MIB setup is too long. [Action] For the number of characters that can be set as a MIB value, see "Configuration Command Reference, 12. SNMP".	
02002016	E3	MIB Set failed due to the lack of necessary MIBs.
	MIB setup was not possible because the MIBs required for setting are insufficient. [Action] Make sure that the required items are met during setup.	
02002017	E3	Illegal character used in MIB setting.
	You are attempting to set up the MIB using invalid characters. [Action] Check the character code list in "Configuration Command Reference, 1. Reading the Manual" and set up the MIB.	
02002018	E3	MIB Set failed to configured the configuration file because the preliminary configuration file is under editing.
	Setting of a MIB into the startup configuration file was not possible because the backup configuration file is being edited. [Action] Stop editing of the backup configuration file.	
02002019	E3	Failed in contact the configuration file while setting up MIB.
	Access to the startup configuration file for MIB settings failed. [Action] Eliminate the cause of the access failure, and try again.	
02002020	E3	MIB value has failed to establish. Errors occurred in the "config" command.
	An error occurred while editing the configuration at MIB setup, and the MIB could not be set. [Action] For details on configuration errors, see "Error Messages Displayed When Editing the Configuration" in the manual "Configuration Command Reference".	

Message ID	Event level	Message text
	Contents and actions	
02002021	E3	Not all MIB configured.
	MIB setup failed, and only some of the MIB values were set. [Action] Try setup again. If the retry still does not work, log in (for example, by using telnet) and set the MIB values.	
02002023	E3	System failed to save the configuration while processing MIB settings.
	While setting up MIB from an SNMP manager, an error occurred during processing to save the configuration. [Action] The configuration has not been saved. Save it (for example, by using telnet).	
02002024	E3	<object name> set as <mib value> at the request of <ip address>.
	<object name> was set to <mib value> because of a request from <ip address>. <object name>: MIB object mnemonic <mib value>: MIB value <ip address>: IPv4 or IPv6 address of the SNMP manager [Action] None.	
02002025	E3	SNMP: MAC address table entry cleared at the request of <ip address>.
	The MAC address table was cleared due to a MAC address table clear request from the SNMP manager at <ip address>. <ip address>: IPv4 or IPv6 address of the SNMP manager [Action] None.	

2.4.4 06XXXXXX-09XXXXXX

This section shows operation messages where the first two digits of message ID are 06 to 09.

Table 2-7: Operation message for the event location SOFTWARE (06XXXXXX-)

Message ID	Event level	Message text
	Contents and actions	
06100001 06100002 06100004 06200001 06200002 06200004 06300001 06300002 06300004 06400001 06400002 06400004 06500001 06500002 06500004 09100001 09100002 09100004	E7	Software failure occurred during operation.
	An error occurred in the software during operation. [Action] Normal operation might not be possible. Take the following actions: 1. Check the log by executing the "show logging" command. If another problem is indicated in the log, take appropriate action according to the error message. 2. Use the "reload" command to restart the device. 3. After you use the "reload" command to restart the system, if the same problem occurs, replace the device.	

Message ID	Event level	Message text
	Contents and actions	
09200001 09200002 09200004 09300001 09300002 09300004 09400001 09400002 09400004 09500001 09500002 09500004 09600001 09600002 09600004 09700001 09800001		
06100003 06200003 06300003 06400003 06500003 09100003 09200003 09300003 09400003 09500003 09600003	E9	System will restart due to software failure occurred during initialization.
	Due to an error occurred in the software during initialization, the device will be restarted. [Action] Check the log by executing the "show logging" command. If another problem is indicated in the log, take appropriate action according to the error message.	
06100005 06200005 06300005 06400005 06500005 09100005 09200005 09300005 09400005 09500005 09600005 09700005 09800005	E9	System will restart due to software failure occurred during operation.
	Due to an error occurred in the software during operation, the device will be restarted. [Action] Check the log by executing the "show logging" command. If another problem is indicated in the log, take appropriate action according to the error message.	

2.4.5 0dXXXXXX

This section shows operation messages where the first two digits of message ID are 0d.

Table 2-8: Operation message for the event location SOFTWARE (0dXXXXXX)

Message ID	Event level	Message text
	Contents and actions	
0d10b001	E7	dhcp_server aborted.
	The DHCP server program (dhcp_server) was forced to stop. The DHCP server detected an anomaly such as a lack of memory, aborted the running, and forced the program to stop. [Action] The DHCP server program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	dhcp_server restarted.
	The DHCP server program (dhcp_server) has restarted. The switch outputs this message when the DHCP server program restarts automatically or a restart is requested by the "restart dhcp" command. [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
0d10b002	E3	The not used IP address which a dhcp_server can lease out is not a subnet <subnet address>.
	An unused IP address lent by dhcp_server is not in the subnet <subnet address>. <subnet address>: Allocation range subnet address [Action] Examine the maximum number of clients for the subnet that dhcp_server can allocate.	
0d10b003	E3	The dhcp_server reused the abandoned IP address <ip address>.
	dhcp_server reused the discarded IP address. <ip address>: Allocation IP address [Action] None.	
0d10b004	E3	The IP address <ip address> which the dhcp_server schedule to lease out is already used by others.
	<ip address> that dhcp_server attempted to lend has been used already in other locations. <ip address>: IP address to be allocated [Action] Check whether the range of lent-out IP addresses and fixed allocated IP addresses overlap each other.	
0d10b005	E3	Failed in NS UPDATE by dhcp_server. : <map>
	NS UPDATE processing by dhcp_server has failed. <map>: Map where the error occurred [Action] Check the zone setting of the Switch authentication key setting, and DNS-server setting. If you are using an authentication key, make sure that time information for both the Switch and DNS server are correct.	
0d10b0e4	E3	dhcp_server: Invalid network address.
	The DHCP server detected an invalid configuration. An invalid network address was specified. [Action] Delete the previously-entered setting, and re-specify the setting using a correct network address.	
0d10b0ec	E3	dhcp_server: Invalid key.(ip dhcp key ... secret-hmac-md5 ...)
	The DHCP server detected an invalid configuration. There is an invalid key. [Action] Delete the previously-entered setting, and re-specify the setting using a correct key.	
0d10b0ee	E3	dhcp_server: Invalid IP address. (ip dhcp excluded-address ...)
	The DHCP server detected an invalid configuration. An invalid exclusion address range was specified. [Action] Delete the previously-entered setting, and re-specify the setting using a correct exclusion address range.	

2.4.6 1eXXXXXX

This section shows operation messages where the first two digits of message ID are 1e.

Table 2-9: Operation message for the event location SOFTWARE (1eXXXXXX)

Message ID	Event level	Message text
	Contents and actions	
1e001000	E7	flowd aborted.
	The flow statistics agent program (flowd) was forced to stop. [Action] The flow statistics agent program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	flowd restarted.
	The flow statistics agent program (flowd) has restarted. The switch outputs this message when the flow statistics agent program restarts automatically or a restart is requested by the "restart sflow" command. [Action] None.	

2.4.7 20XXXXXX-2aXXXXXX

This section shows operation messages where the first two digits of message ID are 20 to 2a.

Table 2-10: Operation message for the event location SOFTWARE (20XXXXXX-)

Message ID	Event level	Message text
	Contents and actions	
20110001	E7	stpd aborted
	The Spanning Tree program (STPd) was forced to stop. [Action] Collect the error save information (stpd.core file under /usr/var/core), log information, and the configuration of the Spanning Tree program. For details about how to collect the information, see the "Troubleshooting Guide". The Spanning Tree program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	stpd restarted
	The Spanning Tree program (stpd) has restarted. The device outputs this message when the Spanning Tree program restarts automatically or a restart is requested by the "restart spanning-tree" and "restart uplink-redundant" commands. [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
20120001	E7	LAd aborted
	The link aggregation program (LAd) was forced to stop. [Action] Collect the error save information (LAd.core file under /usr/var/core), log information, and the configuration of the link aggregation program. For details about how to collect the information, see the "Troubleshooting Guide". The link aggregation program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	LAd restarted.
	The link aggregation program (LAd) has restarted. The switch outputs this message when the link aggregation program restarts automatically or a restart is requested by the "restart link-aggregation" command. [Action] None.	
20130001	E7	gsrpd aborted.
	The GSRP program (gsrpd) was forced to stop. [Action] Collect the error save information (gsrpd.core file under /usr/var/core), log information, and the configuration of the GSRP program. For details about how to collect the information, see the "Troubleshooting Guide". The GSRP program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
20130002	R7	gsrpd restarted.
	The GSRP program (gsrpd) has restarted. The switch outputs this message when the GSRP program restarts automatically or a restart is requested by the "restart gsrp" command. [Action] None.	
20140001	E7	lldpd aborted.
	The LLDP program (lldpd) was forced to stop. [Action] The LLDP program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	lldpd restarted.
	The LLDP program (lldpd) has restarted. The switch outputs this message when the LLDP program restarts automatically or a restart is requested by the "restart lldp" command. [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
20160001	E7	L2MacManager aborted.
	L2MAC manager program (L2MacManager) was forced to stop. [Action] The L2MAC manager program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	L2MacManager restarted.
	The L2MAC manager program (L2MacManager) has restarted. The device outputs this message when the L2MAC manager program restarts automatically or a restart is requested by the "restart vlan mac-manager" command. [Action] None.	
20160002	E4	The MAC-VLAN MAC Address entry can't be registered at hardware tables.
	The MAC address that was set with the MAC VLAN configuration command could not be set for the hardware. [Action] Review the capacity limit. However, depending on the hardware specification, the setting to the maximum of the capacity limit might not be available.	
20170001	E7	axrpd aborted.
	The Ring Protocol program (axrpd) was forced to stop. [Action] Collect the error save information, log information, and the configuration of the Ring Protocol program. For details about how to collect the information, see the "Troubleshooting Guide". The error save information is as follows. Storage directory: /usr/var/core/ File: axrpd.core The Ring Protocol program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	axrpd restarted.
	The Ring Protocol program (axrpd) has restarted. The switch outputs this message when the Ring Protocol program restarts automatically or a restart is requested by the "restart axrp" command. [Action] None.	
20400001	E7	dot1xd aborted
	The IEEE 802.1X program (dot1xd) was forced to stop. [Action] The IEEE 802.1X program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	

Message ID	Event level	Message text
		Contents and actions
	R7	dot1xd restarted.
	The IEEE 802.1X program (dot1xd) has restarted. The switch outputs this message when the IEEE 802.1X program restarts automatically or a re-start is requested by the "restart dot1x" command. [Action] None.	
20400003	E4	The 802.1X Supplicant MAC address can't be registered at hardware tables.
	The MAC address of a terminal, which had been successfully authenticated with IEEE 802.1X, could not be set in the hardware table. [Action] Review the capacity limit. However, depending on the hardware specification, the setting to the maximum of the capacity limit might not be available.	
20400004	E4	The 802.1X Supplicant MAC address of MAC VLAN can't be registered at hardware tables.
	The MAC address of a terminal, which had been successfully authenticated at a MAC VLAN with IEEE 802.1X, could not be set in the hardware table. [Action] Review the capacity limit. However, depending on the hardware specification, the setting to the maximum of the capacity limit might not be available.	
20420001	E7	wad aborted.
	The Web authentication program (wad) was forced to stop. [Action] The Web authentication program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	wad restarted.
	The Web authentication program (wad) has restarted. The switch outputs this message when the Web authentication program restarts automatically or a restart is requested by the "restart web-authentication" command. [Action] Perform authentication again on the authentication client side.	
20420002	E4	The wad MAC Address entry can't be registered at hardware tables.
	Using the Web authentication function, the MAC address of a terminal could not be set in the hardware table. [Action] Review the capacity limit. However, depending on the hardware specification, the setting to the maximum of the capacity limit might not be available.	

Message ID	Event level	Message text
	Contents and actions	
20420003	E4	The wad MAC Address entry failed in the deletion.
	Using the Web authentication function, the MAC address of a registered terminal could not be deleted from the hardware table. [Action] Restart L2MAC manager program (L2MacManager).	
20430001	E7	macauthd aborted.
	The MAC authentication program was forced to stop. [Action] The MAC authentication program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	macauthd restarted.
	The MAC authentication program has restarted. The switch outputs this message when the MAC authentication program restarts automatically or a restart is requested by the "restart mac-authentication" command. [Action] Perform authentication again on the authentication client side.	
20430002	E4	The macauthd MAC address entry can't be registered at hardware tables.
	Using MAC authentication, the MAC address of a terminal could not be set in the hardware table. [Action] Review the capacity limit. However, depending on the hardware specification, the setting to the maximum of the capacity limit might not be available.	
20430003	E4	The macauthd MAC address entry failed in the deletion.
	Using MAC authentication, the MAC address of a registered terminal could not be deleted from the hardware table. [Action] Restart L2MAC manager program (L2MacManager).	
20700001	E7	efmoamd aborted.
	The IEEE 802.3ah/OAM program (efmoamd) was forced to stop. [Action] The IEEE 802.3ah/OAM program should restart automatically. If it does not restart if restarts occur frequently, restart the device.	
	R7	efmoamd restarted.
	The IEEE 802.3ah/OAM program (efmoamd) has restarted. The switch outputs this message when the IEEE 802.3ah/OAM program restarts automatically or a restart is requested by the "restart efmoam" command. [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
20800001	E7	l2ldd aborted.
	The L2 loop detection program (l2ldd) was forced to stop. [Action] The L2 loop detection manager program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	l2ldd restarted.
	The L2 loop detection program (l2ldd) has restarted. The switch outputs this message when the L2 loop detection program restarts automatically or a restart is requested by the "restart loop-detection" command. [Action] None.	
20900001	E7	cfmd aborted.
	The CFM program (cfmd) was forced to stop. [Action] Collect the error save information (cfmd.core file under /usr/var/core), log information, and the configuration of the CFM program. For details about how to collect the information, see the "Troubleshooting Guide". The CFM program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	cfmd restarted.
	The CFM program (cfmd) has restarted. The switch outputs this message when the CFM program restarts automatically or a restart is requested by the "restart cfm" command. [Action] None.	
21000001	E7	snoopd aborted.
	The IGMP snooping/MLD snooping program (snoopd) was forced to stop. [Action] The IGMP snooping/MLD snooping program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	snoopd restarted.
	The IGMP snooping/MLD snooping program (snoopd) has restarted. The switch outputs this message when the IGMP snooping/MLD snooping program restarts automatically or a restart is requested by the "restart snooping" command. [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
25300000	E7	nimd aborted.
	The network interface manager program (nimd) was forced to stop. [Action] The network interface manager program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	nimd restarted.
	The network interface manager program (nimd) has restarted. The device outputs this message when the network interface management program is automatically restarted. [Action] None.	
26100005	E9	System will restart due to software failure occurred during operation.
	Due to an error occurred in the software during operation, the device will be restarted. [Action] Check the log by executing the "show logging" command. If a problem is indicated in the log, take appropriate action according to the error message.	
27000001	E7	accountingd aborted.
	The accounting program (accountingd) was forced to stop. [Action] Collect the error save information (acctd.core file under /usr/var/core), log information, and the configuration of the accounting program. For details about how to collect the information, see the "Troubleshooting Guide". The accounting program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	accountingd restarted.
	The accounting program (accountingd) has restarted. The switch outputs this message when the accounting program restarts automatically or a restart is requested by the "restart accounting" command. [Action] None.	
27000011	E7	System accounting temporary stopped because accounting event congestion detected.
	Accounting event transmission is congested, and accounting of the login and logout commands was stopped temporarily. [Action] Using the "show accounting" command, make sure that the RADIUS server or TACACS+ server is not issuing errors. Check the configuration settings for the RADIUS server or TACACS+ server that is issuing errors. Additionally, make sure that the configurations on the RADIUS server or TACACS+ server side are correct. The congested state will be resolved when any of the following occur: 1. When the number of transmission queue accounting events decreases to 256, after transmission with the RADIUS server or TACACS+ server has recovered.	

Message ID	Event level	Message text
	Contents and actions	
	You can check the number of transmission queue accounting events by checking the item displayed in "InQueue" of the "show accounting" command. 2. When the "restart accounting" command is executed. 3. When the accounting-related configuration is changed as follows: aaa accounting exec, aaa accounting commands, commands related to radius-server, commands related to tacacs-server, ip address of the interface loopback mode	
	R7	System accounting recovered from congestion.
	The accounting event transmission has recovered from congestion, and accounting of login and logout commands resumed. [Action] None.	
27000013	E4	System accounting failed (<number> times).
	Accounting for the login and logout commands failed. This message appears at intervals when accounting fails. If accounting succeeds even once or no failure occurs for one hour, the failure count is cleared. <number>: Count of consecutive failures [Action] 1. Check if the configurations for RADIUS server or TACACS+ have been set. 2. Check the configuration to see if the IP address of the RADIUS server or TACACS+ server is correct. 3. Check the configurations to make sure that the port number for RADIUS server or TACACS+ server is correct.	
2a001000	E7	httpd aborted.
	The HTTP program (httpd) was forced to stop. [Action] The HTTP program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	httpd restarted.
	The HTTP program (httpd) has restarted. The device outputs this message when the HTTP program restarts automatically. [Action] None.	
2a001001	E3	httpd initialization failed(<reason>).
	An attempt to start the HTTP program (httpd) failed. <reason>: Reason for the failure • cannot bind to port <number> (TCP port <number> overlaps with other functions. If multiple TCP port numbers are overlapping, the first number detected is displayed.) [Action] After eliminating overlapping TCP port numbers, use the "restart web-authentication web-server" command to restart the HTTP program.	

2.4.8 30XXXXXX-3fXXXXXX

This section shows operation messages where the first two digits of message ID are 30 to 3f.

Table 2-11: Operation message for the event location SOFTWARE (30XXXXXX-)

Message ID	Event level	Message text
	Contents and actions	
3000b041	E7	dhcp_snoopingd aborted.
	The DHCP snooping program (dhcp_snoopingd) was forced to stop. DHCP snooping detected an anomaly such as a lack of memory, aborted the running, and forced the program to stop. [Action] The DHCP snooping program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	dhcp_snoopingd restarted.
	The DHCP snooping program (dhcp_snoopingd) has restarted. The switch outputs this message when the DHCP snooping program restarts automatically or a restart is executed by the "restart dhcp snooping" command. [Action] None.	
3000b042	E3	Discard of packets occurred by a reception rate limit of DHCP packets and ARP packets.
	Packets were discarded due to the reception rate limit for DHCP packets and ARP packets. [Action] None.	
3000b043	E3	Failed in binding database generate by binding entry exceeded(<mac address>/<vlan id>/<ip address>).
	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 device was exceeded. Review the system configuration. If this message is displayed due to addition of a static entry, delete the relevant static entry.	
3000b044	E3	The binding database can't be restored(<reason>).
	The binding database could not be restored. <reason>: Reason for the failure • File is not found. (A file was not found.) • May be broken. (The binding database might be corrupted.) • The data is not saved. (There is no restorable data.) [Action] Check the storage destination of the binding database.	

Message ID	Event level	Message text
	Contents and actions	
3000b045	E3	The binding database can't be stored(<reason>).
	The binding database could not be stored. <reason>: Reason for the failure • File is not writing. (Writing to the file is not possible.) [Action] Check the storage destination of the binding database.	
3000b046	E3	The binding database was restored from <url>.
	The binding database was restored. <url>: The binding database being read • previous process: The process before the restart • flash: Internal flash memory • mc: MC [Action] None.	
3000b047	E3	Failed in source guard setting by DHCP snooping (<mac address>/<vlan id>/<ip address>/<switch no.>/<nif no.>/<port no.>).
	The terminal filter setting failed. <mac address>/<vlan id>/<ip address>/<switch no.>/<nif no.>/<port no.>: Terminal filter setting information • <mac address>: MAC address • <vlan id>: VLAN ID • <ip address>: IP address • <switch no.>: Switch number • <nif no.>: NIF number • <port no.>: Port number [Action] The capacity limit of the device was exceeded. Review the system configuration.	
3000b048	E3	Failed in source garde setting of ChGr by DHCP snooping (<mac address>/<vlan id>/<ip address>/<channel group number>).
	The terminal filter setting failed. <mac address>/<vlan id>/<ip address>/<channel group number>: Terminal filter setting information • <mac address>: MAC address • <vlan id>: VLAN ID • <ip address>: IP address • <channel group number>: Channel group number [Action] The capacity limit of the device was exceeded. Review the system configuration.	

Message ID	Event level	Message text
	Contents and actions	
3e010001	E7	The event management program(eventManagerd) aborted.
	The event management program (eventManagerd) was forcibly terminated. [Action] The event management program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	The event management program(eventManagerd) restarted.
	The event management program (eventManagerd) has restarted. The switch outputs this message when the event management program restarts automatically or a restart is requested by the "restart event-manager" command. [Action] None.	
3e010003	E3	One or more event reports were discarded by the detector. (discard point = <point name>)
	The event notification was discarded by the monitoring program. After this message is output, this message for the same discard point will not be output until 15 minutes pass. <point name>: Discard point name • system message queue • high priority queue for script • normal priority queue for script • low priority queue for script • last priority queue for script • high priority queue for applet • normal priority queue for applet • low priority queue for applet • last priority queue for applet [Action] Execute as follows for each discard point. • system message queue If necessary, review the monitoring conditions for the operation message monitoring. It is output even if information that is not subject to monitoring is discarded. • high priority queue for script, normal priority queue for script, low priority queue for script, last priority queue for script, high priority queue for applet, normal priority queue for applet, low priority queue for applet, last priority queue for applet If necessary, review the notification priority settings for each monitoring event. After this message is output, this message for the same discard point will not be output until 15 minutes pass.	
3e010004	E3	One or more event reports were discarded by the script functionality. (name = <name>, PID = <pid>)
	The event notification was discarded by the script. <name>: Module name or file name of the script that discarded the event (if these names exceed 100 characters, the first 100 characters are displayed) <pid>: Process ID of the script that discarded the event [Action] Review the event monitoring reception processing of the target script.	

Message ID	Event level	Message text
	Contents and actions	
3e020001	E7	The script management program(scriptManagerd) aborted.
	The script management program (scriptManagerd) was forcibly terminated. [Action] The script management program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	The script management program(scriptManagerd) restarted.
	The script management program (scriptManagerd) has restarted. The switch outputs this message when the script management program restarts automatically or a restart is requested by the "restart script-manager" command. [Action] None.	
3e020003	E3	The resident script started. (script id = <id>)
	The resident script has started. <id>: Target resident script ID [Action] None.	
3e020004	E3	The resident script ended. (script id = <id>)
	The resident script has ended. <id>: Target resident script ID [Action] None.	
3e020005	E3	The resident script could not be started. (script id = <id>)
	Unable to start the resident script. <id>: Target resident script ID [Action] Check if the target script file is installed.	
3e020006	E3	The starting of the resident script was suppressed. (script id = <id>)
	The target resident script was restarted repeatedly, so the startup was suppressed. <id>: Target resident script ID [Action] Check whether there are any problems with the contents of the script file.	
3e020009	E3	The applet action script could not be started. (applet name = <applet name>, sequence = <sequence>)
	Unable to start the applet function action script. After this message is output, this message will not be output until 15 minutes pass or the target action definition is changed. <applet name>: Target applet name <sequence>: Target action sequence number [Action] Check if the target script file is installed.	

Message ID	Event level	Message text
	Contents and actions	
3f000001	E3	Loading MC-Configuration failed. (reason = <reason>)
	An attempt to read the MC information failed when starting up the device in memory card operation mode. <reason>: Reason for the failure • MC is not inserted. (A memory card was not inserted.) • File read failed. (An attempt to read the file failed.) [Action] Check access to the memory card according to the reason for failure.	
3f000002	E3	Changes detected on MC-Configuration. Restarting.
	The system will restart by memory card operation mode processing. [Action] None.	
3f000011	E3	Updating MC-Configuration is completed.
	The update of the running software and device information to the MC has been completed. [Action] None.	
3f000012	E3	Updating MC-Configuration failed. (reason = <reason>)
	An attempt to update the running software and device information to the MC failed. <reason>: Reason for the failure • Not enough space on MC. (There is not enough space on the memory card.) • File write failed. (An attempt to write the file failed.) • MC is not inserted. (A memory card was not inserted.) • MC is busy. (Another process is accessing the memory card. Wait a while, and then re-execute the command.) • Not start-up from flash memory(primary). (Normal startup from the internal flash memory has failed.) [Action] Check access to the memory card according to the reason for failure.	
3f000101	E3	Zero-touch-provisioning started.
	Device startup has started in zero-touch provisioning behavior mode. [Action] None.	
3f000102	E3	Changes detected on zero-touch-provisioning. Restarting.
	The system will restart by zero-touch provisioning behavior mode processing. [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
3f000103	E3	System started with zero-touch-provisioning.
	The system started up in zero-touch provisioning behavior mode. [Action] None.	
3f000104	E3	System started without zero-touch-provisioning. (reason = <reason>)
	The system started up in normal mode. <reason>: Reason for starting in normal mode • No configuration. (Zero-touch provisioning is disabled.) • Link down. (The zero-touch provisioning interface is down.) • Can't communicate with DHCP server. (The DHCP server is not responding.) • Invalid information. (The information obtained from the DHCP server is invalid.) • File get failed. (An attempt to obtain the file failed.) • File read failed. (An attempt to read the file failed.) • File write failed. (An attempt to write the file failed.) [Action] • If the reason of failure is "Link down." Please review the zero-touch provisioning interface. • If the reason of failure is "Can't communicate with DHCP server." or "Invalid information." Please review the DHCP server setting. • If the reason of failure is "File get failed." Please review the file server settings and the free space on the device. • If the reason of failure is "File read failed." or "File write failed." Please review the bulk file and the free space on the device.	
3f000201	E3	System zero-touch-provisioning is disabled, because mc-configuration has been enabled.
	Because the memory card operation mode was enabled, the excluding function zero-touch provisioning became disabled. [Action] None.	
3f000202	E3	System zero-touch-provisioning is enabled, because mc-configuration has been disabled.
	Because the memory card operation mode was disabled, the excluding function zero-touch provisioning became enabled. [Action] None.	

2.5 CONFIG

This section shows event location CONFIG operation messages.

Table 2-12: Operation message for the event location CONFIG

Message ID	Event level	Message text
	Contents and actions	
09300001	E3	This system started with the default configuration file. because the startup configuration file is not found or broken.
	Operation started with default setting information for one of the following reasons. • There is no startup configuration file or it cannot be read. • The number of times a device failure occurred and automatic recovery was performed reached 6 times within a certain period of time. [Action] 1. If you have saved the configuration file, use the "copy" command, and apply the saved configuration file to the startup configuration file. 2. If you have not saved the configuration file, create a new configuration file. 3. Check the log by executing the "show logging" command. If a problem is indicated in the log, take appropriate action according to the error message.	
09300002	E3	Configuration command syntax error. line <line number> : "<error syntax>"
	Application to the running configuration was skipped because a syntax error was detected in the startup configuration file. <line number>: Line number of the target configuration command <error syntax>: Syntax of the target configuration command [Action] Check the contents of the error.	
09300008	E3	Cannot set the automatic setting configuration command.:<command>
	Automatic setting of the configuration command failed. <command>: Command name [Action] Manually set the corresponding command.	
09600006	E3	Configuration access management error. process<process name>:pid<process id>:time <time>
	The lock was released and the device was automatically recovered because a process was accessing the configuration for a long time. <process name>: Occurrence process name <process id>: Occurrence process ID <time>: Occurrence time (day-of-the-week month day hour:minutes:seconds year) [Action] None.	

2.6 ACCESS

This section shows event location ACCESS operation messages.

Table 2-13: Operation message for the event location ACCESS

Message ID	Event level	Message text
	Contents and actions	
00000002	E3	Login incorrect <user name>.
	An attempt to log in by using the <user name> account was made, but the login was not allowed. <user name>: User name [Action] 1. There might have been an unauthorized access (failed account or password authentication) to the Switch from a remote host permitted at the console or the configuration. Check the operational status of the remote host that is permitted at the console or the configuration. 2. This log data is collected even when a legitimate user executes an incorrect operation during login. Therefore, even if this log message is collected, the operation of the remote host might be normal. 3. Check if the account was already registered for the Switch by using the "adduser" command. (Confirmation method: Check if the user has a home directory in ls /usr/home)	
00000003	E3	Login refused for too many users logged in.
	An attempt to connect via telnet or SSH 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.	
00005002	E3	Login <user name> from <host> (<term>).
	A user logged in. <user name>: User name <host>: Host ID • For a remote operation terminal: IP address • For a console terminal: console <term>: Terminal name • For a remote operation terminal: pts/0 or higher • For a console terminal: ttyS0 [Action] None.	
00005003	E3	Logout <user name> from <host> (<term>).
	A user logged out. <user name>: User name <host>: Host ID • For a remote operation terminal: IP address • For a console terminal: console	

Message ID	Event level	Message text
	Contents and actions	
	<term>: Terminal name • For a remote operation terminal: pts/0 or higher • For a console terminal: ttyS0 [Action] None.	
00010001	E3	SNMP agent program received packet from <ip address> with unexpected community name <community name>.
	The SNMP agent received a packet that had the unexpected community name <community name> from <ip address>. <ip address>: IP address of SNMP manager <community name>: Community name [Action] Access was attempted to the Switch from a location other than the locations permitted by the SNMP manager for the configuration. This message is output if the IP address and the community name of the SNMP manager do not match the IP address and the community name of an SNMP manager permitted for the configuration. Check the configuration to make sure that the IP address and the community name of the SNMP manager that accesses the Switch are identical to <ip address> and <community name>. If they do not match, invalid access might be occurring. Contact the administrator of the SNMP manager to tell the responsible party not to access the SNMP manager at <ip address>. The Switch suppresses repeated output to the operation log of accesses from an invalid IP address or community. A maximum of 16 invalid IP address are saved and, for each saved IP address, one out of every 128 invalid access attempts is output to the log.	
00030001	E3	Local authentication succeeded.
	Local authentication was performed and was successful for a user login request or request to change the administrator mode ("enable" command). [Action] None.	
00030002	E3	Local authentication failed.
	Local authentication was performed but authentication failed for a user login request or request to change the administrator mode ("enable" command). [Action] 1. An invalid attempt to access the Switch might have occurred for a remote host permitted by the configuration. Check the operational status of the remote host. 2. This log data is collected even when a legitimate user executes an incorrect operation (such as incorrect password entry) during login. Therefore, even if this log message is collected, the operation of the remote host might be normal.	
00030003	E3	RADIUS authentication accepted from <host>.
	RADIUS authentication was performed successfully for a user login request or request to change the administrator mode ("enable" command). <host>: IP address or host name of the RADIUS server [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
00030004	E3	RADIUS authentication rejected from <host>. "<message>"
	RADIUS authentication was attempted, but authentication failed for a user login request or request to change the administrator mode ("enable" command). <host>: IP address or host name of the RADIUS server <message>: RADIUS server response message [Action] 1. An invalid attempt to access the Switch might have occurred for a remote host permitted by the configuration. Check the operational status of the remote host. 2. This log data is collected even when a legitimate user executes an incorrect operation (such as incorrect password entry) during login. Therefore, even if this log message is collected, the operation of the remote host might be normal. 3. Check the RADIUS server setting.	
00030005	E3	RADIUS server (<host>) didn't response.
	RADIUS authentication was attempted for a user login request or request to change the administrator mode ("enable" command), but the RADIUS server did not respond. <host>: IP address or host name of the RADIUS server [Action] 1. Check the configuration to make sure that the RADIUS server IP address is correct. 2. Check the RADIUS server configuration to make sure that the RADIUS server port number is correct. 3. Make sure that the RADIUS server is turned on. 4. Make sure that the IP address of this Switch is registered for the client IP address on the RADIUS server side.	
00030006	E3	RADIUS server configuration is not defined.
	RADIUS authentication was attempted for a user login request or request to change the administrator mode ("enable" command), but a RADIUS server configuration has not been set up. [Action] 1. Check that a RADIUS configuration is set up. 2. Make sure that acct-only is specified for the RADIUS configuration and that authentication is not limited.	
00030007	E3	Invalid response received from <host>.
	RADIUS/TACACS+ authentication was attempted for a user login request or request to change the administrator mode ("enable" command), but the response from RADIUS/TACACS+ server was invalid. <host>: IP address or host name of RADIUS/TACACS+ server [Action] Make sure that the same RADIUS/TACACS+ key is specified for the Switch and the RADIUS/TACACS+ server.	
00030008	E3	RADIUS authentication failed.
	RADIUS authentication failed for a user login request or request to change the administrator mode ("enable" command) [Action] If any other operation log messages for RADIUS authentication were output, refer to them.	

Message ID	Event level	Message text
	Contents and actions	
0003000a	E3	Can't communicate with RADIUS server (<host>).
	Communication with the RADIUS server failed. <host>: IP address or host name of the RADIUS server [Action] 1. Make sure that there is a route to the RADIUS server. 2. If you are specifying a host name for the RADIUS server, make sure that name resolution can be performed.	
0003000b	E3	RADIUS authorization response with no contents.
	RADIUS command authorization was performed, but a command list was not properly obtained from the RADIUS server. [Action] Make sure that Class, Alaxala-Allow-Commands, and Alaxala-Deny-Commands are properly set in the RADIUS server settings (vendor-specific setting for the Switch).	
00030013	E3	TACACS+ authentication accepted from <host>.
	TACACS+ authentication was successfully performed for a user login request or request to change the administrator mode ("enable" command). <host>: IP address or host name of the TACACS+ server [Action] None.	
00030014	E3	TACACS+ authentication rejected from <host>.
	TACACS+ authentication was attempted for a user login request or request to change the administrator mode ("enable" command), but the TACACS+ server denied it. <host>: IP address or host name of the TACACS+ server [Action] 1. An invalid attempt to access the Switch might have occurred for a remote host permitted by the configuration. Check the operational status of the remote host. 2. This log data is collected even when a legitimate user executes an incorrect operation (such as incorrect password entry) during login. Therefore, the operation status of the remote host might be correct, even if this log data is collected. 3. Check the TACACS+ server setting.	
00030015	E3	TACACS+ server (<host>) didn't response.
	TACACS+ authentication and command authorization (if there is a command authorization specification in the TACACS+ configuration) were attempted for a user login request or request to change the administrator mode ("enable" command), but the TACACS+ server did not respond. <host>: IP address or host name of the TACACS+ server [Action] 1. Check the configuration to make sure that the TACACS+ server IP address is correct. 2. Make sure that the TACACS+ server is turned on.	

Message ID	Event level	Message text
	Contents and actions	
00030016	E3	TACACS+ server configuration is not defined.
	TACACS+ authentication was attempted for a user login request or request to change the administrator mode ("enable" command), but a TACACS+ server configuration did not exist. [Action] 1. Make sure that a TACACS+ configuration is set up. 2. Make sure that acct-only is specified for the TACACS+ configuration and the authentication is not limited.	
00030018	E3	TACACS+ authentication failed.
	TACACS+ authentication failed for a user login request or request to change the administrator mode ("enable" command). [Action] If any other operation log messages were output for TACACS+ authentication, refer to them.	
0003001a	E3	Can't communicate with TACACS+ server (<host>).
	Communication with the TACACS+ server failed. <host>: IP address or host name of the TACACS+ server [Action] 1. Make sure that there is a route to the TACACS+ server. 2. If you are specifying the TACACS+ server by using a host name, make sure that name resolution can be performed. 3. Check the TACACS+ server configuration to make sure that the TACACS+ server port number is correct. 4. Make sure that the TACACS+ server is turned on. 5. Make sure that the IP address of the Switch is registered for the client IP address on the TACACS+ server side.	
0003001b	E3	TACACS+ authorization response with no contents.
	TACACS+ command authorization was performed but a command list was not properly obtained from the TACACS+ server. [Action] Make sure that class, allow-commands, and deny-commands are properly set in the TACACS+ server settings (vendor-specific setting for the Switch).	
0003001c	E3	TACACS+ authorization rejected from <host>.
	TACACS+ command authorization was performed, but the TACACS+ server denied it. <host>: IP address or host name of the TACACS+ server [Action] 1. Make sure that the service name is correct in the TACACS+ server settings (vendor-specific setting for the Switch). 2. Check other settings on TACACS+ server side.	

Message ID	Event level	Message text
	Contents and actions	
0003001d	E3	Local authorization response with no contents.
	Local command authorization was performed, but there is no user name and corresponding command class or command list settings. [Action] Make sure that settings for the command class (username view-class) and the command list (username view, parser view, or commands exec) are set correctly for users authenticated using local login.	

2.7 SCRIPT

This section shows event location SCRIPT operation messages.

Table 2-14: Operation message for the event location SCRIPT

Message ID	Event level	Message text
	Contents and actions	
3e03****	*	<strings>
	Outputs the message text specified by sysmsg() of the Python action library as an operation message. Additionally, the * part of the event level and message ID outputs the numerical value specified by sysmsg(). <strings> Message text specified by sysmsg() [Action] Optional.	

2.8 PORT

This section shows event location PORT operation messages.

Table 2-15: Operation message for the event location PORT

Message ID	Event level	Message text
	Contents and actions	
25011000	E3	Port enabled administratively.
	The port was released from the disabled status by using the "no shutdown" configuration command. [Action] None.	
25011001	E4	Port up.
	The port is up. [Action] None.	
25011002	E4	Transceiver connected.
	A transceiver insertion was detected. [Action] None.	
25011006	E3	Port activated administratively.
	The port was released from the inactive status by using the "activate" command. [Action] None.	
25011100	E3	Port disabled administratively.
	The port was placed in the disabled status by using the "shutdown" or "schedule-power-control shutdown" configuration commands. [Action] None.	
25011101	E4	Error detected on the port.
	Errors were detected at the ports. [Action] For 10BASE-T/100BASE-TX/1000BASE-T/2.5GBASE-T: 1. Make sure that the specified cables are properly connected. 2. Make sure that startup of the remote device has completed. 3. Execute the "test interfaces" command, and make sure that the devices and transceivers have no problem. For 1000BASE-X/10GBASE-R: 1. Make sure that the specified cables are properly connected. Make sure that the end sections of the cables are clean. If they are dirty, clean them. 2. If an optical attenuator is used, check the attenuation value.	

Message ID	Event level	Message text
	Contents and actions	
	3. Make sure that startup of the remote device has completed. 4. Execute the "test interfaces" command, and make sure that the devices and transceivers have no problem.	
25011102	E4	Transceiver notconnected.
	A transceiver removal was detected. [Action] Insert the transceiver properly.	
25011103	E4	Auto negotiation failed.
	Auto negotiation has failed. [Action] • Check the auto negotiation status. • Execute the "test interfaces" command, and make sure that the devices and transceivers have no problem. • If the devices and transceivers are normal, check the cable and destination devices.	
25011104	E4	Many failures occurred in receiving frames to the targeted port due to the port troubles. Execute the Line tests to check the port condition.
	Frame reception at the corresponding port failed multiple times because of errors such as from noise. [Action] • Execute the "test interfaces" command, and make sure that the devices and transceivers have no problem. • If the devices and transceivers are normal, check the cable and destination devices.	
25011105	E4	Many failures occurred in sending frames to the targeted port due to the port troubles. Execute the Line tests to check the port condition.
	Frame transmission at the corresponding port failed multiple times because of errors such as from noise. [Action] • Execute the "test interfaces" command, and make sure that the devices and transceivers have no problem. • If the devices and transceivers are normal, check the cable and destination devices.	
25011106	E3	Port inactivated administratively.
	The port was placed in the inactive status by using the "inactivate" command. [Action] None.	
25011500	E4	Transceiver not supported.
	An unsupported transceiver was detected. [Action] See the transceiver description in the "Hardware Instruction Manual". Insert a supported transceiver into the corresponding port number.	

Message ID	Event level	Message text
	Contents and actions	
25020201	E8	Port restarted because of its hardware failure.
	A port was restarted because a hardware failure occurred at the port. [Action] Check subsequent failure recovery log entries or failure recovery failure log entries. If the system has recovered from the failure, operations can resume. If the recovery failed, switch to an unused port. If you want to reuse the failed port, replace the device. If a transceiver is used, make sure that it is firmly inserted.	
	R8	Port recovered from hardware failure.
	A port has recovered from a hardware failure. [Action] None.	
25020202	E8	Port stopped because of its hardware failure.
	A port was stopped because a hardware failure occurred at the port. [Action] Switch to an unused port. If you want to reuse the failed port, replace the device.	
25020401	E8	Port restarted, but not recovered from hardware failure.
	A port restarted, but the port has not recovered from a hardware failure. [Action] When using a transceiver: 1. After executing the "inactivate" command at a corresponding port, reinsert a transceiver after unplugging it, and execute the "activate" command. 2. Link up the line and check if the failure is resolved. 3. The system may not recover by executing step 2. In that case, change the transceiver after executing the "inactivate" command, and then execute the "activate" command. 4. Link up the line and check if the failure is resolved. 5. If the recovery failed after step 4, switch to an unused port. If you want to reuse the failed port, replace the device. When not using a transceiver: Switch to an unused port. If you want to reuse the failed port, replace the device.	
25100009	E4	Inactivated because of broadcast storm detection.
	A port was deactivated because a broadcast storm was detected. [Action] After recovering from the storm, use the "activate" command to change the port status to active.	
2510000a	E4	Broadcast storm detected.
	A broadcast storm was detected. [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
2510000b	E4	Broadcast storm recovered.
	The system has recovered from a broadcast storm. [Action] None.	
2510000c	E4	Inactivated because of multicast storm detection.
	A port was deactivated because a multicast storm was detected. [Action] After recovering from the storm, use the "activate" command to change the port status to active.	
2510000d	E4	Multicast storm detected.
	A multicast storm was detected. [Action] None.	
2510000e	E4	Multicast storm recovered.
	The system has recovered from a multicast storm. [Action] None.	
2510000f	E4	Inactivated because of unicast storm detection.
	A port was deactivated because a unicast storm was detected. [Action] After recovering from the storm, use the "activate" command to change the port status to active.	
25100010	E4	Unicast storm detected.
	A unicast storm was detected. [Action] None.	
25100011	E4	Unicast storm recovered.
	The system has recovered from a unicast storm. [Action] None.	
25100012	E4	Inactivated because of uni-directional link detection.
	A port was deactivated because a unidirectional link failure was detected. [Action] • Make sure that the IEEE 802.3ah/OAM function is valid at the connection target. • Execute the "test interfaces" command, and make sure that the devices and transceivers have no problem. • If the devices and transceivers are normal, check the cable and destination devices. After the above, activate the port by using the "activate" command.	

Message ID	Event level	Message text
	Contents and actions	
25100013	E4	Inactivated because of loop detection.
	A port was deactivated because a loop was detected. [Action] Check the network configuration.	
25100032	E4	Port activated by automatic restration of the storm-control function.
	The port status inactive was cleared due to automatic recovery of the storm control function. [Action] None.	
25230002	E3	Port half duplex does not support traffic-shape rate feature.
	The port bandwidth control is not available for half-duplex lines. [Action] Take one of the following actions: • If the port bandwidth control is to be used: Change to full duplex line. • If the half-duplex line is to be used: Delete the port bandwidth control by using the "no traffic-shape rate" configuration command.	

2.9 POE

This section shows event location POE operation messages.

Table 2-16: Operation message for the event location POE

Message ID	Event level	Message text
	Contents and actions	
39000001	E3	Initialization PoE configuration.
	Performs the PoE configuration settings. [Action] None.	
39000003	E3	<switch no.>/<nif no.>/<port no.> Supplying power was stopped by the overload detection.
	The power supply has been stopped due to detecting an overload. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Check the powered devices. If devices to which PoE power can be supplied are connected, use the "power inline" configuration command to disable the PoE function on the target port.	
39000004	E3	<switch no.>/<nif no.>/<port no.> Supplying power was stopped by the thermal shutdown.
	Power supply has been stopped because a temperature abnormality was detected in the PoE controller. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Review the installation environment of the device and reconnect.	
39000005	E3	<switch no.>/<nif no.>/<port no.> Supplying power was stopped by the PD disorder.(xxxx)
	Power supply has been stopped because a failure was detected in the powered device. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number (xxxx): Cause of power supply outage [Action] Execute the "activate power inline" command. If the power is not restored, check the powered device or cable, and reconnect.	
39000006	E3	<switch no.>/<nif no.>/<port no.> Unable to supply power by the power shortage.
	Power cannot be supplied due to a power shortage in the entire device. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] If you wish to supply power to this port, please use the "show power inline" command to check Threshold and Allocate, and reduce the number of connected powered devices so that Allocate falls below Threshold. Alternatively, use the "power inline" configuration command to change the priority. After reviewing the settings, please execute the "activate power inline" command.	

Message ID	Event level	Message text
	Contents and actions	
39000009	E8	Init controller failed.
	An attempt to configure PoE settings failed. [Action] None. The device will automatically restart.	
3900000a	E8	PoE controller access failed.(xxxx)
	An attempt to access the PoE controller failed. (xxxx): Cause code (information for manufacturer analysis) [Action] None. The device will automatically restart.	

2.10 MAC

This section shows event location MAC operation messages.

Table 2-17: Operation message for the event location MAC

Message ID	Event level	Message text
	Contents and actions	
20120002	E4	Channel Group(<channel group number>) is Up.
	The channel group status is UP. <channel group number>: Channel group number [Action] None.	
20120003	E4	Channel Group(<channel group number>) is Down - All port detached.
	All ports in the channel group are detached, and the channel group status is DOWN. <channel group number>: Channel group number [Action] For line connection status with remote devices: 1. Check whether the line is DOWN. 2. Check that the remote device LACP setting and line statuses are normal.	
20120004	E4	Channel Group(<channel group number>) is Down - The number of the detached port exceeded the configured number.
	The number of detached ports in the channel group exceeds the set limit, and the channel group status is DOWN. <channel group number>: Channel group number [Action] For line connection status with remote devices: 1. Check whether the line is DOWN. 2. Check that the remote device LACP setting and line statuses are normal.	
20120005	E3	Channel Group(<channel group number>) disabled administratively.
	A channel group was designated as disabled by the configuration. <channel group number>: Channel group number [Action] None.	
20120006	E3	Channel Group(<channel group number>) enabled administratively.
	A channel group was released from the disabled state by the configuration. <channel group number>: Channel group number [Action] None.	
20120007	E3	Port(<switch no.>/<nif no.>/<port no.>) detached from Channel Group(<channel group number>) - Different Partner System ID is detected.

Message ID	Event level	Message text
	Contents and actions	
	The system ID of a remote device does not match between the ports for LACP mode link aggregation, and the port was detached from the channel group. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] Check the following: 1. Is the connection with the remote device correct? 2. Is the system ID setting of the remote device correct?	
20120008	E3	Port(<switch no.>/<nif no.>/<port no.>) detached from Channel Group(<channel group number>) - Different Partner Key is detected.
	The key of a remote device does not match between the ports for LACP mode link aggregation, and the port was detached from the channel group. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] Check the following: 1. Is the connection with the remote device correct? 2. Is the key setting of the remote device correct?	
20120009	E3	Port(<switch no.>/<nif no.>/<port no.>) removed from Channel Group(<channel group number>).
	A port was detached from the channel group because of a configuration link deletion. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] None.	
20120010	E3	Port(<switch no.>/<nif no.>/<port no.>) detached from Channel Group(<channel group number>) - Port down.
	A line is DOWN, and the port was detached from the channel group. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] Check the line status.	
20120011	E3	Port(<switch no.>/<nif no.>/<port no.>) detached from Channel Group(<channel group number>) - Different Port data rate.
	Lines that have different data rates (speeds) exist in the channel group. Lines that have low data rates were detached from the channel group. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] For detached lines, check the settings of the Switch and remote devices.	

Message ID	Event level	Message text
	Contents and actions	
20120013	E3	Port(<switch no.>/<nif no.>/<port no.>) detached from Channel Group(<channel group number>) - Denied by the LACP partner.
	In LACP mode link aggregation, a connection from the remote device was denied due to LACP, and the port was detached from the channel group. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] Check the remote device status.	
20120014	E3	Port(<switch no.>/<nif no.>/<port no.>) detached from Channel Group(<channel group number>) - LACPDU timeout.
	In LACP mode link aggregation, the port did not receive an LACPDU from the remote device, and the port was detached from the channel group because of a timeout. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] Check the remote device status, which is active.	
20120015	E3	Port(<switch no.>/<nif no.>/<port no.>) detached from Channel Group(<channel group number>) - Configuration is changed.
	A port was detached from the channel group because of a configuration change. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] None.	
20120016	E3	Port(<switch no.>/<nif no.>/<port no.>) detached from Channel Group(<channel group number>) - Port moved is detected.
	A port was detached from the channel group because the port was moved in the channel group. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] None.	
20120017	E3	Port(<switch no.>/<nif no.>/<port no.>) detached from Channel Group(<channel group number>) - Partner Aggregation bit is FALSE.
	The application bit of the remote device in the LACP mode was false, and the port was detached from the channel group. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
20120018	E3	Port(<switch no.>/<nif no.>/<port no.>) detached from Channel Group(<channel group number>) - Partner Port number is changed.
	The port number of the remote device was changed, and the port was detached from the channel group. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] None.	
20120019	E3	Port(<switch no.>/<nif no.>/<port no.>) detached from Channel Group(<channel group number>) - Partner Port priority is changed.
	The port priority value of the remote device was changed, and the port was detached from the channel group. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] None.	
20120020	E3	Port(<switch no.>/<nif no.>/<port no.>) detached from Channel Group(<channel group number>) - Operation of detach port limit.
	A port was detached from the channel group because of a detach port limit. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] None.	
20120021	E3	Port(<switch no.>/<nif no.>/<port no.>) added to Channel Group(<channel group number>).
	A port was added to the channel group. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] None.	
20120022	E3	Port(<switch no.>/<nif no.>/<port no.>) attached to Channel Group(<channel group number>).
	A port was aggregated to the channel group. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] None.	
20120023	E3	Port(<switch no.>/<nif no.>/<port no.>) attached to Channel Group(<channel group number>) - A standby port became active.
	Operation by a standby link has started. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number	

Message ID	Event level	Message text
	Contents and actions	
	<channel group number>: Channel group number [Action] None.	
20120024	E3	Port(<switch no.>/<nif no.>/<port no.>) detached from Channel Group(<channel group number>) - This port became a standby port.
	Operation by a standby link stopped. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] None.	

2.11 VLAN

This section shows event location VLAN operation messages.

2.11.1 2011XXXX

This section shows operation messages where the first four digits of message ID are 2011.

Table 2-18: Operation message for the event location VLAN (2011XXXX)

Message ID	Event level	Message text
	Contents and actions	
20110002	E3	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.	
20110003	E3	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.	
20110006	E3	STP(<mode>): Topology change detected - BPDU Timeout detected on the root port(<switch no.>/<nif no.>/<port no.>).
	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 <mst instance id>: Multiple Spanning Tree (MSTI) and MST instance ID <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Check the line status.	
20110007	E3	STP(<mode>): Topology change detected - Topology Change Notification BPDU received on the port(<switch no.>/<nif no.>/<port no.>).
	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 <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number	

Message ID	Event level	Message text
	Contents and actions	
	[Action] Check the line status.	
20110008	E4	STP(<mode>): Port status becomes Forwarding on the port(<switch no.>/<nif no.>/<port no.>).
	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 <mst instance id>: Multiple Spanning Tree (MSTI) and MST instance ID <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] None.	
20110009	E4	STP(<mode>): Port status becomes Blocking on the port(<switch no.>/<nif no.>/<port no.>).
	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 <mst instance id>: Multiple Spanning Tree (MSTI) and MST instance ID <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] None.	
20110010	E4	STP(<mode>): Port status becomes Down- BPDU received on the BPDU GUARD port(<switch no.>/<nif no.>/<port no.>).
	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 <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Check the line status.	

Message ID	Event level	Message text
	Contents and actions	
20110011	E3	STP(<mode>): Spanning Tree Protocol enabled - BPDU received on the Port Fast(<switch no.>/<nif no.>/<port no.>).
	A port has become subject to the Spanning Tree Protocol because the port was set with the Port-Fast 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 <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Check the line status.	
20110012	E3	STP (<mode>) : Topology change detected - BPDU Timeout detected on the root port(ChGr:<channel group number>).
	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 <mst instance id>: Multiple Spanning Tree (MSTI) and MST instance ID <channel group number>: Channel group number [Action] Check the line status.	
20110013	E3	STP (<mode>) : Topology change detected - Topology Change Notification BPDU received on the port(ChGr:<channel group number>).
	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 number>: Channel group number [Action] Check the line status.	
20110014	E3	STP (<mode>) : Spanning Tree Protocol enabled - BPDU received on the Port Fast(ChGr:<channel group number>).
	A port has become subject to the Spanning Tree Protocol because the port was set with the Port-Fast 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 number>: Channel group number [Action] Check the line status.	

Message ID	Event level	Message text
	Contents and actions	
20110015	E4	STP (<mode>) : Port status becomes Forwarding on the port(ChGr:<channel group number>).
	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 <mst instance id>: Multiple Spanning Tree (MSTI) and MST instance ID <channel group number>: Channel group number [Action] None.	
20110016	E4	STP (<mode>) : Port status becomes Blocking on the port(ChGr:<channel group number>).
	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 <mst instance id>: Multiple Spanning Tree (MSTI) and MST instance ID <channel group number>: Channel group number [Action] None.	
20110017	E4	STP (<mode>) : Port status becomes Down- BPDU received on the BPDU GUARD port(ChGr:<channel group number>).
	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 number>: Channel group number [Action] Check the line status.	
20110022	E3	STP : Cleared MAC Address Table entry.
	A MAC Address Table entry was cleared because a topology change BPDU was received. [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
20110023	E3	STP(<mode>): Topology change detected - BPDU Timeout detected on the alternate port(<switch no.>/<nif no.>/<port no.>).
	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 <mst instance id>: Multiple Spanning Tree (MSTI) and MST instance ID <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Check the line status.	
20110024	E3	STP(<mode>): Topology change detected - BPDU Timeout detected on the backup port(<switch no.>/<nif no.>/<port no.>).
	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 <mst instance id>: Multiple Spanning Tree (MSTI) and MST instance ID <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Check the line status.	
20110025	E3	STP (<mode>) : Topology change detected - BPDU Timeout detected on the alternate port(ChGr:<channel group number>).
	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 <mst instance id>: Multiple Spanning Tree (MSTI) and MST instance ID <channel group number>: Channel group number [Action] Check the line status.	

Message ID	Event level	Message text
	Contents and actions	
20110026	E3	STP (<mode>) : Topology change detected - BPDU Timeout detected on the backup port(ChGr:<channel group number>).
	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 <mst instance id>: Multiple Spanning Tree (MSTI) and MST instance ID <channel group number>: Channel group number [Action] Check the line status.	
20110027	E3	STP(MST): This bridge becomes the CIST Root Bridge.
	The Switch has become the CIST root bridge. [Action] None.	
20110028	E3	STP(CIST): This bridge becomes the CIST Regional Root Bridge.
	The Switch has become the CIST regional root bridge. [Action] None.	
20110029	E3	STP(MST Instance <mst instance id>): This bridge becomes the MSTI Regional Root Bridge.
	The Switch has become the MSTI regional root bridge. <mst instance id>: MST instance ID [Action] None.	
20110031	E3	STP(CIST): This bridge becomes the CIST Regional Designated Bridge.
	The Switch has become the CIST regional designated bridge. [Action] None.	
20110032	E3	STP(MST Instance <mst instance id>): This bridge becomes the MSTI Regional Designated Bridge.
	The Switch has become the MSTI regional designated bridge. <mst instance id>: MST instance ID [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
20110037	E4	STP (<mode>) : Port status becomes Blocking on the port(<switch no.>/<nif no.>/<port no.>), because IEEE802.1Q Tagged BPDU was received from the port which is not 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 IEEE 802.1Q VLAN 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 <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Check the settings of the partner device.	
20110038	E4	STP (<mode>) : Port status becomes Blocking on the port(ChGr:<channel group number>), because IEEE802.1Q Tagged BPDU was received from the port which is not 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 IEEE 802.1Q VLAN 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 number>: Channel group number [Action] Check the settings of the partner device.	
20110039	E4	STP : Exceeded the number of the maximum spanning tree.
	The number of trees exceed 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.	
20110040	E4	STP(<mode>): Port status becomes Blocking - BPDU that priority is high was received on the ROOT GUARD port(<switch no.>/<nif no.>/<port no.>).
	A port was placed in the Blocking status because it was set with the root 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 <mst instance id>: Multiple Spanning Tree (MSTI) and MST instance ID <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Check the settings of the partner device.	

Message ID	Event level	Message text
	Contents and actions	
20110041	E4	STP(<mode>): Port status becomes Blocking - BPDU that priority is high was received on the ROOT GUARD port(ChGr:<channel group number>).
	A port was placed in the Blocking status because it was set with the root 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 <mst instance id>: Multiple Spanning Tree (MSTI) and MST instance ID <channel group number>: Channel group number [Action] Check the settings of the partner device.	

2.11.2 2013XXXX (GSRP aware)

This section shows operation messages where the first four digits of message ID are 2013.

Table 2-19: Operation message for the event location VLAN (2013XXXX)

Message ID	Event level	Message text
	Contents and actions	
20130015	E3	GSRP aware : MAC Address Table entry cleared, because GSRP flush request received on port <port list>, GSRP <gsrp group id> VLAN group <vlan group id> Source MAC address <mac address>.
	The GSRP flush request frame was received, and the MAC address table was cleared. <port list>: Port range <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID <mac address>: MAC address [Action] None.	
20130019	E3	MAC Address Table entry cleared, because flush request received on port <port list>, Source MAC address <mac address>.
	The MAC address table was cleared because a Flush Request frame was received. <port list>: Port range <mac address>: Device MAC address of the frame-sending source [Action] None.	

2.11.3 2017XXXX (Ring Protocol)

This section shows operation messages where the first four digits of message ID are 2017.

Table 2-20: Operation message for the event location VLAN (2017XXXX)

Message ID	Event level	Message text
	Contents and actions	
20170003	E3	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. <ring id>: Ring ID [Action] None.	
20170005	E3	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 output. <ring id>: Ring ID [Action] None.	
20170014	E3	AXRP(virtual-link <link id>) : cleared MAC address table by receiving flush frames.
	A virtual link flush control frame was received with Ring Protocol, and MAC address table entries were cleared. This message is for the clearing of MAC address table entries for learning at all ring ports. <link id>: Virtual link ID [Action] None.	
20170021	E3	AXRP (multi-fault-detection <ring id>) : cleared MAC address table by receiving flush frames.
	A multi-failure flush control frame was received, and the MAC address table was cleared. A flush control frame for multiple failures is a flash control frame that only clears the MAC address table sent by the shared node when the multi-fault monitoring function is enabled. <ring id>: Ring ID [Action] None.	
20170024	E4	AXRP : logical inconsistency occurred.
	An internal state conflict occurred in the Ring Protocol. [Action] Please execute the "restart axrp" command to restart the Ring Protocol program.	

2.11.4 2080XXXX (L2 loop detection)

This section shows operation messages where the first four digits of message ID are 2080.

Table 2-21: Operation message for the event location VLAN (2080XXXX)

Message ID	Event level	Message text
	Contents and actions	
20800001	E4	L2LD : Port(<switch no.>/<nif no.>/<port no.>) inactivated because of loop detection from port(<switch no.>/<nif no.>/<port no.>).
	The active port has been blocked because a loop failure was detected. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Check the network configuration.	
20800002	E4	L2LD : Port(<switch no.>/<nif no.>/<port no.>) inactivated because of loop detection from ChGr(<channel group number>).
	The active port has been blocked because a loop failure was detected. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] Check the network configuration.	
20800003	E4	L2LD : ChGr(<channel group number>) inactivated because of loop detection from port(<switch no.>/<nif no.>/<port no.>).
	The active port has been blocked because a loop failure was detected. <channel group number>: Channel group number <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Check the network configuration.	
20800004	E4	L2LD : ChGr(<channel group number>) inactivated because of loop detection from ChGr(<channel group number>).
	The active port has been blocked because a loop failure was detected. <channel group number>: Channel group number [Action] Check the network configuration.	
20800005	E4	L2LD : Port(<switch no.>/<nif no.>/<port no.>) loop detection from port(<switch no.>/<nif no.>/<port no.>).
	A loop failure was detected. Loop failure detection logs are not output for the same port or channel group for one minute after the loop failure detection logs (20800005 to 20800008) are output. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Check the network configuration.	

Message ID	Event level	Message text
	Contents and actions	
20800006	E4	L2LD : Port(<switch no.>/<nif no.>/<port no.>) loop detection from ChGr(<channel group number>).
	A loop failure was detected. Loop failure detection logs are not output for the same port or channel group for one minute after the loop failure detection logs (20800005 to 20800008) are output. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] Check the network configuration.	
20800007	E4	L2LD : ChGr(<channel group number>) loop detection from port(<switch no.>/<nif no.>/<port no.>).
	A loop failure was detected. Loop failure detection logs are not output for the same port or channel group for one minute after the loop failure detection logs (20800005 to 20800008) are output. <channel group number>: Channel group number <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Check the network configuration.	
20800008	E4	L2LD : ChGr(<channel group number>) loop detection from ChGr(<channel group number>).
	A loop failure was detected. Loop failure detection logs are not output for the same port or channel group for one minute after the loop failure detection logs (20800005 to 20800008) are output. <channel group number>: Channel group number [Action] Check the network configuration.	
20800009	E4	L2LD : Port(<switch no.>/<nif no.>/<port no.>) activate by automatic restoration of the L2loop detection function.
	The port status inactive was cleared due to automatic recovery of the L2 loop detection function. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] None.	
20800010	E4	L2LD : ChGr(<channel group number>) activate by automatic restoration of the L2loop detection function.
	The port status inactive was cleared due to automatic recovery of the L2 loop detection function. <channel group number>: Channel group number [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
20800011	E4	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 exceed 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.	

2.11.5 2090XXXX (CFM)

This section shows operation messages where the first four digits of message ID are 2090.

Table 2-22: Operation message for the event location VLAN (2090XXXX)

Message ID	Event level	Message text
	Contents and actions	
20900003	E4	MD Level <level> MA <no.>: detected on fault of OtherCCM in MEP <mep-id>.
	The relevant MEP detected a failure (OtherCCM). <level>: Domain level <no.>: MA identification number <mepid>: MEP ID [Action] A partner device is not recognized as the same MA. Check that the domain level, MA ID, domain name, and MA name match the partner devices.	
20900004	E4	MD Level <level> MA <no.>: detected on fault of ErrorCCM in MEP <mep-id>.
	The relevant MEP detected a failure (ErrorCCM). <level>: Domain level <no.>: MA identification number <mepid>: MEP ID [Action] A partner device and the configuration do not match. Check whether the MEP ID is different from the partner device, and make sure the send interval (interval) matches that of the partner device.	
20900005	E4	MD Level <level> MA <no.>: detected on fault of Timeout in MEP <mepid>.
	The relevant MEP detected a failure (Timeout). <level>: Domain level <no.>: MA identification number <mepid>: MEP ID [Action] The switch is not receiving CCM from partner devices. Check the network status.	

Message ID	Event level	Message text
	Contents and actions	
20900006	E4	MD Level <level> MA <no.>: detected on fault of PortState in MEP <mepid>.
	The relevant MEP detected a failure (PortState). <level>: Domain level <no.>: MA identification number <mepid>: MEP ID [Action] A partner device line failure or a port blocking status was detected. Check the status of the partner device.	
20900007	E4	MD Level <level> MA <no.>: detected on fault of RDI in MEP <mepid>.
	The relevant MEP detected a failure (RDI). <level>: Domain level <no.>: MA identification number <mepid>: MEP ID [Action] A failure was detected in a partner device. Check the status of the partner device.	
20900008	E4	Exceeded the number of the maximum port.
	The number of ports exceeds the number for which MEP and MIP can be set. [Action] Check the number of settings.	

2.11.6 2110XXXX-2120XXXX

This section shows operation messages where the first four digits of message ID are 2110 to 2120.

Table 2-23: Operation message for the event location VLAN (2110XXXX-)

Message ID	Event level	Message text
	Contents and actions	
21100001	E3	IGMP snooping: IGMP querier changed on VLAN <vlan id> - lost IGMP querier address <ipv4 address>.
	An advertisement (IGMPQuery) from the IGMP querier <ipv4 address> on a VLAN (<vlan id>) has disappeared. The IGMP querier information is deleted. The availability of the IPv4 multicast group member (recipient host) cannot be checked, and IPv4 multicast data forwarding is not properly executed. <vlan id>: VLAN ID <ipv4 address>: IPv4 address [Action] 1. Check the connection with the IGMP querier <ipv4 address>. 2. Check if the IGMP querier change message (message ID is 21100002) was output. 3. If the connection with the IGMP querier cannot be checked, execute the "ip igmp snooping querier" configuration command to enable the IGMP querier function of the Switch.	

Message ID	Event level	Message text
	Contents and actions	
21100002	E3	IGMP snooping: IGMP querier changed on VLAN <vlan id> - new IGMP querier address <ipv4 address>.
	An 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.	
21100003	E3	IGMP snooping: IPv4 address not defined on VLAN <vlan id>, IGMP querier function stopped.
	An IGMP querier on the VLAN (<vlan id>) was stopped because the IPv4 address is not set. <vlan id>: VLAN ID [Action] 1. Set an IPv4 addresses for the appropriate VLAN. 2. Execute the "show igmp-snooping" command to check that the IPv4 address set for the appropriate VLAN is displayed.	
21100004	E3	IGMP snooping: The number of the IGMP snooping entry exceeded the capacity of this system.
	The number of learn entries used in IGMP snooping exceeds the capacity limit of the device. [Action] The number of entries exceeds the capacity limit. Review the system configuration and setting so that you can reduce the number of entries.	
21100005	E4	The IGMP snooping entry can't be registered at hardware tables(VLAN:<vlan id> MAC address:<mac address>).
	An IGMP snooping entry cannot be set in a hardware table. <vlan id>: VLAN ID <mac address>: MAC address [Action] Review the system configuration. However, depending on the hardware specification, the setting to the maximum of the capacity limit might not be available.	
21100008	E3	IGMP snooping: The number of the dynamic mrouter-port exceeded the capacity of this system.
	Learning is not possible because the number of automatically learned multicast router ports exceeds the capacity limit. [Action] Delete unnecessary multicast router information or review the configuration.	

Message ID	Event level	Message text
	Contents and actions	
21100009	E3	IGMP snooping: Multicast router(<type>:<ipv4 address>) found on port <switch no.>/<nif no.>/<port no.> of VLAN <vlan id>.
	A multicast router was detected. <type>: Detection means (IGMP, PIM) <ipv4 address>: IPv4 address <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID [Action] None.	
21100010	E3	IGMP snooping: Multicast router(<type>:<ipv4 address>) found on ChGr <channel group number> of VLAN <vlan id>.
	A multicast router was detected. <type>: Detection means (IGMP, PIM) <ipv4 address>: IPv4 address <channel group number>: Channel group number <vlan id>: VLAN ID [Action] None.	
21100011	E3	IGMP snooping: Multicast router(<type>:<ipv4 address>) lost on port <switch no.>/<nif no.>/<port no.> of VLAN <vlan id>.
	The multicast router was deleted. <type>: Detection means (IGMP, PIM) <ipv4 address>: IPv4 address <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <vlan id>: VLAN ID [Action] None.	
21100012	E3	IGMP snooping: Multicast router(<type>:<ipv4 address>) lost on ChGr <channel group number> of VLAN <vlan id>.
	The multicast router was deleted. <type>: Detection means (IGMP, PIM) <ipv4 address>: IPv4 address <channel group number>: Channel group number <vlan id>: VLAN ID [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
21200001	E3	MLD snooping: MLD querier changed on VLAN <vlan id> - lost MLD querier address <ipv6 address>.
	The MLD querier information was deleted because an advertisement (MLD Query) from the MLD querier <ipv6 address> on a VLAN (<vlan id>) disappeared. The IPv6 multicast data will not be properly relayed because the existence of the IPv6 multicast group listener (recipient host) cannot be checked. <vlan id>: VLAN ID <ipv6 address>: IPv6 address [Action] 1. Check the connection with the MLD querier <ipv6 address>. 2. Check if the MLD querier change message (message ID is 21200002) was output. 3. If the connection with the MLD querier cannot be checked, execute the "ipv6 mld snooping querier" configuration command to enable the MLD querier function of the Switch.	
21200002	E3	MLD snooping: MLD querier changed on VLAN <vlan id> - new MLD querier address <ipv6 address>.
	An 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.	
21200003	E3	MLD snooping: IPv6 address not defined on VLAN <vlan id>, MLD querier function stopped.
	An MLD querier on the VLAN (<vlan id>) was stopped because the IPv6 address is not set. <vlan id>: VLAN ID [Action] 1. Set an IPv6 addresses for the appropriate VLAN. 2. Execute the "show mld-snooping" command to check that the IPv6 address set for the appropriate VLAN is displayed.	
21200004	E3	MLD snooping: The number of the MLD snooping entry exceeded the capacity of this system.
	The number of learn entries used in MLD snooping exceeds the capacity limit of the device. [Action] The number of entries exceeds the capacity limit. Review the system configuration and setting so that you can reduce the number of entries.	

Message ID	Event level	Message text
	Contents and actions	
21200005	E4	The MLD snooping entry can't be registered at hardware tables(VLAN:<vlan id> MAC address:<mac address>).
	An MLD snooping entry cannot be set in a hardware table. <vlan id>: VLAN ID <mac address>: MAC address [Action] Review the system configuration. However, depending on the hardware specification, the setting to the maximum of the capacity limit might not be available.	

2.11.7 2510XXXX

This section shows operation messages where the first four digits of message ID are 2510.

Table 2-24: Operation message for the event location VLAN (2510XXXX)

Message ID	Event level	Message text
	Contents and actions	
25100001	E4	VLAN (<vlan id>) Status is Up.
	The VLAN status is UP. <vlan id>: VLAN ID [Action] None.	
25100002	E4	VLAN (<vlan id>) Status is Down.
	The VLAN status is DOWN. <vlan id>: VLAN ID [Action] Each line status check that belongs to VLAN.	
25100005	E4	The mac-address-table static entry can't be registered at hardware tables(VLAN:<vlan id> MAC address:<mac address>).
	A mac-address-table static configuration entry cannot be set in a hardware table. <vlan id>: VLAN ID <mac address>: MAC address [Action] Review the system configuration. However, depending on the hardware specification, the setting to the maximum of the capacity limit might not be available. In that case, review the parameter of the "system l2-table mode" configuration command.	

Message ID	Event level	Message text
	Contents and actions	
25100007	E4	Protocol based VLAN (<vlan id>) registration failed on the port(<switch no.>/<nif no.>/<port no.>).
	A protocol VLAN could not be set up. You attempted to use a specification that duplicated another VLAN for which a protocol was already specified. <vlan id>: VLAN ID <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Review the system configuration.	
2510001b	E3	Sum of number of VLAN on ports exceeded capacity.
	The total number of VLANs for each port exceed the capacity limit. [Action] Change the total number of VLANs to within the capacity limit, and restart the device.	
25100021	E4	The vlan-protocol <protocol name> registration failed on the VLAN <vlan id>.
	The setting of a protocol for the protocol VLAN failed. You attempted to use a specification that duplicated a protocol already set for the port. <protocol name>: Name of the protocol that you are attempting to add <vlan id>: VLAN ID [Action] Review the system configuration.	
25100022	E4	Protocol <frame type> registration failed on the vlan-protocol <protocol name>.
	The setting of a protocol value used for the VLAN protocol failed. You attempted to use a specification that duplicated a protocol already set for the port. <frame type>: Frame type of the protocol that you are attempting to add • ethertype <hex>: EtherType value of Ethernet V2-format frame • llc <hex>: LLC value (DSAP, SSAP) of 802.3-format frame • snap-ethertype <hex>: EtherType value of 802.3-format frame <protocol name>: Protocol name [Action] Review the system configuration.	

2.12 ULR

This section shows event location ULR operation messages.

Table 2-25: Operation message for the event location ULR

Message ID	Event level	Message text
	Contents and actions	
20a00001	E4	ULR:Active port is switched to secondary port(<switch no.>/<nif no.>/<port no.>) from primary port(<switch no.>/<nif no.>/<port no.>).
	The active port was switched to the secondary port because an error occurred in the primary port. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Check the failure in the primary port.	
20a00002	E4	ULR:Active port is switched to primary port(<switch no.>/<nif no.>/<port no.>) from secondary port(<switch no.>/<nif no.>/<port no.>).
	The active port was switched to the primary port because an error occurred in the secondary port. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Check the failure in the secondary port.	
20a00003	E4	ULR:Active port is switched to secondary port(<switch no.>/<nif no.>/<port no.>) from primary port(ChGr:<channel group number>).
	The active port was switched to the secondary port because an error occurred in the primary port. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] Check the failure in the primary port.	
20a00004	E4	ULR:Active port is switched to primary port(<switch no.>/<nif no.>/<port no.>) from secondary port(ChGr:<channel group number>).
	The active port was switched to the primary port because an error occurred in the secondary port. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] Check the failure in the secondary port.	
20a00005	E4	ULR:Active port is switched to secondary port(ChGr:<channel group number>) from primary port(<switch no.>/<nif no.>/<port no.>).
	The active port was switched to the secondary port because an error occurred in the primary port. <channel group number>: Channel group number <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Check the failure in the primary port.	

Message ID	Event level	Message text
	Contents and actions	
20a00006	E4	ULR:Active port is switched to primary port(ChGr:<channel group number>) from secondary port(<switch no.>/<nif no.>/<port no.>).
	The active port was switched to the primary port because an error occurred in the secondary port. <channel group number>: Channel group number <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Check the failure in the secondary port.	
20a00007	E4	ULR:Active port is switched to secondary port(ChGr:<channel group number>) from primary port(ChGr:<channel group number>).
	The active port was switched to the secondary port because an error occurred in the primary port. <channel group number>: Channel group number [Action] Check the failure in the primary port.	
20a00008	E4	ULR:Active port is switched to primary port(ChGr:<channel group number>) from secondary port(ChGr:<channel group number>).
	The active port was switched to the primary port because an error occurred in the secondary port. <channel group number>: Channel group number [Action] Check the failure in the secondary port.	
20a00009	E4	ULR:Active port is switched to secondary port(<switch no.>/<nif no.>/<port no.>) from primary port(<switch no.>/<nif no.>/<port no.>), because command execution.
	The active port was switched from the primary port to the secondary port because the "set switch-port-backup active" command was executed. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] None.	
20a00010	E4	ULR:Active port is switched to primary port(<switch no.>/<nif no.>/<port no.>) from secondary port(<switch no.>/<nif no.>/<port no.>), because command execution.
	The active port was switched back from the secondary port to the primary port because the "set switchport-backup active" command was executed. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
20a00011	E4	ULR:Active port is switched to secondary port(<switch no.>/<nif no.>/<port no.>) from primary port(ChGr:<channel group number>), because command execution.
	The active port was switched from the primary port to the secondary port because the "set switchport-backup active" command was executed. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] None.	
20a00012	E4	ULR:Active port is switched to primary port(<switch no.>/<nif no.>/<port no.>) from secondary port(ChGr:<channel group number>), because command execution.
	The active port was switched back from the secondary port to the primary port because the "set switchport-backup active" command was executed. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] None.	
20a00013	E4	ULR:Active port is switched to secondary port(ChGr:<channel group number>) from primary port(<switch no.>/<nif no.>/<port no.>), because command execution.
	The active port was switched from the primary port to the secondary port because the "set switchport-backup active" command was executed. <channel group number>: Channel group number <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] None.	
20a00014	E4	ULR:Active port is switched to primary port(ChGr:<channel group number>) from secondary port(<switch no.>/<nif no.>/<port no.>), because command execution.
	The active port was switched back from the secondary port to the primary port because the "set switchport-backup active" command was executed. <channel group number>: Channel group number <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] None.	
20a00015	E4	ULR:Active port is switched to secondary port(ChGr:<channel group number>) from primary port(ChGr:<channel group number>), because command execution.
	The active port was switched from the primary port to the secondary port because the "set switchport-backup active" command was executed. <channel group number>: Channel group number	

Message ID	Event level	Message text
	Contents and actions	
	[Action] None.	
20a00016	E4	ULR:Active port is switched to primary port (ChGr:<channel group number>) from secondary port (ChGr:<channel group number>), because command execution.
	The active port was switched back from the secondary port to the primary port because the "set switchport-backup active" command was executed. <channel group number>: Channel group number [Action] None.	
20a00017	E4	ULR:Primary port(<switch no.>/<nif no.>/<port no.>) became the active port.
	The primary port has become the active port. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] None.	
20a00018	E4	ULR:Primary port(ChGr:<channel group number>), became the active port.
	The primary port has become the active port. <channel group number>: Channel group number [Action] None.	
20a00019	E4	ULR:Secondary port(<switch no.>/<nif no.>/<port no.>) became the active port.
	The secondary port has become the active port. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] None.	
20a00020	E4	ULR:Secondary port(ChGr:<channel group number>) became the active port.
	The secondary port has become the active port. <channel group number>: Channel group number [Action] None.	
20a00021	E4	ULR:Both uplink redundant port(<switch no.>/<nif no.>/<port no.>) and port(<switch no.>/<nif no.>/<port no.>) are down.
	Both the primary port and the secondary port have gone down. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Make sure that no error occurred between the primary and secondary port.	

Message ID	Event level	Message text
	Contents and actions	
20a00022	E4	ULR:Both uplink redundant port(<switch no.>/<nif no.>/<port no.>) and port(ChGr:<channel group number>) are down.
	Both the primary port and the secondary port have gone down. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] Make sure that no error occurred between the primary and secondary port.	
20a00023	E4	ULR:Both uplink redundant port(ChGr:<channel group number>) and port(<switch no.>/<nif no.>/<port no.>) are down.
	Both the primary port and the secondary port have gone down. <channel group number>: Channel group number <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Make sure that no error occurred between the primary and secondary port.	
20a00024	E4	ULR:Both uplink redundant port(ChGr:<channel group number>) and port(ChGr:<channel group number>) are down.
	Both the primary port and the secondary port have gone down. <channel group number>: Channel group number [Action] Make sure that no error occurred between the primary and secondary port.	
20a00025	E4	ULR:Active port is switched to primary port(<switch no.>/<nif no.>/<port no.>) from secondary port(<switch no.>/<nif no.>/<port no.>), because preemption execution.
	The active port was switched from the secondary port to the primary port because automatic preemption was executed. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] None.	
20a00026	E4	ULR:Active port is switched to primary port(<switch no.>/<nif no.>/<port no.>) from secondary port(ChGr:<channel group number>), because preemption execution.
	The active port was switched from the secondary port to the primary port because automatic preemption was executed. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <channel group number>: Channel group number [Action] None.	
20a00027	E4	ULR:Active port is switched to primary port(ChGr:<channel group number>) from secondary port(<switch no.>/<nif no.>/<port no.>), because preemption execution.

Message ID	Event level	Message text
	Contents and actions	
	The active port was switched from the secondary port to the primary port because automatic preemption was executed. <channel group number>: Channel group number <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] None.	
20a00028	E4	ULR:Active port is switched to primary port(ChGr:<channel group number>) from secondary port(ChGr:<channel group number>), because preemption execution.
	The active port was switched from the secondary port to the primary port because automatic preemption was executed. <channel group number>: Channel group number [Action] None.	
20a00029	E4	ULR:Exceeded the number of MAC Address Table entry update request to uplink-switch from active port(<switch no.>/<nif no.>/<port no.>).
	The number of MAC address table entry update requests from an uplink port of the Switch to an upstream uplink switch exceeded the limit. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] None.	
20a00030	E4	ULR:Exceeded the number of MAC Address Table entry update request to uplink-switch from active port(ChGr:<channel group number>).
	The number of MAC address table entry update requests from an uplink port of the Switch to an upstream uplink switch exceeded the limit. <channel group number>: Channel group number [Action] None.	
20a00031	E4	ULR:Port(<switch no.>/<nif no.>/<port no.>) inactivated because of 'reset-flush-port'.
	The port was deactivated by the port resetting. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] None.	
20a00032	E4	ULR:ChGr(<channel group number>) inactivated because of 'reset-flush-port'.
	The port was deactivated by the port resetting. <channel group number>: Channel group number [Action] None.	

Message ID	Event level	Message text
	Contents and actions	
20a00033	E4	ULR:Port(<switch no.>/<nif no.>/<port no.>) activated because of 'reset-flush-port'.
	The port was released from the inactive status by the port resetting. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] None.	
20a00034	E4	ULR:ChGr(<channel group number>) activated because of 'reset-flush-port'.
	The port was released from the inactive status by the port resetting. <channel group number>: Channel group number [Action] None.	

2.13 IP

This section shows event location IP operation messages.

Table 2-26: Operation message for the event location IP

Message ID	Event level	Message text
	Contents and actions	
2600000d	E4	The IP configuration to VLAN (<vlan id>) can't be registered at hardware tables.
	An IP configuration for a VLAN (<vlan id>) cannot be registered in the hardware tables. <vlan id>: ID of the VLAN for which an IP configuration was set [Action] 1. Change the VLAN ID. 2. Review the capacity limit. However, depending on specifications of the cache applied to the hardware, the setting to the maximum of the capacity limit might not be available.	