AX3660S Software Manual

Message Log Reference

For Version 12.1 Rev.11

AX38S-S017X-C0

Alaxala

■ Relevant products

This manual applies to the models in the AX3660S series of switches. It also describes the function of OS-L3M version 12.1 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

December 2023 (Edition 1) AX38S-S017X-C0

■ Copyright

Preface

■ Applicable products and software versions

This manual applies to the models in the AX3660S series of switches. It also describes the function of OS-L3M version 12.1 of the software. The described function is that supported by the software licenses and by optional licenses.

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

Unless otherwise noted, this manual describes the functions common to both the SL-L3A and SL-L3L software licenses. Functions that are not common are indicated as follows.

[SL-L3A]:

The description applies to the SL-L3A software license.

■ Corrections to the manual

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

■ Intended readers

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

Readers must have an understanding of the following:

- The basics of network system management

■ Manual URL

You can view this manual on our website at:

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 a switch.

● **To learn how to unpack the switch and the basic settings for initial installation**

Quick Start Guide
(AX36S-Q002X)

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

Hardware Instruction Manual
(AX36S-H002X)

Transceiver
Hardware Instruction Manual
(AX-COM-H001X)

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

Configuration Guide
Vol.1
(AX38S-S010X)
Vol.2
(AX38S-S011X)
Vol.3
(AX38S-S012X)

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

Configuration
Command Reference
Vol.1
(AX38S-S013X)
Vol.2
(AX38S-S014X)

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

Operation Command
Reference
Vol.1
(AX38S-S015X)
Vol.2
(AX38S-S016X)

● **To check messages and logs**

Message Log Reference
(AX38S-S017X)

● **To learn how to troubleshoot a problem**

Troubleshooting Guide
(AX36S-T002X)

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

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

- AX3660S series switch

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

■ Abbreviations used in the manual

AC	Alternating Current
ACK	ACKnowledge

ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second (can also appear as bps)
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DNSSL	Domain Name System Search List
DR	Designated Router
DSA	Digital Signature Algorithm
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DSS	Digital Signature Standard
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
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
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
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
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force

IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MLD	Multicast Listener Discovery
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	packets per second (can also appear as pps)
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PGP	Pretty Good Privacy
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PMTU	Path Maximum Transmission Unit
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
PTP	Precision Time Protocol

QoS	Quality of Service
QSFP+	Quad Small Form factor Pluggable Plus
QSFP28	28Gbps Quad Small Form factor Pluggable
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
RDNSS	Recursive Domain Name System Server
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSA	Rivest, Shamir, Adleman
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SFP+	enhanced Small Form-factor Pluggable
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
Sync-E	Synchronous Ethernet
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
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
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VLAN	Virtual LAN
VNI	VXLAN Network Identifier
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
VTEP	VXLAN Tunnel End Point
VXLAN	Virtual eXtensible Local Area Network
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WS	Work Station
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

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" section of each command in the manual "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
	Message text format	"3 Message Text Format"

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	
TRO	Tracking object log [SL-L3A]	Message text format
RTM	IPv4 or IPv6 routing information	
MRP	IPv4 multicast routing information	
MR6	IPv6 multicast routing information	
BFD	BFD information	

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
TRO	N	Y	N	Y	N
RTM	Y	Y	N	Y	N
MRP, MR6	N	Y	N	Y	N
BFD	N	Y	N	Y	N

Legend

Y: Supported

N: Not supported

#

When a stack is configured, the operation logs for the backup switch is also acquired in the master switch.

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 the format of operation logs for message types KEY, RSP, SKY, and SRS, see "1.3.2 Format of operation logs".

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 • TRO, RTM, MRP, MR6, BFD	• 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 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.

Item	Operation log	Reference log
	• 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 12,000 entries, overflowing old logs will be deleted.	

#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 login or logout is performed

5.When the device is restarted accompanying ppupdate

6.When the device is restarted by pressing the RESET button

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 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

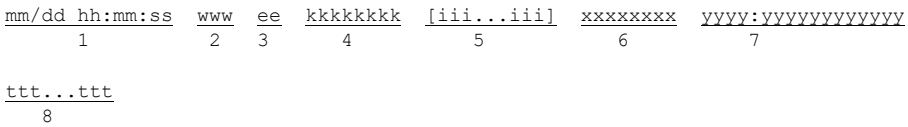
Operation messages of message type ERR or EVT can be sent as private SNMP notifications. This is called a system message trap. You can use the "snmp-server traps" configuration command to specify the importance of the operation message sent as an SNMP notification.

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



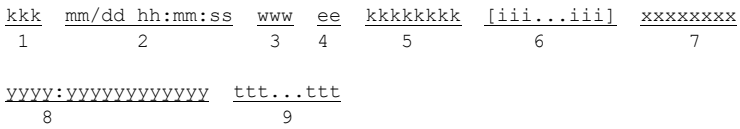
1. Time: Displays the date and time when the event indicated in the message occurred.
2. The switch number (two digits) and the switch status (any of the following characters):
   - I: Indicates the initial status.
   - S: Indicates the standalone status.
   - M: Indicates the master status.
   - B: Indicates the backup status.
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

Note that the switch status indicates the status of each member switch of a stack. For details on switch status, see "Configuration Guide Vol. 1, 7.3.3 Switch status".

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: Date and time that the event occurred.
3. The switch number (two digits) and the switch status (any of the following characters):
   - I: Indicates the initial status.
   - S: Indicates the standalone status.
   - M: Indicates the master status.
   - B: Indicates the backup status.
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

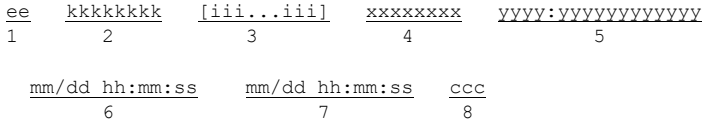
   This information contains a code that indicates the detailed information about the event.

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



1. Event level
2. Event location
3. Event interface ID

   It may not be displayed depending on the event location.

   The switch number that is acquired with the log is set as the switch number. Therefore, for logs acquired before the switch number is changed, the switch number before the change is set.

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 restarting the device or stopping the device operation.

Event level	Displayed information	Description
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 the target hardware.
	R8	Indicates the recover from critical error.
7	E7	Indicates that a software error has occurred.
	R7	Indicates the recover from software error.
6	E6	Not used
	R6	Not used
5	E5	Not used
	R5	Not used
4	E4	Indicates information on network failure detection, line and power.
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
STACK	Stack control function
ACCESS	Switch access permissions

ID	Location or function of the event that occurred
SCRIPT	User-created scripts
PORT	Port control 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
GigabitEthernet <switch no.>/<nif no.>/<port no.>	Ethernet interface with a maximum line speed of 1000 Mbit/s
TenGigabitEthernet <switch no.>/<nif no.>/<port no.>	Ethernet interface with a maximum line speed of 10 Gbit/s
FortyGigabitEthernet <switch no.>/<nif no.>/<port no.>	Ethernet interface with a maximum line speed of 40 Gbit/s
HundredGigabitEthernet <switch no.>/<nif no.>/<port no.>	Ethernet interface with a maximum line speed of 100 Gbit/s
MGMT 0	Management port

Legend

<switch no.>: Indicates the switch number.

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

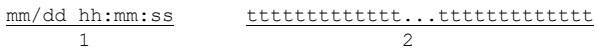
<port no.>: Indicates the port number.

1.3 Message text format

1.3.1 Format for screen output

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

Figure 1-4: Format for screen output



1. Time: Displays the date and time when the event indicated in the message occurred.
2. Message text: Indicates the event that occurred and information related to the event.

To output IPv4 routing protocol and IPv6 routing protocol messages to the operation terminal screen, use the following commands.

- debug protocols unicast

  Start the screen output on the operation terminal.

- no debug protocols unicast

  Stop the screen output on the operation terminal.

1.3.2 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 1-5: Format of operation logs

1. Message type
2. Time: Date and time that the event occurred.
3. Message text

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.	
0000011f	E5	An access error was detected on the internal flash memory.
	An access error to the internal flash memory was detected. [Action] Replace the device as the internal flash memory may be damaged.	
00020102	E7	Hardware exceeded tolerance level of low temperature(<temperature> degree). Check room temperature.
	The hardware temperature went below the permissible temperature range (<temperature> ℃ or lower). <temperature>: -10 [Action] 1. Check and, if necessary, improve the environment such as the room temperature around the devices. 2. Check and, if necessary, replace the fan.	
	R7	The temperature of hardware returned to normal level (<temperature> degree).
	The hardware temperature returned to normal (<temperature> ℃). <temperature>: -7 [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> ℃ or higher). <temperature>50 (with fixed power supply model or FAN -04 equipped) <temperature>40 (when equipped with FAN -04R) [Action] 1. Check and improve the environment such as ventilation and heat sources around the devices. 2. Check and, if necessary, replace the fan.	
	R7	The temperature of hardware returned to normal level (<temperature> degree).
	The hardware temperature returned to normal (<temperature> ℃).	

Message ID	Event level	Message text
	Contents and actions	
	<temperature>47 (with fixed power supply model or FAN -04 equipped) <temperature>37 (when equipped with FAN -04R) [Action] None.	
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 (60°C or higher) (with fixed power supply model or FAN -04 equipped) <temperature>Detected temperature (50°C or higher) (when equipped with FAN -04R) [Action] 1. Check and improve the environment such as ventilation and heat sources around the devices. 2. Check and, if necessary, replace the fan.	
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>: Intake air 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.	
25000110	E8	Switching unit stopped because its hardware failure detected during the self diagnosis.
	A failure was detected during hardware self-diagnosis. [Action] Replace the Switch.	
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]	

Message ID	Event level	Message text
	Contents and actions	
	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 Switch.	
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.	
250a0210	E3	Synchronous Ethernet with internal clock was selected.
	Behavior using the internal clock has started. [Action] None.	

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	
00000001	E4	<ps> is power off.
	The displayed power unit is off. <ps> displays a power supply unit (either PS1 or PS2) that is turned off. <ps>: PS1 or PS2 [Action] 1. Check the power cable connection and the power source, and then connect them properly. 2. Check 1 and if there is no problem, replace the device.	
	R4	<ps> is normal.
	The displayed power unit is operating normally. <ps> displays a power supply unit (either PS1 or PS2) that is in a normal state. This message appears when the following conditions are met: • When the power redundancy-mode redundancy-check configuration is not set, and the power unit state changes from an anomalous state to a normal state, or from non-power-supplied state to a normal state, the power unit in the normal state is displayed. • Appears if the power redundancy-mode redundancy-check configuration is set when the input power is not supplied. <ps>: PS1 or PS2 [Action] None.	
00000002	E8	<ps> is power off.
	For fixed power supply model The displayed power unit is off. <ps> displays a power supply unit (either PS1 or PS2) that is turned off. <ps>: PS1 or PS2 [Action] 1. Check the power cable connection and the power source, and then connect them properly. 2. Check 1 and if there is no problem, replace the device. For replaceable power supply model The displayed power supply unit is turned off. <ps> displays a power supply unit (either PS1 or PS2) that is turned off. <ps>: PS1 or PS2 [Action] 1. Check the power cable connection and the power source, and then connect them properly. 2. If the power supply unit has failed, replace it.	
	R8	<ps> is normal.

Message ID	Event Level	Message text
	Contents and actions	
	For fixed power supply model The displayed power unit is operating normally. <ps> displays a power supply unit (either PS1 or PS2) that is in a normal state. This message appears when the following conditions are met: • When the power redundancy-mode redundancy-check configuration is set, and the power unit state changes from an anomalous state to a normal state, or from non-power-supplied state to a normal state, the power unit in the normal state is displayed. • Appears if the power redundancy-mode redundancy-check configuration is deleted when the input power is not supplied or in the power failure status. <ps>: PS1 or PS2 [Action] None. For replaceable power supply model The displayed power supply unit is in a normal state. <ps> displays a power supply unit (either PS1 or PS2) that is in a normal state. This message appears when the following conditions are met: • When the power supply unit state changes from an anomalous state to a normal state, or from an unequipped state to a normal state, the power supply unit in the normal state is displayed. • When either one of the power supply units in a redundant configuration is removed, the power supply unit in the normal state is displayed. <ps>: PS1 or PS2 [Action] None.	
00000003	E3	Failed in accumulated running time access to <ps>.
	Access to the total operating time for the power supply unit failed. <ps> displays the power supply unit (either PS1 or PS2) for which access to the total operating time failed. <ps>: PS1 or PS2 [Action] This event does not affect communication and usual operation. However, you cannot use the total operating time management function. If you want to use this function, replace the power supply unit.	
00000006	E8	<ps> is unknown.
	The power supply unit is unknown. <ps> displays a power supply unit (either PS1 or PS2) that is unknown. <ps>: PS1 or PS2 [Action] 1. The power supply unit might not be fully inserted. Insert the power supply unit properly. 2. The software of this version does not support the power supply unit. Check the type of the power supply unit and the software version. Either change the power supply unit, or update the software. 3. The Switch does not support the power supply unit. Replace the power supply unit.	
	R8	Unknown <ps> was removed.

Message ID	Event Level	Message text
	Contents and actions	
	An unknown power supply unit was removed. This message appears when an unknown power supply unit is removed after the log "<ps> is unknown." appears. <ps> displays the power unit (either PS1 or PS2) that was removed. <ps>: PS1 or PS2 [Action] None.	
00000007	E8	The direction of the fan of <ps> is mismatch.
	The direction of the fan does not match between the fan unit and the power supply unit. <ps> displays a power supply unit (either PS1 or PS2) that has a different fan direction. <ps>: PS1 or PS2 [Action] Replace the power supply unit or the fan unit to match the airflow between them.	
	R8	The direction of the fan of <ps> is normal.
	The direction of the fan matches between the fan unit and the power supply unit. <ps> displays a power supply unit (either PS1 or PS2) that has a matching fan direction. <ps>: PS1 or PS2 [Action] None.	
00000102	E8	Power unit isn't redundantly mounted.
	The power supply unit is not redundant. [Action] Check the installation status of the power supply unit. If the power supply unit is not redundant, set no power redundancy-mode by the configuration command.	
	R8	Power unit is mounted redundantly or mode changed.
	The power supply unit has become redundant. The operation mode was changed. [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	
00000002	E8	<fan> stopped.
	For fixed power supply model The displayed fan is in a stopped state. <fan> displays a fan in a stopped state. <fan> Any of FAN (1), FAN (2), FAN (3), or FAN (4) [Action] Replace the Switch. For replaceable power supply model The displayed fan is stopped or not installed. <fan> displays a fan that has stopped or is not implemented. <fan> Any of FAN1(1), FAN2(1), FAN3(1), FAN3(2), FAN3(3), or FAN3(4) [Action] 1. Check the installation status of the power supply unit or fan unit. Check the installation status either visually or by using the "show system" command. 2. If the power supply unit or fan unit has failed, replace it.	
	R8	<fan> is normal.
	The displayed fan is in a normal state. <fan> displays a fan in a normal state. For fixed power supply model <fan> Any of FAN (1), FAN (2), FAN (3), or FAN (4) For replaceable power supply model <fan> Any of FAN1(1), FAN2(1), FAN3(1), FAN3(2), FAN3(3), or FAN3(4) [Action] None.	
00000004	E3	Failed in accumulated running time access to the fan unit.
	Access to the total operating time for the fan unit failed. [Action] This event does not affect communication and usual operation. However, you cannot use the total operating time management function. If you want to use this function, replace the fan unit.	
00000006	E8	<fan> is unknown.
	The fan unit is unknown. <fan> FAN3 [Action] 1. The fan unit might not be fully inserted. Insert the fan unit properly. 2. The Switch does not support the fan unit. Replace the fan unit.	

Message ID	Event Level	Message text
	Contents and actions	
	R8	Unknown <fan> was removed.
	An unknown fan unit was removed. This message is displayed when an unknown fan unit is removed after the log "<fan> is unknown" appears. <fan> FAN3 [Action] None.	
00000007	E3	The direction of the fan changed to <airflow>.
	The fan direction of the fan unit was changed. <airflow> displays the direction of the fan in the replaced fan unit. <airflow>: Fan direction of the fan unit • F-to-R: Intake air at the front and exhaust air at the rear • R-to-F: Intake air at the rear and exhaust air at the front [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	
00003001	E3	System restarted due to abort reset operation.
	The device was restarted because the RESET button was pressed. [Action] None.	
00003002	E3	System restarted due to default reset operation.
	The device was restarted because the default switch was pressed. [Action] None.	
00003003	E3	System restarted due to fatal error detected by software.
	The software detected a fatal error and restarted the system. [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 one of the following causes. • Execute the "reload" command • Detect addition, deletion, or status change of member switches in stack configuration • Detect the SW (Switch processor) failure in stack configuration • Restart the network interface management program [Action] Check the log using the "show logging" command to determine the cause of the device restart. The logs for each restart cause are shown below. If the target logs exist, take an action appropriate for each log. • Detect addition, deletion, or status change of member switches in stack configuration Event location = restart log in STACK • Detect the SW failure in stack configuration E8 EQUIPMENT 25040201 2101 Hardware restarted because of its failure. • Restart the network interface management program E7 SOFTWARE 25300000 1001 nimd aborted. R7 SOFTWARE 25300000 1001 nimd restarted.	

Message ID	Event Level	Message text
	Contents and actions	
00003005	E3	System restarted due to fatal error detected by kernel.
	The kernel detected a fatal error and restarted the system. [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.	
00003006	E3	System restarted due to WDT timeout.
	The device was restarted because of a WDT (watchdog timer) timeout. [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.	
00003007	E3	System restarted due to hardware error detected by kernel.
	The device was restarted because of a hardware failure. [Action] Replace the Switch.	
00003008	E3	System restarted due to hardware error detected.
	The device was restarted because of a hardware failure. [Action] Replace the Switch.	
00003101	E7	Memory exhausted. Possibly too many users logged in, or too many sessions(via ftp,http,...) established.
	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	Recovered from memory exhaustion.
	The CPU has recovered from a lack of memory. [Action] None.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
	1. Check if the device has received a large quantity of packets for the local device (such as for ping or telnet), in a broadcast, or in a multicast. If there is too much access from the network management device, limit the amount of access to the minimum necessary. 2. 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>[on VRF <vrf id>].
	Synchronization was lost with the NTP server at <ip address>. <ip address>: IPv4 address of NTP server <vrf id>: VRF ID [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.	
00008602	E3	NTP detected an invalid packet from <ip address>[on VRF <vrf id>].
	An invalid packet from the NTP server at <ip address> was detected. <ip address>: IPv4 address of NTP server <vrf id>: VRF ID [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	E7	Software failure occurred during operation.
	An error occurred in the software during operation. [Action]	

<table>
<tr><th rowspan="2">Message ID</th><th>Event Level</th><th>Message text</th></tr>
<tr><th colspan="2">Contents and actions</th></tr>
<tr><td>01200001
01200002
01200004
01300001
01300002
01300004
01400001
01400002
01400004
01600001
01600002
01600004
01700001
01700002
01700004
01800001
01800002
01800004
01900001
01900002
01900004
01910001
01910002
01910004</td><td colspan="2">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.</td></tr>
<tr><td rowspan="2">01100003
01200003
01300003
01400003
01600003
01700003
01800003
01900003
01910003</td><td>E9</td><td>System restarted due to software failure occurred during initialization.</td></tr>
<tr><td colspan="2">An error occurred in the software during initialization, and the device 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.</td></tr>
<tr><td rowspan="2">01100005
01200005
01300005
01400005
01600005
01700005
01800005
01900005
01910005</td><td>E9</td><td>System restarted due to software failure occurred during operation.</td></tr>
<tr><td colspan="2">An error occurred in the software during operation, and the device 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.</td></tr>
</table>

Message ID	Event Level	Message text
	Contents and actions	
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).	
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.	
01910203	E3	System restarted after hardware reset.
	The system was restarted by the RESET button.	

Message ID	Event Level	Message text
	Contents and actions	
	[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.

Message ID	Event Level	Message text
	Contents and actions	
	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.	
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 Vol. 1, 13. 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 Vol. 1, 13. 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 Vol. 1, 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.	

Message ID	Event Level	Message text
	Contents and actions	
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".	
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> [on VRF <vrf id>].
	<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 <vrf id>: VRF ID [Action] None.	
02002025	E3	SNMP: MAC address table entry cleared at the request of <ip address> [on VRF <vrf id>].
	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 <vrf id>: VRF ID [Action] None.	

2.4.4 05XXXXXX-09XXXXXX

This section shows operation messages where the first two digits of message ID are 05 to 09.

Table 2-7: Operation message for the event location SOFTWARE (05XXXXXX-)

Message ID	Event Level	Message text
	Contents and actions	
05000001 05000002 05000004 06100001 06100002 06100004 06200001 06200002 06200004 06300001 06300002 06300004 06400001 06400002 06400004 06500001 06500002 06500004 07000001 07000002 07000004 09100001 09100002 09100004 09200001 09200002 09200004 09300001 09300002 09300004 09400001 09400002 09400004 09500001 09500002 09500004 09600001 09600002 09600004 09700001 09800001	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.	
05000003 06100003 06200003 06300003 06400003 06500003 07000003 09100003 09200003 09300003 09400003 09500003 09600003	E9	System restarted due to software failure occurred during initialization.
	An error occurred in the software during initialization, and the device 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.	
05000005 06100005 06200005 06300005 06400005 06500005 07000005 09100005 09200005 09300005 09400005 09500005 09600005 09700005 09800005	E9	System restarted due to software failure occurred during operation.
	An error occurred in the software during operation, and the device 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.	
05001001	E7	Rtm aborted [:<error string>].

<table>
<tr><th rowspan="2">Message ID</th><th>Event Level</th><th>Message text</th></tr>
<tr><th colspan="2">Contents and actions</th></tr>
<tr><td></td><td colspan="2">The unicast routing program (rtm) was forced to stop.
<error string>: Error cause
• Cannot allocate memory: The program was forced to stop because of lack of memory.
• Blank: The program was forced to stop because of other causes.
[Action]
• If the cause of the forced stop is lack of memory:
The reason is that the memory area is full. Check whether the system has exceeded the usage limit (see "Configuration Guide Vol. 1, 3 Capacity Limit". If the usage is within the limit, carry out the action for when the cause of the forced stop is something other than lack of memory.
• If the cause of the forced stop is something other than lack of memory:
(1) Check whether other log messages related to unicast routing protocol (message type: RTM) have been issued. Then, carry out the appropriate actions.
(2) The unicast routing program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.</td></tr>
<tr><td></td><td>R7</td><td>Rtm restarted.</td></tr>
<tr><td></td><td colspan="2">The unicast routing program (rtm) has restarted.
The switch outputs this message when the unicast routing program restarts automatically, or the restart is requested by the "restart unicast" command.
[Action]
None.</td></tr>
<tr><td>05001010</td><td>E3</td><td>The number of maximum multipath set by the configuration is different from the maximum value when this system starts.</td></tr>
<tr><td></td><td colspan="2">The maximum multi-path count that was set at configuration differs from the maximum value during startup of this Switch.
[Action]
1. Using the "show system" command, check the maximum multi-path count displayed in Current selected unicast multipath number.
2. To change the value of 1 to configure a multi-path, for all protocols that you want to use multi-path with, set and save the maximum multi-path count in the configuration used to restart the device. After restarting the device, you can operate the system with the maximum multi-path count that you set in the configuration.
3. If you do not change the value of 1, return the setting of the maximum multi-path count that you set at the configuration back to the original value.</td></tr>
</table>

2.4.5 0dXXXXXX-0fXXXXXX

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

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

Message ID	Event Level	Message text
	Contents and actions	
0d00b001	E7	dhcpd aborted.
	The DHCP relay program (dhcpd) was forced to stop. The DHCP relay detected an anomaly such as a lack of memory, aborted the running, and forced the program to stop. [Action] The DHCP relay program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	dhcpd restarted.
	The DHCP relay program (dhcpd) has restarted. The switch outputs this message when the DHCP relay program restarts automatically. [Action] None.	
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.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
	<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.	
0e008001	E3	Virtual router <vrid> of <interface name> state has transitioned to <state>.
	The virtual router active status transitioned to <state>. <vrid>: Virtual router ID <interface name>: Name of interface on which VRRP is configured <state>: Virtual router status [Action] None.	
0e008002	E3	Virtual router <vrid> of <interface name> received VRRP packet with IP TTL not equal to 255.
	The virtual router received a VRRP ADVERTISEMENT packet whose TTL (Time-to-Live) in the IP header was not 255. <vrid>: Virtual router ID <interface name>: Name of interface on which VRRP is configured [Action] Check the remote device that makes up the same virtual router.	

Message ID	Event Level	Message text
	Contents and actions	
0e008003	E3	Virtual router <vrid> of <interface name> received VRRP packet that length less than the length of the VRRP header.
	The virtual router received a VRRP ADVERTISEMENT packet that had an invalid length. <vrid>: Virtual router ID <interface name>: Name of interface on which VRRP is configured [Action] Check the remote device that makes up the same virtual router.	
0e008004	E3	Virtual router <vrid> of <interface name> received VRRP packet that does not pass the authentication check.
	Authentication of a received VRRP ADVERTISEMENT packet failed. <vrid>: Virtual router ID <interface name>: Name of interface on which VRRP is configured [Action] Check the password settings for the Switch and the remote device that makes up the same virtual router.	
0e008005	E3	Virtual router <vrid> of <interface name> received VRRP packet for which the address list does not match the locally configured list for the virtual router.
	The IP address of a virtual router specified in a received VRRP ADVERTISEMENT packet does not match the settings of the Switch. <vrid>: Virtual router ID <interface name>: Name of interface on which VRRP is configured [Action] Check the IP address settings of virtual routers for the Switch and for the remote device that makes up the same virtual router.	
0e008006	E3	Virtual router <vrid> of <interface name> received VRRP packet for which the advertisement interval is different than the one configured for local virtual router.
	The sending interval specified in a received VRRP ADVERTISEMENT packet does not match the settings of the Switch. <vrid>: Virtual router ID <interface name>: Name of interface on which VRRP is configured [Action] Check the sending intervals for the Switch and the remote device that makes up the same virtual router.	
0e008007	E3	VRRP packet received with unsupported version number.
	The VRRP version specified in a received VRRP ADVERTISEMENT packet does not match the VRRP version of the Switch. [Action] When constructing the Switch with a virtual router, set the VRRP version of the remote device to 2 for IPv4, and 3 for IPv6, respectively.	

Message ID	Event Level	Message text
	Contents and actions	
0e008008	E3	Virtual router <vrid> of <interface name> priority was changed to <priority>.
	The VRRP priority was changed to <priority>. <vrid>: Virtual router ID <interface name>: Name of interface on which VRRP is configured <priority>: Virtual router priority [Action] None.	
0e008012	E3	Virtual router <vrid> of <interface name> was finished.
	The virtual router ended. <vrid>: Virtual router ID <interface name>: Name of interface on which VRRP is configured [Action] None.	
0e008014	E7	vrrpd aborted.
	The VRRP program (vrrpd) was forced to stop. [Action] The VRRP program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	vrrpd restarted.
	The VRRP program (vrrpd) has restarted. The switch outputs this message when the VRRP program restarts automatically. [Action] None.	
0e008015	E3	Virtual router <vrid> of <interface name> received VRRP packet with IP HopLimit not equal to 255.
	The virtual router received a VRRP ADVERTISEMENT packet whose HopLimit in the IP header was not 255. <vrid>: Virtual router ID <interface name>: Name of interface on which VRRP is configured [Action] Check the remote device that makes up the same virtual router.	
0e008016	E3	Virtual router <vrid> of <interface name> priority changed to <priority>, because error detected on line by vrrp-polling.
	VRRP polling detected a line failure, and the VRRP priority was changed to <priority>. <vrid>: Virtual router ID <interface name>: Name of interface on which VRRP is configured <priority>: Virtual router priority [Action] If switching occurs frequently, adjusting the configuration might solve the problem.	

Message ID	Event Level	Message text
	Contents and actions	
0e008017	E3	<interface name> assigned virtual router <vrid> is down because of error detected by track.
	The interface in which VRRP is set is down because the tracking function detected a failure. <interface name>: Name of interface on which VRRP is configured <vrid>: Virtual router ID [Action] If switching occurs frequently, adjusting the configuration might solve the problem.	
0e008018	E3	<interface name> assigned virtual router <vrid> is up because of recovery detected by track.
	The interface in which VRRP is set was brought up because the tracking function detected recovery from a failure. <interface name>: Name of interface on which VRRP is configured <vrid>: Virtual router ID [Action] None.	
0e008019	E3	Critical interface of <interface name> is down.
	A fault monitoring interface is down. <interface name>: Interface name of a failure-monitoring target [Action] None.	
0e008020	E3	Critical interface of <interface name> is up.
	A fault monitoring interface is up. <interface name>: Interface name of a failure-monitoring target [Action] None.	
0e008021	E4	The VRRP virtual MAC address entry can't be registered at hardware tables.
	The virtual MAC address of VRRP could not be set for the hardware. [Action] Change the virtual router ID to a different value. Change the VLAN ID of the VLAN for setting the virtual router to a different value.	
0e008022	E3	Virtual router <vrid> of <interface name> advertisement interval set default advertisement interval (1 second) because not supported Advertisement interval configured.
	An unsupported value is set for the advertisement packet sending interval. The advertisement interval runs with the default value. <vrid>: Virtual router ID <interface name>: Name of interface on which VRRP is configured [Action] If the VRRP behavior mode (ietf-ipv6-spec-07-mode) configuration is set, set it to a value of 40 seconds or less.	

Message ID	Event Level	Message text
	Contents and actions	
0e008023	E3	Virtual router <vrid> of <interface name> disabled because Primary virtual router is not running.
	The follower virtual router is invalid because the primary virtual router is not set. <vrid>: Virtual router ID <interface name>: Interface name [Action] Configure the primary virtual router.	
0e008024	E3	Virtual router <vrid> of <interface name> enabled because Primary virtual router started.
	The follower virtual router is now enabled because the primary virtual router has been set. <vrid>: Virtual router ID <interface name>: Interface name [Action] None.	
0e008025	E3	Critical interface of <interface type> <interface number> is down.
	A fault monitoring interface is down. <interface type><interface number>: Interface that is specified as the fault monitoring interface • Ethernet interface • Port channel interface [Action] None.	
0e008026	E3	Critical interface of <interface type> <interface number> is up.
	A fault monitoring interface is up. <interface type><interface number>: Interface that is specified as the fault monitoring interface • Ethernet interface • Port channel interface [Action] None.	
0e008027	E3	Critical interface of <interface number> is up. But priority not changed because of different interface type.
	A fault monitoring interface is up at mixed speeds. The priority did not change. <interface number>: Interface number specified for the fault monitoring interface • <nif no.>/<port no.>: NIF number/port number [Action] None.	

Message ID	Event Level	Message text
	Contents and actions	
0f306003 0f406003	E3	The multicast routing program will restart, because the multicast (PIM) max-interfaces configuration changed.
	IP multicast routing program will restart because the IP multicast (PIM) information of the running configuration was changed by the "ip pim max-interface" configuration command. [Action] None.	
0f406001	E7	mrp aborted.
	The IP multicast routing program was forced to stop. [Action] 1. Check whether other log messages related to the IP multicast routing program (message type: MRP) were issued. Then, carry out the appropriate actions. 2. The IP multicast routing program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	mrp restarted.
	The IP multicast routing program has restarted. The switch outputs this message when the IP multicast routing program restarts automatically or a restart is requested by the "restart ipv4-multicast" command. [Action] None.	
0f406004	E3	IPv4 multicast routing entry had exceeded maximum value <number> for limit, entry has discarded[on VRF <vrf id>].
	An entry was discarded because the items of IPv4 multicast route information exceed the limit maximum value of <number>. <number>: Maximum number of items of IPv4 multicast route information <vrf id>: VRF ID [Action] An unauthorized access might have occurred. • Check if more than the expected number of additional requests for multicast route information were generated. The number of items of multicast route information exceeds the limit maximum value. • Check the configuration ("ip pim mroute-limit" command). • Check the network configuration and reconsider the configuration of the Switch.	
0f406005	E3	IPv4 multicast routing entry has recovered from the state of discard[on VRF <vrf id>].
	IPv4 multicast route information has recovered from the state in which entries were discarded. <vrf id>: VRF ID [Action] None.	
0f406006	E3	IGMP source-limit <number> has been exceeded on interface <interface name> [of VRF <vrf id>] due to over-request. Request have been discarded.

Message ID	Event Level	Message text
	Contents and actions	
	The interface <interface name> received a request that exceeded the IGMP source limit value of <number>. A request was discarded. <number>: IGMP group limit value <interface name>: Interface name <vrf id>: VRF ID [Action] An unauthorized access might have occurred. • Check if more than the expected number of additional requests were generated for sources belonging to the IGMP group. • Check the configuration ("ip igmp source-limit" command). • Check the network configuration and reconsider the configuration of the Switch.	
0f406007	E3	IGMP source-limit on requests on interface <interface name> [of VRF <vrf id>] has recovered from state of discard.
	The interface <interface name> has recovered from state in which sources belonging to IGMP group were discarded. <interface name>: Interface name <vrf id>: VRF ID [Action] None.	
0f406008	E3	IGMP group-limit <number> has been exceeded on interface <interface name> [of VRF <vrf id>] due to over-request. Request have been discarded.
	The interface <interface name> received a request that exceeded the IGMP group limit value of <number>. A request was discarded. <number>: IGMP group limit value <interface name>: Interface name <vrf id>: VRF ID [Action] An unauthorized access might have occurred. • Check if more than the expected number of additional requests for the IGMP group were generated. • Check the configuration ("ip igmp group-limit" command). • Check the network configuration and reconsider the configuration of the Switch.	
0f406009	E3	IGMP group-limit on requests on interface <interface name> [of VRF <vrf id>] has recovered from state of discard.
	The interface <interface name> has recovered from the state in which IGMP groups were discarded. <interface name>: Interface name <vrf id>: VRF ID [Action] None.	
0f40600a	E3	IPv4 multicast forwarding entry had exceeded maximum value <number> for limit, entry has discarded[on VRF <vrf id>].

Message ID	Event Level	Message text
	Contents and actions	
	An entry was discarded because the IPv4 multicast forwarding entry items exceeded the maximum value, <number>. <number>: Maximum number of IPv4 multicast forwarding entry items <vrf id>: VRF ID [Action] An unauthorized access might have occurred. • Check if more than the expected number of additional requests for multicast forwarding entries were generated. The number of multicast forwarding entry items exceeds the maximum value. • Check if a negative cache is generated, due to reception of multicast packets that were not forwarded. • Check the configuration ("ip pim mcache-limit" command). • Check the network configuration and reconsider the configuration of the Switch.	
0f40600b	E3	IPv4 multicast forwarding entry has recovered from the state of discard[on VRF <vrf id>].
	IPv4 multicast forwarding entries have recovered from the discard state. <vrf id>: VRF ID [Action] None.	

2.4.6 11XXXXXX-1fXXXXXX

This section shows operation messages where the first two digits of message ID are 11 to 1f.

Table 2-9: Operation message for the event location SOFTWARE (11XXXXXX-)

Message ID	Event Level	Message text
	Contents and actions	
11010001	E3	The list number <policy list no.> of the policy base routing changed to the sequence number <sequence>.
	The route with priority <sequence> was selected in the list number <policy list no.> of the policy-based routing. <policy list no.>: The list number of the policy-based routing <sequence>: Priority of route information in the list [Action] None.	
11010002	E3	The list number <policy list no.> of the policy base routing changed to the default operation.
	The default was selected in the list number <policy list no.> of the policy-based routing. <policy list no.>: The list number of the policy-based routing [Action] None.	

Message ID	Event Level	Message text
	Contents and actions	
11109901	E7	policyd aborted.
	The policy-based program (policyd) was forced to stop. [Action] Collect the error save information (policyd.core file under /usr/var/core), log information, and the configuration of the policy-based program. For details about how to collect the information, see the "Troubleshooting Guide". The policy-based program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	policyd restarted.
	The policy-based program (policyd) has restarted. The switch outputs this message when the policy-based program restarts automatically or a restart is requested by the "restart policy" command. [Action] None.	
1920a002	E7	mr6 aborted.
	IPv6 multicast routing program was forced to stop. [Action] 1. Check whether other log messages related to the IPv6 multicast routing program (message type: MR6) were issued. Then, carry out the appropriate actions. 2. The IPv6 multicast routing program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	mr6 restarted.
	The IPv6 multicast routing program has restarted. The switch outputs this message when the IPv6 multicast routing program restarts automatically or a restart is requested by the "restart ipv6-multicast" command. [Action] None.	
1920a003	E3	The multicast routing program will restart, because the multicast (PIM6) max-interfaces configuration changed.
	The IPv6 multicast routing program will restart because the IPv6 multicast (PIM6) information of the running configuration was changed by the "ipv6 pim max-interface" configuration command. [Action] None.	
1920a005	E3	IPv6 multicast routing entry had exceeded maximum value <number> for limit, entry has discarded[on VRF <vrf id>].
	An entry was discarded because the items of IPv6 multicast route information exceed the limit maximum value of <number>.	

Message ID	Event Level	Message text
	Contents and actions	
	<number>: Maximum number of items of IPv6 multicast route information <vrf id>: VRF ID [Action] An unauthorized access might have occurred. • Check if more than the expected number of additional requests for multicast route information were generated. The number of items of multicast route information exceeds the limit maximum value. • Check the configuration ("ipv6 pim mroute-limit" command). • Check the network configuration and reconsider the configuration of the Switch.	
1920a006	E3	IPv6 multicast routing entry has recovered from the state of discard[on VRF <vrf id>].
	IPv6 multicast route information has recovered from the state in which entries were discarded. <vrf id>: VRF ID [Action] None.	
1920a007	E3	IPv6 multicast forwarding entry had exceeded maximum value <number> for limit, entry has discarded[on VRF <vrf id>].
	An entry was discarded because the IPv6 multicast forwarding entry items exceeded the maximum value, <number>. <number>: Maximum number of IPv6 multicast forwarding entry items <vrf id>: VRF ID [Action] An unauthorized access might have occurred. • Check if more than the expected number of additional requests for multicast forwarding entries were generated. The number of multicast forwarding entry items exceeds the maximum value. • Check if a negative cache is generated, due to reception of multicast packets that were not forwarded. • Check the configuration ("ipv6 pim mcache-limit" command). • Check the network configuration and reconsider the configuration of the Switch.	
1920a008	E3	IPv6 multicast forwarding entry has recovered from the state of discard[on VRF <vrf id>].
	IPv6 multicast forwarding entries have recovered from the discard state. <vrf id>: VRF ID [Action] None.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
	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.	
1f00b011	E7	dhcp6_server aborted.
	The IPv6 DHCP server program (dhcp6_server) was forced to stop. The IPv6 DHCP server detected an anomaly such as a lack of memory, aborted the running, and forced the program to stop. [Action] The IPv6 DHCP server program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	dhcp6_server restarted.
	The IPv6 DHCP server program (dhcp6_server) has restarted. The switch outputs this message when the IPv6 DHCP server program restarts automatically or a restart is requested by the "restart ipv6-dhcp server" command. [Action] None.	
1f01b021	E7	dhcp6_relay aborted.
	The IPv6 DHCP relay program (dhcp6_relay) was forced to stop. The IPv6 DHCP relay detected an anomaly such as a lack of memory, aborted the running, and forced the program to stop. [Action] The IPv6 DHCP relay program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	dhcp6_relay restarted.
	The IPv6 DHCP relay program (dhcp6_relay) has restarted. The switch outputs this message when the IPv6 DHCP relay program restarts automatically or a restart is requested by the "restart ipv6-dhcp relay" command. [Action] None.	
1f01b024	E3	IPv6 DHCP packet discarded by relay agent, because prefix entry exceeded the maximum.
	The relay agent discarded IPv6 DHCP packets because the number of prefix entries exceeded the maximum number. After output of this message, output of the same message is suppressed for the next five minutes. [Action] 1. Use the "show ipv6 dhcp relay binding" command to check the capacity client count.	

Message ID	Event Level	Message text
	Contents and actions	
	2. If the capacity client count for the Switch exceeds the capacity limit, reexamine and then change the capacity client count. If you want to check the number of IPv6 DHCP packets that have actually been discarded, execute the "show ipv6 dhcp traffic" command to display the IPv6 DHCP relay statistics and check the items in lease prefix over.	

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 switch outputs this message when the Spanning Tree program restarts automatically or a restart is requested by the "restart spanning-tree" command. [Action] None.	
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]	

Message ID	Event Level	Message text
	Contents and actions	
	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.	
20150001	E7	oadpd aborted.
	The OADP program (oadpd) was forced to stop. [Action] The OADP program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	oadpd restarted.
	The OADP program (oadpd) has restarted. The switch outputs this message when the OADP program restarts automatically or a restart is requested by the "restart oadp" command. [Action] None.	
20160001	E7	L2MacManager aborted.

Message ID	Event Level	Message text
	Contents and actions	
	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 switch outputs this message when the L2MAC manager program restarts automatically or a restart is requested by the "restart vlan" 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 (standalone): axrpd_rapid.core File (stack): 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.	
	R7	dot1xd restarted.
	The IEEE 802.1X program (dot1xd) has restarted.	

Message ID	Event Level	Message text
	Contents and actions	
	The switch outputs this message when the IEEE 802.1X program restarts automatically or a restart 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.	
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).	

Message ID	Event Level	Message text
	Contents and actions	
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 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.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
	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.	
25090003	E3	System changes to the schedule power control because it became schedule time.
	The time for the power-control schedule has started, and the scheduled power control is enabled. [Action] None.	
25090004	E3	System changes from the schedule power control because it ended schedule time.
	The time for the power-control schedule has ended, and the scheduled power control is disabled. [Action] None.	

Message ID	Event Level	Message text
	Contents and actions	
25090005	E3	The schedule power control is enable because it is schedule time.
	The device is in the scheduled time range, and the scheduled power control is enabled. [Action] None.	
25090006	E3	The schedule power control is disable because it is not schedule time.
	The device is in the normal time range, and the scheduled power control is disabled. [Action] None.	
25090007	E3	The schedule power control is disable because system started by reset switch on schedule time.
	Even though the system is within the scheduled time range, the system has been started by using the RESET button, and the scheduled power control is disabled. [Action] None.	
25090008	E3	The schedule power control continues disable because set power-control-schedule disable executed.
	The scheduled time for power control has been reached. The scheduled power control mode is still disabled because the schedule-disabled mode was set by using the "set power-control-schedule" command. [Action] None.	
25090009	E3	System changes to the schedule power control by set power-control-schedule command.
	The scheduled power control has been started by using the "set power-control-schedule" command. [Action] None.	
2509000a	E3	System changes from the schedule power control by set power-control-schedule command.
	The scheduled power control has been stopped by using the "set power-control-schedule" command. [Action] None.	
2509000b	E3	The schedule power control is disable because set power-control-schedule disable executed.
	The scheduled time has been reached. The scheduled power control is disabled because the schedule-disabled mode was set by using the "set power-control-schedule" command. [Action] None.	
25300000	E7	nimd aborted.

Message ID	Event Level	Message text
	Contents and actions	
	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 switch outputs this message when the network interface manager program restarts automatically or a restart is requested by the "restart vlan" command. [Action] None.	
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. 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	

Message ID	Event Level	Message text
	Contents and actions	
	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 switch outputs this message when the HTTP program restarts automatically or restarts of HTTP program and NETCONF program are requested by the "restart netconf" command. [Action] None.	

2.4.8 30XXXXXX-3eXXXXXX

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

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.	

Message ID	Event Level	Message text
	Contents and actions	
	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.	
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.)	

Message ID	Event Level	Message text
	Contents and actions	
	[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>/<nif no.>/<port no.>).
	The terminal filter setting failed. <mac address>/<vlan id>/<ip address>/<nif no.>/<port no.>: Terminal filter setting information • <mac address>: MAC address • <vlan id>: VLAN ID • <ip address>: IP address • <nif no.>: NIF number • <port no.>: Port number [Action] The capacity limit of the device was exceeded. Review the system configuration.	
32001001	E7	trackobjd aborted.
	The track object program (trackobjd) was forced to stop. [Action] The track object program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	trackobjd restarted.
	The track object program (trackobjd) has restarted. The switch outputs this message when the track object program restarts automatically or a restart is requested by the "restart track-object" command. [Action] None.	
34000010	E9	Switch <switch no.> restarted because stackd aborted.
	The switch was restarted because the stack management program (stackd) was forcibly ended. <switch no.>: Switch number Note, however, that 0 is displayed if the switch number cannot be acquired. [Action] If this message is repeatedly output, replace the device.	

Message ID	Event Level	Message text
	Contents and actions	
36000001	E7	The BFD program (bfdd) aborted.
	The BFD program (bfdd) was forced to stop. [Action] The BFD program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	The BFD program (bfdd) restarted.
	The BFD program (bfdd) has restarted. The switch outputs this message when the BFD program restarts automatically or a restart is requested by the "restart bfd" command. [Action] None.	
3a000001	E7	overlayd aborted.
	The overlay VXLAN program (vxland) was forced to stop. It detected an anomaly such as a lack of memory, aborted the running, and forced the program to stop. [Action] The overlay program will restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	overlayd restarted.
	The overlay VXLAN program (vxland) has restarted. The switch outputs this message when the overlay program restarts automatically or a restart is requested by the "restart overlay" command. [Action] None.	
3a000003	E4	The VXLAN tunnel entry can't be registered at hardware tables.
	The VXLAN tunnel entry information for the VXLAN function cannot be registered in the hardware tables. [Action] Review the capacity limit. However, depending on the hardware specification, the setting to the maximum of the capacity limit might not be available.	
3a000012	E4	The VXLAN Layer2 Nexthop entry can't be registered at hardware tables.
	The Nexthop entry information for a VXLAN Network port configured with link aggregation cannot be registered in the hardware tables. [Action] Review the configuration so that it falls within the capacity limit.	
3b000001	E7	ptpd aborted.
	The PTP program (ptpd) was forced to stop. [Action]	

Message ID	Event Level	Message text
	Contents and actions	
	The PTP program should restart automatically. If it does not restart or if restarts occur frequently, restart the device.	
	R7	ptpd restarted.
	The PTP program (ptpd) has restarted. The switch outputs this message when the PTP program restarts automatically. [Action] None.	
3c000001	E4	The flow rate-alarm state changed from conform to exceed. (interface = <interface name>, QoS flow list = <qos flow list name>, sequence = <sequence>)
	The bandwidth status of the QoS flow entry changed from the bandwidth compliance status to bandwidth non-compliance status. <interface name>: Interface name <qos flow list name>: QoS flow list name <sequence> sequence number [Action] None.	
3c000002	E4	The flow rate-alarm state changed from exceed to conform. (interface = <interface name>, QoS flow list = <qos flow list name>, sequence = <sequence>)
	The bandwidth status of the QoS flow entry changed from the bandwidth non-compliance status to the bandwidth compliance status. <interface name>: Interface name <qos flow list name>: QoS flow list name <sequence> sequence number [Action] None.	
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>)

<table>
<tr><th rowspan="2">Message ID</th><th>Event Level</th><th>Message text</th></tr>
<tr><th colspan="2">Contents and actions</th></tr>
<tr><td></td><td colspan="2">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.</td></tr>
<tr><td>3e010004</td><td>E3</td><td>One or more event reports were discarded by the script functionality. (name = <name>, PID = <pid>)</td></tr>
<tr><td></td><td colspan="2">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.</td></tr>
<tr><td>3e020001</td><td>E7</td><td>The script management program(scriptManagerd) aborted.</td></tr>
<tr><td></td><td colspan="2">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.</td></tr>
<tr><td></td><td>R7</td><td>The script management program(scriptManagerd) restarted.</td></tr>
<tr><td></td><td colspan="2">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.</td></tr>
</table>

Message ID	Event Level	Message text
	Contents and actions	
	[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.	
3e020007	E3	The script files of the master switch do not match those of other switches.
	The script files do not match between the master switch and other member switches. [Action] Synchronize the script files by the "install script sync" command.	
3e020008	E3	The script file could not be synchronized. (file name = <file name>)
	Script files could not be synchronized between the master switch and other member switches. <file name> script file name [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. If there are no problems, synchronize the script files by the "install script sync" command.	
3e020009	E3	The applet action script could not be started. (applet name = <applet name>, sequence = <sequence>)

Message ID	Event Level	Message text
	Contents and actions	
	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.	

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	
09200006	E3	There is mismatch between master switch and switch <switch no.> configuration.
	The configuration of the master switch differs from that of other member switches. <switch no.>: Switch number [Action] Restart the member switch <switch no.> to match the configurations of the member and master switches.	
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.	
09300007	E3	Configuration edit status forcedly finished.
	The configuration status was forced to switch from editable status to editing-completed status. [Action] Have all users in the configuration command mode exit from the configuration command mode, and then restart the editing.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
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 STACK

This section shows event location STACK operation messages.

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

Message ID	Event Level	Message text
	Contents and actions	
34000001	E3	Switch <switch no.> changed to <role> switch and initializing.
	The member switch changed its status to <role> and started initialization. <switch no.>: Switch number <role>: Switch status • master: Master • backup: Backup [Action] None.	
34000002	E3	Switch <switch no.> changed to <role> switch and started switchover.
	The member switch changed its status to <role> and started switchover. <switch no.>: Switch number <role>: Switch status • master: Master [Action] None.	
34000003	E3	Master switch detected switch <switch no.> and adding to stack.
	The master switch added the member switch <switch no.> to STACK. <switch no.>: Switch number [Action] None.	
34000004	E3	Switch <switch no.> was deleted from stack.
	The member switch was deleted from the stack configuration. <switch no.>: Switch number [Action] Check the status of the member switch and the status of the stack port used to connect the member switch.	
34000005	E3	Stack port(<switch no.>/<nif no.>/<port no.>) connected with switch <switch no.> of Machine ID <mac address>.
	The stack port was connected with a member switch that has the chassis MAC address <mac address>. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <switch no.>: Switch number <mac address>: Chassis MAC address [Action] None.	

Message ID	Event Level	Message text
	Contents and actions	
34000006	E3	Stack port(<switch no.>/<nif no.>/<port no.>) disconnected with switch <switch no.> of Machine ID <mac address>.
	The stack port was disconnected from a member switch that has the chassis MAC address <mac address>. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <switch no.>: Switch number <mac address>: Chassis MAC address [Action] Check the status of both the stack port and the disconnected member switch.	
34000007	E3	Switch <switch no.> connected to stack port(<switch no.>/<nif no.>/<port no.>) cannot join in stack for <reason>.
	A member switch connected to the stack port cannot participate in the stack configuration. <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number <switch no.>: Switch number <reason>: Reason why the member switch cannot participate in the stack configuration • equal switch number: The switch number of this member switch matches the switch number of another member switch connected to the stack port. • unequal license: The software license or optional license of this member switch and other member switches connected to the stack port do not match. • over switch maximum number: The number of other member switches connected to the same stack port as this member switch exceeds the maximum number. [Action] 1. If equal switch number, change the switch number of the other member switch connected to the stack port. 2. If unequal license, match the license of this member switch to the licenses of the other member switches connected to the stack port. 3. If over switch maximum number, isolate other member switches connected to the stack port.	
34000008	E3	Master switch ordered switch <switch no.> to restart because master switch detected stack error.
	The master switch instructed this member switch to restart because the master switch detected an error. <switch no.>: Switch number [Action] If this message is repeatedly output, replace the member switch that has the displayed switch number.	
34000009	E3	Switch <switch no.> restarted because this switch was disconnected from other switch in stack building.
	The member switch was restarted because it was isolated from the other member switches during the stack building process. <switch no.>: Switch number [Action] Check the status of all stack ports between the member switch and the other member switches.	

Message ID	Event Level	Message text
	Contents and actions	
3400000a	E3	Switch <switch no.> restarted because this switch synchronized configuration of master switch.
	The member switch was restarted because it synchronized with the configuration of the master switch. <switch no.>: Switch number [Action] None.	
3400000b	E3	Switch <switch no.> restarted because hardware has stopped.
	The member switch was restarted because the hardware stopped. <switch no.>: Switch number [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.	
3400000c	E3	Switch <switch no.> restarted because this switch detected other master switch.
	The member switch <switch no.> was restarted because another master switch was detected. <switch no.>: Switch number [Action] None.	
3400000d	E9	Switch <switch no.> restarted due to restart order from master switch.
	The member switch was restarted as instructed by the master switch. <switch no.>: Switch number [Action] If this message is repeatedly output, replace the member switch.	
3400000e	E9	Switch <switch no.> restarted due to stack error.
	The member switch was restarted because an error occurred in the stack. <switch no.>: Switch number [Action] If this message is repeatedly output, replace the member switch.	
3400000f	E9	Switch <switch no.> restarted because this switch failed synchronization of configuration of master switch.
	The member switch was restarted because it failed to synchronize with the configuration of the master switch. <switch no.>: Switch number [Action] 1. Check if the software version, the software license, and the optional license of the master switch match those of the member switches. 2. Check the master switch configuration settings related to the relevant member switches.	

Message ID	Event Level	Message text
	Contents and actions	
34000011	E3	Switch <switch no.> initialized as <role> switch.
	The initialization of the member switch was completed with its switch status as <role>. <switch no.>: Switch number <role>: Switch status • master: Master • backup: Backup [Action] None.	
34000012	E3	Master switch detected switch <switch no.> initialized.
	The master switch recognized that the initialization of the member switch <switch no.> was completed. <switch no.>: Switch number [Action] None.	
34000013	E3	Switch <switch no.> finished switchover as <role> switch.
	The switchover of the member switch was completed with its switch status as <role>. <switch no.>: Switch number <role>: Switch status • master: Master [Action] None.	
38000001	E3	Switch <switch no.> failed to read the learned MAC Address Table during the synchronization process.
	The member switch failed to read the MAC address table learned during the synchronization process. <switch no.>: Switch number [Action] If this message is repeatedly output, replace the member switch.	

2.7 ACCESS

This section shows event location ACCESS operation messages.

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

Message ID	Event Level	Message text
	Contents and actions	
00000001	E3	Unknown host address <ip address> [on VRF <vrf id>].
	An attempt to connect via telnet, ftp, or SSH from <ip address> was not permitted. <ip address>: IPv4 address or IPv6 address <vrf id>: VRF ID [Action] 1. There might have been an unauthorized access (an access from a remote host other than one permitted by the configuration) to the Switch. Check the remote host whose IPv4 address or IPv6 address is <ip address>. 2. If remote access from <ip address> is permitted, the configuration might be incorrect. Check the configuration. 3. If you want to permit remote access from <ip address>, specify access permissions for the configuration. 4. If remote access from VRF <vrf id> is permitted, the configuration might be incorrect. Check the configuration. 5. If you want to permit remote access from VRF <vrf id>, specify access permissions for the configuration.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
00005002	E3	Login <user name> from <host> [on VRF <vrf id>] (<term>).
	A user logged in. <user name>: User name <host>: Host ID • For a remote operation terminal: IPv4 or IPv6 address • For a console terminal: console <vrf id>: VRF ID <term>: Terminal name • For a remote operation terminal: ttyp0 or higher • For a console terminal: tty00 [Action] None.	
00005003	E3	Logout <user name> from <host> [on VRF <vrf id>] (<term>).
	A user logged out. <user name>: User name <host>: Host ID • For a remote operation terminal: IPv4 or IPv6 address • For a console terminal: console <vrf id>: VRF ID <term>: Terminal name • For a remote operation terminal: ttyp0 or higher • For a console terminal: tty00 [Action] None.	
00010001	E3	SNMP agent program received packet from <ip address>[on VRF <vrf id>] 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>: IPv4 or IPv6 address of the SNMP manager <vrf id>: VRF ID <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 is 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.

Message ID	Event Level	Message text
	Contents and actions	
	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.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
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.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
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.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
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.	
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.	

2.8 SCRIPT

This section shows event location SCRIPT operation messages.

Table 2-15: 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.	

2.9 PORT

This section shows event location PORT operation messages.

Table 2-16: 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 state by using the "no shutdown" or "no schedule-power-control shutdown" configuration commands. [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 state 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, or 10GBASE-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, 40GBASE-R, or 100GBASE-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.	

Message ID	Event Level	Message text
	Contents and actions	
	2. If an optical attenuator is used, check the attenuation value. 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.	
25011107	E3	Jumbo frame configuration is not supported with the port speed.
	The speed of the connected port does not support jumbo frames. For details, see "mtu" command or "system mtu" command in the manual "Configuration Command Reference Vol. 1".	

Message ID	Event Level	Message text
	Contents and actions	
	[Action] None.	
25011500	E4	Transceiver not supported.
	An unsupported transceiver was detected, or a transceiver was detected on an unusable port#. The unsupported transceivers are: • For AX3660S-48XT4QW: QSFP28 transceiver when the line speed of the QSFP28/QSFP+ shared port is not set to communication-enabled with 100 Gbit/s using the "system interface hundredgigabitethernet" configuration command. • AX3660S-24T4X, AX3660S-24T4XW, and AX3660S-48T4XW series switches SFP+ transceiver when 10G uplink is not supported by software license or optional license. [Action] • See the transceiver description in the "Hardware Instruction Manual". Insert a supported transceiver into the corresponding port number. • Check whether the target port number can be used by referring to the description of the device in the "Hardware Instruction Manual".	
25011501	E4	This transceiver is not supported in stackport.
	A transceiver whose type is unsupported was detected in the stack port. [Action] When using the QSFP28/QSFP+ shared port as a stack port, see the "Stack port" in the "Hardware Instruction Manual". Insert a supported transceiver into the corresponding port number.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
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. Unusable ports# cannot be restored.	
250a0200	E3	Synchronous Ethernet by port (priority <priority>) was started.
	Started running using the external clock on the target port. <priority> priority [Action] None.	
250a0201	E4	Synchronous Ethernet by port (priority <priority>) was stopped.
	Running using the external clock on the target port was stopped. <priority> priority [Action] 1. Make sure that the cable is properly connected. 2. Check the status of the device connected to the receiving port for an external clock.	
250a0211	E3	Synchronous Ethernet by port (priority <priority>) was locked.
	Synchronized with the external clock via the target port. <priority> priority [Action] None.	
250a0212	E3	Synchronous Ethernet by port (priority <priority>) was unlocked.
	Synchronization with the external clock has been lost on the target port. <priority> priority [Action] None.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
2510000a	E4	Broadcast storm detected.
	A broadcast storm was detected. [Action] None.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
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.	
25100013	E4	Inactivated because of loop detection.
	A port was deactivated because a loop was detected. [Action] Check the network configuration.	
2510002e	E4	The frequency of MAC address movement exceeded the threshold.
	The frequency of MAC address learning movement exceeded the threshold. [Action] Revise the network configuration.	
2510002f	E4	The frequency of MAC address movement fell below the threshold.
	The frequency of MAC address learning movement has fallen below the threshold. [Action] None.	
25100030	E4	The port was inactivated because the frequency of MAC address movement exceeded the threshold.
	A port was deactivated because the frequency of MAC address learning movement exceeded the threshold. [Action] Revise the network configuration.	
25100031	E4	The inactive port was automatically activated.
	Automatic recovery of MAC address learning movement monitoring releases the port from inactive status. [Action] None.	
25230000	E3	Unable to use traffic-shape rate feature because value exceeding setting range was specified.
	The port bandwidth control is not available because a value outside the valid setting range was specified. [Action] Change the bandwidth to inside the setting range. For the setting range, see the rate parameter description in the "Configuration Command Reference Vol. 1, traffic-shape rate".	

Message ID	Event Level	Message text
	Contents and actions	
25230001	E3	Unable to use traffic-shape rate feature because its setting unit was an unjust value.
	The port bandwidth control is not available because the units of the setting are invalid. [Action] Change the units to specifiable units. For the setting units that can be specified, see the rate parameter description in the "Configuration Command Reference Vol. 1, traffic-shape rate".	
25230003	E3	Unable to use WFQ feature because minimum rate exceeding setting range was specified for queue <queue no.>.
	The scheduling mode that includes WFQ is not available because the minimum guaranteed bandwidth specified in <queue no.> is outside the range of valid settings. <queue no.>: Queue number [Action] Change the minimum guaranteed bandwidth to a value inside the range of valid settings. For the setting range, see the wfq parameter description in the "Configuration Command Reference Vol. 1, qos-queue-list".	
25230004	E3	Unable to use WFQ feature because unit of the minimum rate specified for queue <queue no.> was unjustified.
	The scheduling mode that includes WFQ is not available because the units used in the setting of the minimum guaranteed bandwidths specified in <queue no.> are invalid. <queue no.>: Queue number [Action] Change the units to specifiable units. For the setting units that can be specified, see the wfq parameter description in the "Configuration Command Reference Vol. 1, qos-queue-list".	
25230005	E3	Unable to use WFQ feature because total value of minimum rate exceeding the maximum rate of the port.
	The scheduling mode that includes WFQ is not available because the total value of the minimum guaranteed bandwidths exceeds the maximum send bandwidth. [Action] Using the "qos-queue-list" configuration command, adjust the total value of the minimum guaranteed bandwidths so that the total is within the maximum send bandwidth.	

#

This is a port that can be used with an optional license (expansion of number of ports), and is a port when the target optional license is not set.

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.	

Message ID	Event Level	Message text
	Contents and actions	
20120007	E3	Port(<switch no.>/<nif no.>/<port no.>) detached from Channel Group(<channel group number>) - Different Partner System ID is detected.
	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.	

Message ID	Event Level	Message text
	Contents and actions	
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 <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	

Message ID	Event Level	Message text
	Contents and actions	
	• 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.	
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>).

Message ID	Event Level	Message text
	Contents and actions	
	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.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
20110022	E3	STP : Cleared MAC Address Table entry.
	A MAC Address Table entry was cleared because a topology change BPDU was received. [Action] None.	
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 IEEE 802.1Q 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 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 IEEE 802.1Q 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 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.	

<table>
<tr><th rowspan="2">Message ID</th><th>Event Level</th><th>Message text</th></tr>
<tr><th colspan="2">Contents and actions</th></tr>
<tr><td rowspan="2">20110041</td><td>E4</td><td>STP(<mode>): Port status becomes Blocking - BPDU that priority is high was received on the ROOT GUARD port(ChGr:<channel group number>).</td></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td rowspan="2">20110042</td><td>E3</td><td>STP (<mode>) : Topology change detected - BPDU Timeout detected on the root port(VLID:<link id>).</td></tr>
<tr><td colspan="2">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
<link id>: Virtual link ID
[Action]
Check the line status.</td></tr>
<tr><td rowspan="2">20110043</td><td>E3</td><td>STP (<mode>) : Topology change detected - Topology Change Notification BPDU received on the port(VLID:<link id>).</td></tr>
<tr><td colspan="2">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
• CIST: Multiple Spanning Tree (CIST)
• MST Instance <mst instance id>: Multiple Spanning Tree (MSTI) and MST instance ID
<link id>: Virtual link ID
[Action]
Check the line status.</td></tr>
</table>

Message ID	Event Level	Message text
	Contents and actions	
20110044	E3	STP (<mode>) : Topology change detected - BPDU Timeout detected on the alternate port(VLID:<link id>).
	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 <link id>: Virtual link ID [Action] Check the line status.	
20110045	E3	STP (<mode>) : Topology change detected - BPDU Timeout detected on the backup port(VLID:<link id>).
	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 <link id>: Virtual link ID [Action] Check the line status.	
20110047	E4	STP (<mode>) : Port status becomes Forwarding on the port(VLID:<link id>).
	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 <link id>: Virtual link ID [Action] None.	
20110048	E4	STP (<mode>) : Port status becomes Blocking on the port(VLID:<link id>).
	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	

Message ID	Event Level	Message text
	Contents and actions	
	• CIST: Multiple Spanning Tree (CIST) • MST Instance <mst instance id>: Multiple Spanning Tree (MSTI) and MST instance ID <link id>: Virtual link ID [Action] None.	

2.11.2 2013XXXX (GSRP)

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	
20130002	E3	GSRP <gsrp group id> VLAN group <vlan group id> : state transitioned to Backup.
	The GSRP status transitioned to Backup. The device outputs this message when GSRP initialization is complete, backup-lock in the GSRP configuration is deleted, or the "restart vlan" command is executed in the Master status while the GSRP device has not identified the partner device. <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID [Action] None.	
20130003	E3	GSRP <gsrp group id> VLAN group <vlan group id> : state transitioned to Master, because the number of active ports was more than neighbor's.
	The GSRP status transitioned to Master because the device has more active ports than the neighboring GSRP switch. <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID [Action] None.	
20130004	E3	GSRP <gsrp group id> VLAN group <vlan group id> : state transitioned to Master, because the priority was higher than neighbor's.
	The GSRP status transitioned to Master because the priority of the device is higher than that of the neighboring GSRP switch. <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID [Action] None.	

Message ID	Event Level	Message text
	Contents and actions	
20130005	E3	GSRP <gsrp group id> VLAN group <vlan group id> : state transitioned to Master, because the MAC address was larger than neighbor's.
	The GSRP status transitioned to Master because the MAC address of the device is larger than that of the neighboring GSRP switch. <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID [Action] None.	
20130006	E4	GSRP <gsrp group id> VLAN group <vlan group id> : state transitioned to Master, because "set gsrp master" command was executed.
	The GSRP status transitioned to Master because the "set gsrp master" command was executed. <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID [Action] None.	
20130007	E4	GSRP <gsrp group id> VLAN group <vlan group id> : state transitioned to Master, because the direct link failure was detected.
	The GSRP status transitioned to Master because a direct link failure was detected. The switch outputs this message when the direct-down parameter is set in the "no-neighbor-to-master" GSRP configuration command, and GSRP status transitioned to Master because a direct link down was detected while in the Backup (neighbor unknown) status. <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID [Action] None.	
20130008	E3	GSRP <gsrp group id> VLAN group <vlan group id> : state transitioned from Master to Backup, because the number of active ports was less than neighbor's.
	The GSRP status transitioned from Master to Backup because the device has fewer active ports than the neighboring GSRP switch. <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID [Action] None.	
20130009	E3	GSRP <gsrp group id> VLAN group <vlan group id> : state transitioned from Master to Backup, because the priority was lower than neighbor's.
	The GSRP status transitioned from Master to Backup because the priority of the device is lower than that for the neighboring GSRP switch. <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID [Action] None.	

Message ID	Event Level	Message text
	Contents and actions	
20130010	E3	GSRP <gsrp group id> VLAN group <vlan group id> : state transitioned from Master to Backup, because the MAC address was smaller than neighbor's.
	The GSRP status transitioned from Master to Backup because the MAC address of the device is smaller than that for the neighboring GSRP switch. <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID [Action] None.	
20130011	E4	GSRP <gsrp group id> VLAN group <vlan group id> : state transitioned to Backup(No Neighbor).
	The GSRP status transitioned to Backup (neighbor unknown). <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID [Action] Check that the port for direct link was implemented correctly and is active. Also, check the current GSRP status by using the configuration and the operation command.	
20130012	E4	GSRP <gsrp group id> VLAN group <vlan group id> : state transitioned from Backup(No Neighbor) to Backup.
	The GSRP status transitioned from Backup (neighbor unknown) to Backup. <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID [Action] None.	
20130013	E3	GSRP <gsrp group id> VLAN group <vlan group id> : advertise timeout detected on Master.
	The timeout period for receiving GSRP Advertise frames is detected. The switch outputs this message only when the GSRP status is Master. <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID [Action] Check that the port for direct link was implemented correctly and is active. Also, check the current GSRP status by using the configuration and the operation command.	
20130014	E4	GSRP <gsrp group id> VLAN group <vlan group id> : advertise timeout detected on Backup(Lock).
	The timeout period for receiving GSRP Advertise frames is detected. The switch outputs this message only when the GSRP status is Backup (Lock). <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID [Action] Check that the port for direct link was implemented correctly and is active. Also, check the current GSRP status by using the configuration and the operation command.	

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.	
20130016	E4	GSRP <gsrp group id> VLAN group <vlan group id> : state transitioned from Master to Backup, because the double Master detected.
	The GSRP status of the device and neighboring machine are both Master, so both transitioned to Backup. <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID [Action] Check that the direct link port operates normally. Also, check the current GSRP status by using the configuration and the operation command.	
20130017	E3	GSRP <gsrp group id> VLAN group <vlan group id> VLAN id <vlan id> : removed from vlan-group, because configuration is a disagreement, Ring protocol and GSRP.
	While using the Ring Protocol there was a configuration mismatch between the Ring Protocol and GSRP, so the corresponding VLAN was no longer part of the vlan-group. <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID <vlan id>: VLAN ID [Action] Change the configuration so that the contents of Ring Protocol vlan-mapping and GSRP vlan-group match.	
20130018	E4	GSRP <gsrp group id> VLAN group <vlan group id> : state transitioned to Master, because forced shift time was expired.
	The GSRP status transitioned to Master due to elapsing of the time set for the automatic master transition wait time. <gsrp group id>: GSRP group ID <vlan group id>: VLAN group ID [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.	

Message ID	Event Level	Message text
	Contents and actions	
20130020	E4	GSRP : Virtual MAC address learning frame cannot be sent in the port where capacity was exceeded.
	The number of VLAN ports that can send the frames for virtual MAC address learning exceeded the capacity limit. Control frames cannot be sent from VLAN ports whose capacity limit is exceeded. [Action] Decrease the number of sending ports for frames for virtual MAC address learning. Alternatively, set the sending interval to a longer interval.	

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	
20170001	E3	AXRP <ring id> : activated state monitoring.
	Monitoring of the Ring Protocol state started. The switch outputs this message when Ring Protocol initialization is complete and you set the behavior mode of the Ring Protocol configuration to the master mode. <ring id>: Ring ID [Action] None.	
20170002	E3	AXRP <ring id> : detected fault recovery by receiving health check frames.
	Monitoring of the Ring Protocol state detected a recovery from a failure. The switch outputs this message when it receives a health-check frame at the master node and detects a recovery from a failure. <ring id>: Ring ID [Action] None.	
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.	
20170004	E4	AXRP <ring id> : detected fault by health check timeout.
	Monitoring of the Ring Protocol state detected a failure. The switch outputs this message when it detects a health-check timeout at the master node. <ring id>: Ring ID [Action] A failure may be occurring at the link or the node in a corresponding ring. Check the link and the node states.	

Message ID	Event Level	Message text
	Contents and actions	
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.	
20170016	E3	AXRP <ring id> : detected fault recovery by receiving health check frames, but suspended the fault recovery process.
	Monitoring of the Ring Protocol state detected a recovery from a failure, but a setting suppresses a path switchback. The switch outputs this message when it detects a recovery from a failure at the master node. <ring id>: Ring ID [Action] Either wait for the suppression-time timeout specified by the "preempt-delay" configuration command or manually remove the path switchback suppression state with the "clear axrp preempt-delay" command.	
20170017	E3	AXRP <ring id> : canceled the suspension of the fault recovery process.
	Removal of Ring Protocol path switchback suppression was executed. The switch outputs this message when the path switchback suppression state is removed during such suppression at the master node. <ring id>: Ring ID [Action] None.	
20170018	E3	AXRP <ring id> : activated multi fault state monitoring.
	Multi-fault monitoring of Ring Protocol started. <ring id>: Ring ID [Action] None.	

Message ID	Event Level	Message text
	Contents and actions	
20170019	E3	AXRP <ring id> : detected multi fault recovery by receiving multi fault detection frames.
	Multi-fault monitoring of Ring Protocol detected recovery from multiple failures. The switch outputs this message when it receives a multi-fault monitoring frame at a shared node and detects recovery from multiple failures. <ring id>: Ring ID [Action] None.	
20170020	E4	AXRP <ring id> : detected multi fault by multi fault detection timeout.
	Multi-fault monitoring of Ring Protocol detected multiple failures. The switch outputs this message when the multi-fault monitoring function detects a timeout at the shared node. <ring id>: Ring ID [Action] Multiple failures might be occurring in a corresponding ring. Check the link and the node states.	
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.	
20170023	E4	AXRP <ring id> : detected fault by ring port status becoming Down.
	Monitoring of the Ring Protocol state detected a failure. This message is output when the switch status is standalone and the ring port goes down on the master node. <ring id>: Ring ID [Action] Check the status of the ring port of the target ring.	

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.	

Message ID	Event Level	Message text
	Contents and actions	
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.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
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.	
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 <mepid>.
	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 <mepid>.
	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.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
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.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
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.	
21100006	E3	IGMP snooping: Learning of IGMP snooping entries started because a master switch switchover occurred. (aging time = <time> seconds)
	Learning of IGMP snooping entries has started due to the switch status changing from backup to master in a stack configuration. <time>Learning time (seconds) [Action] None.	
21100007	E3	IGMP snooping: Learning of IGMP snooping entries finished after a master switch switchover occurred.
	Learning of IGMP snooping entries has finished due to the switch status changing from backup to master in a stack configuration. [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.	
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	

Message ID	Event Level	Message text
	Contents and actions	
	[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.	
25100006	E4	The VLAN MAC Address entry can't be registered at hardware tables(VLAN:<vlan id> MAC address:<mac address>).
	A VLAN MAC address entry cannot be set for hardware. <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.	

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.	
25100008	E4	VLAN (<vlan id>) vlan-mac registration failed.
	The vlan-mac setting failed. The number of VLANs that can be set for vlan-mac exceed the capacity limit. <vlan id>: VLAN ID [Action] Review the system configuration.	
25100019	E4	The vlan mapping entry can't be registered at hardware tables(VLAN <vlan id>, port(<switch no.>/<nif no.>/<port no.>)).
	Tag translation information entries cannot be registered in the hardware tables. <vlan id>: VLAN ID <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number [Action] Review the system configuration. However, depending on the hardware specification, the setting to the maximum of the capacity limit might not be available.	
2510001b	E3	Sum of number of VLAN on ports exceeded capacity.
	The total number of VLANs for each port exceed the capacity limit. [Action] Execute any of the following measures: • Use the "copy" command to apply the configuration file, with the total number of VLANs for each port being within the capacity limit, to the running-config file. • Change the total number of VLANs to within the capacity limit, and execute the "restart vlan" command. • 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.	

Message ID	Event Level	Message text
	Contents and actions	
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 switchport-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.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
	<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 [Action] None.	

Message ID	Event Level	Message text
	Contents and actions	
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.	
20a00022	E4	ULR:Both uplink redundant port(<switch no.>/<nif no.>/<port no.>) and port(ChGr:<channel group number>) are down.

Message ID	Event Level	Message text
	Contents and actions	
	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.
	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]	

Message ID	Event Level	Message text
	Contents and actions	
	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.	
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.	

Message ID	Event Level	Message text
	Contents and actions	
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	
26000001	E4	The ARP entry can't be registered at hardware tables. (<ipv4 address> [VRF <vrf id>])
	An ARP entry cannot be registered in the hardware tables. <ipv4 address>: IPv4 address of the ARP entry that cannot be registered in the hardware tables <vrf id> VRF ID [Action] Review the capacity limit. However, depending on specifications of the cache applied to the hardware, certain IP address combinations do not allow the setting to the maximum of the capacity limit.	
26000002	E4	The ARP entry can't be deleted from hardware tables.
	An ARP entry cannot be deleted from the hardware tables. [Action] Replace the Switch.	
26000003	E4	The NDP entry can't be registered at hardware tables. (<ipv6 address> [VRF <vrf id>])
	An NDP entry cannot be registered in the hardware tables. <ipv6 address>: IPv6 address of the NDP entry that cannot be registered in the hardware tables <vrf id> VRF ID [Action] Review the capacity limit. However, depending on specifications of the cache applied to the hardware, certain IPv6 address combinations do not allow the setting to the maximum of the capacity limit.	
26000004	E4	The NDP entry can't be deleted from hardware tables.
	An NDP entry cannot be deleted from the hardware tables. [Action] Replace the Switch.	
26000005	E4	IPv4 unicast routing information can't be registered at hardware tables. (<ipv4 prefix>/<masklen> [VRF <vrf id>])
	An IPv4 unicast routing table entry cannot be registered in the hardware tables. <ipv4 prefix>: IPv4 unicast routing table entry that cannot be registered in the hardware tables <masklen>: Subnet mask length of the above IPv4 unicast routing table entry <vrf id> VRF ID [Action] Review the capacity limit. However, depending on specifications of the cache applied to the hardware, certain IP addresses do not allow the setting to the maximum of the capacity limit.	

Message ID	Event Level	Message text
	Contents and actions	
26000006	E4	IPv4 unicast routing information can't be deleted from hardware tables.
	An IPv4 unicast routing table entry cannot be deleted from the hardware tables. [Action] Replace the Switch.	
26000007	E4	IPv4 multicast routing information can't be registered at hardware tables. (Source:<ipv4 address> Group:<ipv4 address> [VRF <vrf id>])
	An IPv4 multicast routing table entry cannot be registered in the hardware tables. <ipv4 address>: Source IPv4 address and group address of the IPv4 multicast routing table entry that cannot be registered in the hardware tables <vrf id> VRF ID [Action] Review the capacity limit. However, depending on specifications of the cache applied to the hardware, certain IP addresses do not allow the setting to the maximum of the capacity limit.	
26000008	E4	IPv4 multicast routing information can't be deleted from hardware tables.
	An IPv4 multicast routing table entry cannot be deleted from the hardware tables. [Action] Replace the Switch.	
26000009	E4	IPv6 unicast routing information can't be registered at hardware tables. (<ipv6 prefix>/<prefixlen> [VRF <vrf id>])
	An IPv6 unicast routing table entry cannot be registered in the hardware tables. <ipv6 prefix>: IPv6 unicast routing table entry that cannot be registered in the hardware tables <prefixlen>: Prefix length of the above IPv6 unicast routing table entry <vrf id> VRF ID [Action] Review the capacity limit. However, depending on specifications of the cache applied to the hardware, certain IPv6 addresses do not allow the setting to the maximum of the capacity limit.	
2600000a	E4	IPv6 unicast routing information can't be deleted from hardware tables.
	An IPv6 unicast routing table entry cannot be deleted from the hardware tables. [Action] Replace the Switch.	
2600000b	E4	IPv6 multicast routing information can't be registered at hardware tables. (Source:<ipv6 address> Group:<ipv6 address> [VRF <vrf id>])
	An IPv6 multicast routing table entry cannot be registered in the hardware tables. <ipv6 address>: Source address and group address of the IPv6 multicast routing table entry that cannot be registered in the hardware tables <vrf id> VRF ID	

Message ID	Event Level	Message text
	Contents and actions	
	[Action] Review the capacity limit. However, depending on specifications of the cache applied to the hardware, certain IPv6 addresses do not allow the setting to the maximum of the capacity limit.	
2600000c	E4	IPv6 multicast routing information can't be deleted from hardware tables.
	An IPv6 multicast routing table entry cannot be deleted from the hardware tables. [Action] Replace the Switch.	
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.	
50000003	E4	Duplication of IPv4 address <ipv4 address> with the node of MAC address <mac address> was detected.
	The IPv4 address <ipv4 address> is being used by the device that has the MAC address <mac address>. <ipv4 address>: IPv4 address that is registered for the interface for the Switch <mac address>: MAC address of the device for which the duplicate IPv4 address was detected [Action] 1. Change either this IPv4 address or the IPv4 address of the device that has the MAC address <mac address>. 2. When using VRRP, this message might be output frequently when the CPU load is heavy. In that case, increase the value of timers advertise for the VRRP configuration between devices comprising the VRRP.	
50000006	E4	The number of pieces of the ARP entry exceeds the capacity of this system.
	The number of ARP table entries exceeds the capacity limit of the Switch. [Action] If this message is issued often, take the following action: 1. Delete unnecessary information from the ARP configuration. 2. If unnecessary entries have been generated dynamically, delete them by using the "clear arp-cache" command while specifying the vrf all parameter. 3. Review the network system configuration, and change it to a new system configuration by reducing the number of ARP table entries.	

Message ID	Event Level	Message text
	Contents and actions	
50000007	E4	Because the number of pieces of the ARP entry exceeds the capacity of <vrf>, the old entry was deleted and the new entry was added.
	The number of ARP table entries for <vrf> has exceeded the maximum value for each VRF. Old entries are deleted, and new entries are added. <vrf>: VRF that exceeds the maximum ARP • VRF <vrf id>: VRF, the VRF ID of which is <vrf id> • global network: Global network [Action] If this message is issued often, take the following action: 1. Delete unnecessary information from the ARP configuration. 2. If unnecessary entries have been generated dynamically, delete them by using the "clear arp-cache" command. 3. Review the network system configuration, and change it to a new system configuration by reducing the number of ARP table entries.	
50000013	E4	The number of pieces of the IPv4 unicast routing information exceeds the capacity of this system.
	The number of IPv4 unicast route information entries exceeds the capacity limit of the Switch. [Action] 1. Delete unnecessary information from the IPv4 unicast route information. 2. Review the network system configuration, and change it to a new system configuration by reducing IPv4 unicast route information. 3. After implementing 1 or 2, specify vrf all * parameter for the "clear ip route" command.	
51000006	E4	The number of pieces of the IPv4 Multicast Routing entry exceeds the capacity of this system.
	The number of IPv4 multicast route information entries exceed the capacity limit of the Switch. [Action] 1. Delete unnecessary information from the IPv4 multicast route information. 2. Review the network system configuration, and change it to a new system configuration by reducing the IPv4 multicast route information.	
60000002	E4	The number of pieces of the NDP entry exceeds the capacity of this system.
	The number of NDP table entries exceeds the capacity limit of the Switch. [Action] If this message is issued often, take the following action: 1. Delete unnecessary information from the ndp configuration. 2. If unnecessary entries have been generated dynamically, delete them by specifying the vrf all parameter in the "clear ipv6 neighbors" command. 3. Review the network system configuration, and change it to a new system configuration by reducing the number of NDP table entries.	

Message ID	Event Level	Message text
	Contents and actions	
60000003	E4	Duplication of IPv6 address <ipv6 address> with the node of MAC address <mac address> was detected.
	Address duplication detection processing detected IPv6 address duplication. The IPv6 address <ipv6 address> that is set in the Switch conflicts with the device whose MAC address is <mac address>. Therefore, <ipv6 address> in this device is unavailable. You cannot use an unavailable IPv6 address until you change or delete the setting, and then re-specify it. To check the addresses that are unavailable because of address overlap, use the "show ipv6 interface" command. <ipv6 address>: IPv6 address of the Switch interface that has become unavailable because of address duplication detection <mac address>: MAC address of a device for which address duplication detection was detected [Action] 1. If <ipv6 address> set in the Switch is incorrect, change <ipv6 address> of the Switch. 2. If <ipv6 address> on the other device is incorrect, change <ipv6 address> of the conflicting device, delete <ipv6 address> for the Switch, and then re-specify it. 3. When using VRRP, this message might be output frequently when the CPU load is heavy. In that case, increase the value of timers advertise for the VRRP configuration between devices comprising the VRRP.	
60000004	E4	Because the number of pieces of the NDP entry exceeds the capacity of <vrf>, the old entry was deleted and the new entry was added.
	The number of NDP table entries for <vrf> has exceeded the maximum value for each VRF. Old entries are deleted, and new entries are added. <vrf>: VRF that exceeds the maximum NDP • VRF <vrf id>: VRF, the VRF ID of which is <vrf id> • global network: Global network [Action] If this message is issued often, take the following action: 1. Delete unnecessary information from the ndp configuration. 2. If unnecessary entries have been generated dynamically, delete them by executing the "clear ipv6 neighbors" command. 3. Review the network system configuration, and change it to a new system configuration by reducing the number of NDP table entries.	
60000008	E4	The number of pieces of the IPv6 unicast routing information exceeds the capacity of this system.
	The number of IPv6 unicast route information entries exceeds the capacity limit of the Switch. [Action] 1. Delete unnecessary information from the IPv6 unicast route information. 2. Review the network system configuration, and change it to a new system configuration by reducing IPv6 unicast route information. 3. After implementing 1 or 2, execute the "clear ipv6 route" command while specifying the vrf all * parameter.	

Message ID	Event Level	Message text
	Contents and actions	
61000005	E4	The number of pieces of the IPv6 Multicast Routing entry exceeds the capacity of this system.
	The number of IPv6 multicast route information entries exceed the capacity limit of the Switch. [Action] 1. Delete unnecessary information from the IPv6 multicast route information. 2. Review the network system configuration, and change it to a new system configuration by reducing the IPv6 multicast route information.	

3 Message Text Format

3.1 Tracking object log (TRO) [SL-L3A]

The following table describes the tracking object log.

Table 3-1: Tracking object log

No.	Message text	Description
1	Track object <track object id> is up. (type ICMP, address <destination address> [VRF <vrf id>])	Event (local device)
		The tracking status of the policy-based routing has transitioned from Down to Up. [Explanation of message variables] <track object id>: Tracking ID of the policy-based routing <destination address>: Polling destination address <vrf id>: VRF ID [Action] None.
2	Track object <track object id> is down. (type ICMP, address <destination address> [VRF <vrf id>])	Event (local device)
		The tracking status of the policy-based routing has transitioned from Up to Down. [Explanation of message variables] <track object id>: Tracking ID of the policy-based routing <destination address>: Polling destination address <vrf id>: VRF ID [Action] None.

3.2 IPv4 routing protocol information (RTM)

This section explains IPv4 routing protocol event information.

3.2.1 RIP

The following table gives the event information for IPv4 routing protocol information (RTM).

Table 3-2: IPv4 routing protocol (RIP) event information

No.	Message text	Description
1	rip_recv_response: Bad metric (<metric>) for net <destination address> from <source address> [(VRF <vrf id>)]	Error (remote device)
		Route information that has an invalid metric value (0, or 17 or larger) was received. [Explanation of message variables] <metric>: Metric value of the route information <destination address>: Route information destination address <source address>: Source gateway <vrf id>: VRF ID [Action] Check the unicast routing program (RIP) for the source gateway.
2	rip_recv_response: Bad mask (<mask>) for net <destination address> from <source address> [(VRF <vrf id>)]	Error (remote device)
		Route information that has an invalid network mask was received. [Explanation of message variables] <mask>: Route information network mask <destination address>: Route information destination address <source address>: Source gateway <vrf id>: VRF ID [Action] Check the unicast routing program (RIP) for the source gateway.
3	rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - ignoring version 0 packets	Error (remote device)
		A received RIP packet was ignored because the version field is 0. [Explanation of message variables] <rip command>: Received message type • Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry <source address>: Source gateway <vrf id>: VRF ID [Action] Check the unicast routing program (RIP) for the source gateway.
4	rip_recv:	Error (remote device)

No.	Message text	Description
	Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - reserved field not zero	A received RIP packet was ignored because the reserved field is not 0. [Explanation of message variables] <rip command>: Received message type • Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry <source address>: Source gateway <vrf id>: VRF ID [Action] Check the unicast routing program (RIP) for the source gateway.
5	rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - authentication failure [(Key-ID <key id>)]	Error (local or remote device)
		A received RIP packet was ignored because of an authentication error. This operation message is output according to the following conditions: 1. The messages from the first to the 16th event are output. 2. After 17 times from the beginning of the event occurrence, this message is output once every 256 times the event occurs. 3. If an event occurs 3 minutes or more after the last event occurred, this message is output depending on 1 and 2 above. Note that the above number of messages includes the count of the following messages: rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - illegal authentication type rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - illegal authentication key identifier (Key-ID <key id>) rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - illegal authentication sequence number (Key-ID <key id>) [Explanation of message variables] <rip command>: Received message type • Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry <source address>: Source gateway <vrf id>: VRF ID <key id>: Key identifier [Action] Check whether the authentication key for the local device RIP matches the authentication key for the remote device RIP. If they do not match, specify the authentication keys so that they do match.
6	rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - TRACE packets not supported	Warning (remote device)
		A received RIP packet was ignored because TRACE packets are not supported. [Explanation of message variables] <rip command>: Received message type

No.	Message text	Description
		• TraceOn, TraceOff <source address>: Source gateway <vrf id>: VRF ID [Action] Check the specifications of the unicast routing program (RIP) for the source gateway.
7	rip_init: Old copy of rtm is running	Error (local device)
		Unicast routing program might already be running. The unicast routing program automatically restarts. [Explanation of message variables] None. [Action] Take appropriate action by following the rtm aborted log.
8	RIP: The total number of RIP targets is more than the maximum permitted	Error (local device)
		The total number of RIP targets (neighboring) exceeds the maximum number permitted. [Explanation of message variables] None. [Action] Check, and if necessary, revise the RIP settings so that the maximum number of neighboring routers does not exceed the capacity limit.
9	rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - illegal authentication type	Error (remote device)
		A received RIP packet was ignored because the authentication type of authentication information is invalid. This operation message is output according to the following conditions: 1. The messages from the first to the 16th event are output. 2. After 17 times from the beginning of the event occurrence, this message is output once every 256 times the event occurs. 3. If an event occurs 3 minutes or more after the last event occurred, this message is output depending on 1 and 2 above. Note that the above number of messages includes the count of the following messages: rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - authentication failure [(Key-ID <key id>)] rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - illegal authentication key identifier (Key-ID <key id>) rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - illegal authentication sequence number (Key-ID <key id>) [Explanation of message variables] <rip command>: Received message type • Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry

No.	Message text	Description
		<source address>: Source gateway <vrf id>: VRF ID [Action] Check the unicast routing program (RIP) for the source gateway.
10	rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - illegal authentication key identifier (Key-ID <key id>)	Error (local or remote device) A received RIP packet was ignored because the key identifier of authentication information was invalid. This operation message is output according to the following conditions: 1. The messages from the first to the 16th event are output. 2. After 17 times from the beginning of the event occurrence, this message is output once every 256 times the event occurs. 3. If an event occurs 3 minutes or more after the last event occurred, this message is output depending on 1 and 2 above. Note that the above number of messages includes the count of the following messages: rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - authentication failure [(Key-ID <key id>)] rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - illegal authentication type rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - illegal authentication sequence number (Key-ID <key id>) [Explanation of message variables] <rip command>: Received message type • Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry <source address>: Source gateway <vrf id>: VRF ID <key id>: Key identifier [Action] Check whether the key identifier of authentication information for the local device RIP matches the key identifier of authentication information for the remote device RIP. If they do not match, specify the key identifiers so that they do match.
11	rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - illegal authentication sequence number (Key-ID <key id>)	Error (remote device) A received RIP packet was ignored because the sequence number of authentication information was invalid. This operation message is output according to the following conditions: 1. The messages from the first to the 16th event are output. 2. After 17 times from the beginning of the event occurrence, this message is output once every 256 times the event occurs. 3. If an event occurs 3 minutes or more after the last event occurred, this message is output depending on 1 and 2 above.

No.	Message text	Description
		Note that the above number of messages includes the count of the following messages: rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - authentication failure [(Key-ID <key id>)] rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - illegal authentication type rip_recv: Ignoring RIP <rip command> packet from <source address> [(VRF <vrf id>)] - illegal authentication key identifier (Key-ID <key id>) [Explanation of message variables] <rip command>: Received message type • Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry <source address>: Source gateway <vrf id>: VRF ID <key id>: Key identifier [Action] Check the unicast routing program (RIP) for the source gateway.

3.2.2 OSPF [SL-L3A]

The following table gives the event information for IPv4 routing protocol information (RTM).

Table 3-3: IPv4 routing protocol (OSPF) event information

No.	Message text	Description
1	OSPF SENT <source address> -> <destination address> [(VRF <vrf id>)] : <error string>.	Warning (local device)
		An attempt to send an OSPF packet failed. [Explanation of message variables] <source address>: Source IPv4 address <destination address>: Destination IPv4 address <vrf id>: VRF ID <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
2	OSPF: Helper to adjacency <router id> address <address> [(VRF <vrf id>)] failed because restart time is up.	Information (remote device)
		The helper router behavior stopped because the waiting time for restart elapsed. [Explanation of message variables] <router id>: Neighboring router's router ID <address>: Neighboring router's IPv4 address <vrf id>: VRF ID [Action] Check if the neighboring router has stopped the restart. If it has not stopped, adjust the restart time of the neighboring router.

No.	Message text	Description
3	OSPF: Helper to adjacency <router id> address <address> [(VRF <vrf id>)] failed because network topology is changed.	Warning (local device or network)
		The helper router behavior stopped because the topology was changed. [Explanation of message variables] <router id>: Neighboring router's router ID <address>: Neighboring router's IPv4 address <vrf id>: VRF ID [Action] None.
4	OSPF RECV [Area <area id>] <source address> -> <destination address> [(VRF <vrf id>)] : <log type>.	Warning (local device or remote device)
		A received OSPF packet is invalid. However, multicast packets received from broadcast-type interfaces that have not been set as OSPF interfaces are discarded without log acquisition. [Explanation of message variables] <area id>: Area ID <source address>: Source IPv4 address <destination address>: Destination IPv4 address <vrf id>: VRF ID <log type>: One of the following log types: • IP: bad destination • IP: bad protocol • IP: received my own packet • OSPF: bad packet type • OSPF: bad version • OSPF: bad checksum • OSPF: packet too small • OSPF: packet size > ip length • OSPF: bad area id • OSPF: unknown neighbor • OSPF: area mismatch • OSPF: bad virtual link • OSPF: bad authentication type • OSPF: bad authentication key • OSPF: interface down • HELLO: netmask mismatch • HELLO: hello timer mismatch • HELLO: dead timer mismatch • HELLO: NBMA neighbor unknown • HELLO: extern option mismatch • DD: extern option mismatch

No.	Message text	Description
		• HELLO: router id confusion • DD: router id confusion • LS ACK: Unknown LSA type • LS REQ: empty request • LS REQ: bad request • LS UPD: LSA checksum bad [Action] The action to be taken depends on the type of the log. • IP: bad destination If <source address> is not a directly-connected network, or OSPF has not been set for the interface <destination address>, modify the OSPF interface settings. • IP: bad protocol • IP: received my own packet • OSPF: bad packet type • OSPF: bad version • OSPF: bad checksum • OSPF: packet too small • OSPF: packet size > ip length • OSPF: bad area id A neighboring router is sending an invalid packet. Check the unicast routing program (OSPF) of the neighboring router. • OSPF: unknown neighbor Non-Hello packets were received from the neighboring router that is not recognized by Hello, but no action is required. • OSPF: area mismatch • OSPF: bad virtual link If packets are received from the new neighboring router, modify the area settings. In other cases, no action is required. • OSPF: bad authentication type • OSPF: bad authentication key Modify the authentication settings. • OSPF: interface down None. • HELLO: netmask mismatch • HELLO: hello timer mismatch • HELLO: dead timer mismatch • HELLO: NBMA neighbor unknown Modify the OSPF interface settings.

No.	Message text	Description
		• HELLO: extern option mismatch • DD: extern option mismatch Modify the stub area settings. • HELLO: router id confusion • DD: router id confusion Modify the router ID settings. • LS ACK: Unknown LSA type • LS REQ: empty request • LS REQ: bad request • LS UPD: LSA checksum bad A neighboring router is sending an invalid packet. Check the unicast routing program (OSPF) of the neighboring router.
5	OSPF: Abort due to <address> mask <mask1> advertisement was blocked by LSA <lsid> mask <mask2> Age <age>.	Error (local device) There is a conflict between LSDB <lsid> and the route. The unicast routing program automatically restarts. [Explanation of message variables] <address>: Route information destination address <mask1>: Route information network mask <lsid>: LSID of LSA <mask2>: LSA network mask <age>: Time elapsed from generation of LSA [Action] Take appropriate action by following the rtm aborted log.
6	OSPF: Lost adjacency <router id> address <address>(<interface name>) due to sequence mismatch (<sequence1> versus <sequence2>).	Warning (local device or remote device) A neighboring router was lost due to a sequence mismatch. [Explanation of message variables] <router id>: Neighboring router's router ID <address>: Neighboring router's IPv4 address <interface name>: Interface name <sequence1>: Sequence number in control data <sequence2>: Sequence number in the DD message [Action] If this warning occurs frequently, extend the interval for retransmitting the OSPF packets (retransmitinterval).
7	OSPF: Lost adjacency <router id> address <address>(<interface name>) because no Hello received recently.	Warning (remote device or network) Adjacency was terminated because Hello packets that should be sent periodically from the neighboring router were not received during a given interval. This occurs when the neighboring router is deactivated, or if a problem occurs in communication between the Switch and the neighboring router. [Explanation of message variables] <router id>: Neighboring router's router ID <address>: Neighboring router's IPv4 address

No.	Message text	Description
		<interface name>: Interface name [Action] If this warning occurs frequently, shorten the interval for sending Hello packets (hellointerval) or extend the maximum interval for receiving Hello packets (routerdeadinterval).
8	OSPF: Lost adjacency <router id> address <address>(<interface name>) because neighbor didn't receive my Hello recently.	Warning (remote device or network)
		Adjacency was terminated because the neighboring router no longer recognizes the Switch. This occurs when the neighboring router is restarted or Hello packets sent by the Switch are not properly received by the neighboring router. [Explanation of message variables] <router id>: Neighboring router's router ID <address>: Neighboring router's IPv4 address <interface name>: Interface name [Action] If this warning occurs frequently, shorten the interval for sending Hello packets (hellointerval) or extend the maximum interval for receiving Hello packets (routerdeadinterval).
9	OSPF: Lost adjacency <router id1> address <address>(<interface name>) due to bad LS Request (<lsid> <router id2> <ls type>).	Error (remote device)
		The neighboring router was lost due to an invalid LS request. [Explanation of message variables] <router id1>: Neighboring router's router ID <address>: Neighboring router's IPv4 address <interface name>: Interface name <lsid>: LSID of LSA <router id2>: LSA advertising router ID <ls type>: LSA LS type code [Action] Check the unicast routing program (OSPF) of the neighboring router.
10	OSPF: Adjacency <router id> address <address>(<interface name>) is established.	Information (local or remote device)
		A connection with the OSPF neighboring router was successfully established. [Explanation of message variables] <router id>: Neighboring router's router ID <address>: Neighboring router's IPv4 address <interface name>: Interface name [Action] None.
11	OSPF: Checksum failed at LSA type <ls type> ID <lsid> adv-router <router id> in this system's LSDB that belongs to Area <area id>, Domain <domain id> [on VRF <vrf id>].	Error (local device)
		LSDB checksum is invalid. The unicast routing program automatically restarts. [Explanation of message variables] <ls type>: LSA LS type code <lsid>: LSID of LSA <router id>: LSA advertising router ID

No.	Message text	Description
		<area id>: LSA area ID <domain id>: LSA domain ID <vrf id>: VRF ID [Action] Take appropriate action by following the rtm aborted log.
12	OSPF: Recovered from stub router (in [(VRF <vrf id>)] domain <domain id>).	Information (local device)
		The stub router behavior will now end. [Explanation of message variables] <vrf id>: VRF ID <domain id>: OSPF domain ID [Action] None.
13	OSPF: Graceful restart failed (in [(VRF <vrf id>)] domain <domain id>) because adjacency <router id> address <address> doesn't help me.	Warning (remote device or network)
		Graceful restart failed because the neighboring router is not working as a helper router. [Explanation of message variables] <vrf id>: VRF ID <domain id>: OSPF domain ID <router id>: Neighboring router's router ID <address>: Neighboring router's IPv4 address [Action] Check the graceful restart configuration of the neighboring router.
14	OSPF: Graceful restart failed (in [(VRF <vrf id>)] domain <domain id>) because adjacency <router id> address <address> gives up me.	Warning (remote device or network)
		Graceful restart failed because the neighboring router stopped working as a helper router. [Explanation of message variables] <vrf id>: VRF ID <domain id>: OSPF domain ID <router id>: Neighboring router's router ID <address>: Neighboring router's IPv4 address [Action] If this error frequently occurs, check the OSPF status of the neighboring router and the cause of the helper function stopping.
15	OSPF: Graceful restart failed (in [(VRF <vrf id>)] domain <domain id>) because restart time is up.	Warning (local device)
		Graceful restart failed because the reconnection and LSA synchronization with all neighboring routers connected before restart were not possible within the restart time. [Explanation of message variables] <vrf id>: VRF ID <domain id>: OSPF domain ID [Action] Check the restart time configuration.

No.	Message text	Description
16	OSPF: Graceful restart finished successfully (in [(VRF <vrf id>)] domain <domain id>).	Information (local device)
		Graceful restart was successful. [Explanation of message variables] <vrf id>: VRF ID <domain id>: OSPF domain ID [Action] None.

3.2.3 BGP4 [SL-L3A]

The following table gives the event information for IPv4 routing protocol information (RTM).

Table 3-4: IPv4 routing protocol (BGP4) event information

No.	Message text	Description
1	bgp_check_auth: Synchronization failure with BGP task <task name>	Error (remote device)
		The value of the header marker of the message received by BGP4 task is invalid. [Explanation of message variables] <task name>: BGP4 task name [Action] Check the unicast routing program (BGP4) in the peer.
2	bgp_trace: Unsupported BGP version <version>!!!	Error (local device)
		The BGP version number in control data was invalid. The unicast routing program automatically restarts. [Explanation of message variables] <version>: BGP version number in control data [Action] Take appropriate action by following the rtm aborted log.
3	bgp_log_notify: Notify message received from <bgp name> [(<description>)] is truncated (length <length>)	Error (remote device)
		The length of the NOTIFICATION message received from the relevant peer was invalid. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received data length [Action] Check the unicast routing program (BGP4) in the peer.
4	bgp_send:	Warning (local device)

No.	Message text	Description
	Sending <length> bytes to <bgp name> [(<description>)] blocked (no spooling requested): <error string>	An attempt to send a message to the relevant peer failed because the socket buffer becomes full. [Explanation of message variables] <length>: Send request message length <bgp name>: Target peer name <description>: Description name of the destination peer <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
5	bgp_send: Sending <length> bytes to <bgp name> [(<description>)] failed: <error string>	Warning (local device)
		An attempt to send a message to the relevant peer has failed. [Explanation of message variables] <length>: Send request message length <bgp name>: Target peer name <description>: Description name of the destination peer <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
6	bgp_send: Sending <length> bytes to <bgp name> [(<description>)]: Connection closed	Warning (local device, remote device, or network)
		Sending of the message to the peer failed because the connection was disconnected. [Explanation of message variables] <length>: Send request message length <bgp name>: Target peer name <description>: Description name of the destination peer [Action] If this error occurs frequently, check the cause of the disconnection.
7	bgp_send: Sending to <bgp name> [(<description>)] looping: <error string>	Warning (local device)
		An attempt to send a message to the relevant peer has timed out. [Explanation of message variables] <bgp name>: Target peer name <description>: Description name of the destination peer <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
8	bgp_send_open: Internal error! peer <bgp name> [(<description>)], version <version>	Error (local device)
		The BGP version number of the OPEN message to be sent to the relevant peer was invalid. The unicast routing program automatically restarts. [Explanation of message variables] <bgp name>: Target peer name <description>: Description name of the destination peer

No.	Message text	Description
		<version>: BGP version number in the send message [Action] Take appropriate action by following the rtm aborted log.
9	bgp_path_attr_error from <routine>: Update error subcode <code> (<error string>) for peer <bgp name> [(<description>)] detected. <length> bytes error data - 1st five: <error data>	Error (remote device)
		An error was detected in the UPDATE message received from the relevant peer. [Explanation of message variables] <routine>: Internal routine name <code> (<error string>): Error cause <bgp name>: Source peer name <description>: Description name of the source peer <length>: Error data length <error data>: First five bytes of error data [Action] Check the unicast routing program (BGP4) in the peer.
10	bgp_recv: Read from peer <bgp name> [(<description>)] failed: <error string>	Warning (local device)
		An attempt to receive a message from the relevant peer failed. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
11	bgp_recv: Peer <bgp name> [(<description>)]: Received unexpected EOF	Warning (local device, remote device, or network)
		An attempt to receive a message from the relevant peer failed due to disconnection. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] If this error occurs frequently, check the cause of the disconnection.
12	bgp_read_message: Peer <bgp name> [(<description>)]: <message type> message arrived with length <length>	Error (remote device)
		An invalid-length message was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <message type>: Received message type • invalid, Open, Update, Notification, KeepAlive <length>: Received data length [Action] Check the unicast routing program (BGP4) in the peer.

No.	Message text	Description
13	bgp_read_message: Peer <bgp name> [(<description>)]: <message type1> arrived, expected <message type2> [or <message type2>]	Error (remote device) A message whose message type is inappropriate for the current state was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <message type1>: Received message type • invalid, Open, Update, Notification, KeepAlive <message type2>: Message type appropriate for the current state • invalid, Open, Update, Notification, KeepAlive [Action] Check the unicast routing program (BGP4) in the peer.
14	bgp_get_open: Peer <bgp name> [(<description>)]: Received short version <version> message (<length> octets)	Error (remote device) An invalid-length OPEN message was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <version>: BGP version number in the received message <length>: Received data length [Action] Check the unicast routing program (BGP4) in the peer.
15	bgp_get_open: Received unsupported version <version> message from peer <bgp name> [(<description>)]	Warning (remote device) An OPEN message that has an unsupported BGP version was received from a peer. [Explanation of message variables] <version>: BGP version number of received messages <bgp name>: Source peer name <description>: Description name of the source peer [Action] Make sure that the peer supports BGP version 4.
16	bgp_get_open: Peer <bgp name> [(<description>)]: Hold time too small (<holdtime>)	Error (remote device) An OPEN message whose hold time is less than three seconds was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <holdtime>: Hold time in the received message [Action] Check the peer configuration.

No.	Message text	Description
17	bgp_get_open: Peer <bgp name> [(<description>)]: Invalid BGP identifier <router id>	Error (remote device)
		An OPEN message that has an invalid BGP identifier was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <router id>: BGP identifier in the received message [Action] Check the unicast routing program (BGP4) in the peer.
18	bgp_get_open: Peer <bgp name> [(<description>)]: Unsupported optional parameter <option>	Error (remote device)
		An OPEN message that contains an invalid option code was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <option>: Option code in the received message [Action] Check the unicast routing program (BGP4) in the peer.
19	bgp_recv_open: Peer <bgp name> [(<description>)] claims AS <as1>, <as2> configured	Warning (local device or remote device)
		An OPEN message that has a different AS number than the configured AS number was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <as1>: AS number of the received message <as2>: AS number of the peer in the configuration [Action] Check the configuration.
20	bgp_recv_open: Peer <bgp name> [(<description>)] accepted mismatched versions: Peer <version1> this system <version2>	Warning (remote device)
		A KEEPALIVE message that has a mismatched BGP version number was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <version1>: Remote BGP version number <version2>: Local BGP version number [Action] Make sure that the peer supports BGP version 4.
21	bgp_pp_recv: No group for <bgpp name> found, dropping peer	Warning (local device or remote device)
		An OPEN message was received from a peer that was not set. [Explanation of message variables] <bgpp name>: Source peer name [Action] Check the configuration.

No.	Message text	Description
22	bgp_pp_recv: Rejecting connection from <bgp name> [(<description>)], peer in state <state>	Warning (remote device or network)
		An OPEN message was received from the relevant peer during the Idle, OpenConfirm, or Established status. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <state>: Peer status • Idle, OpenConfirm, Established [Action] The connection has become unstable. If this error occurs frequently, check the cause of the instability.
23	bgp_pp_recv: Dropping <bgpp name> version <version>, <bgp name> [(<description>)] wants version 4	Warning (remote device)
		An OPEN message that has an unsupported BGP version was received from a peer. [Explanation of message variables] <bgpp name>, <bgp name>: Source peer name <version>: BGP version number of received messages <description>: Description name of the source peer [Action] Check the BGP version supported by the peer.
24	bgp_pp_recv: Peer <bgp name> [(<description>)] sent unexpected extra data, probably insane	Error (remote device)
		Unnecessary data is appended to the message from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.
25	bgp_check_capability_match: Capability of peer <bgp name> [(<description>)] is unmatched	Warning (remote device)
		The capability settings specified for the Switch are not specified for the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] Check the configuration.

No.	Message text	Description
26	bgp_write_flush: Sending <length1> (sent <length2>) bytes to <bgp name> [(<description>)] failed: <error string>	Warning (local device)
		An attempt to send a message to the relevant peer has failed. [Explanation of message variables] <length1>: Send request data length <length2>: Sent data length <bgp name>: Target peer name <description>: Description name of the destination peer <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
27	bgp_write_flush: Sending <length1> (sent <length2>) bytes to <bgp name> [(<description>)]: Connection closed	Warning (local device, remote device, or network)
		Sending of the message to the peer failed because the connection was disconnected. [Explanation of message variables] <length1>: Send request data length <length2>: Sent data length <bgp name>: Target peer name <description>: Description name of the destination peer [Action] If this error occurs frequently, check the cause of the disconnection.
28	bgp_write_flush: Sending to <bgp name> [(<description>)] (sent <length1>, <length2> remain[s]) looping: <error string>	Warning (local device)
		An attempt to send a message to the relevant peer has timed out. [Explanation of message variables] <bgp name>: Target peer name <description>: Description name of the destination peer <length1>: Sent data length <length2>: Length of the data that remains unsent <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
29	bgp_peer_connected: task_get_addr_local(<bgp name> [(<description>)]): <error string>	Warning (local device)
		Extraction of the local address used for establishing a connection to the relevant peer failed. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
30	bgp_connect_start:	Warning (local device)

No.	Message text	Description
	Peer <bgp name> [(<description>)] local address <ipv4 address> unavailable, connection failed	An attempt to establish a connection failed because the local address used for establishing a connection to the relevant peer could not be used (bind failure). [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer <ipv4 address>: Local address used for peering [Action] If this error frequently occurs, determine the cause of the error.
31	bgp_traffic_timeout: Holdtime expired for <bgp name> [(<description>)]	Warning (remote device or network)
		A hold timeout for the relevant peer occurred. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] Check the unicast routing program (BGP4) in the peer.
32	bgp_traffic_timeout: Error sending KEEPALIVE to <bgp name> [(<description>)]: <error string>	Warning (local device)
		An attempt to send a KEEPALIVE message to the relevant peer failed. [Explanation of message variables] <bgp name>: Target peer name <description>: Description name of the destination peer <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
33	bgp_listen_accept: accept(<socket>): <error string>	Warning (local device)
		An attempt to accept the connection failed. [Explanation of message variables] <socket>: Socket descriptor number <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
34	bgp_listen_accept: task_get_addr_local() failed, terminating!!	Error (local device)
		Extraction of the local address used for establishing a connection failed. The connection will be closed. [Explanation of message variables] None. [Action] If this error frequently occurs, check the unicast routing program (BGP4) in the peer.
35	bgp_listen_start: Couldn't get BGP listen socket!!	Error (local device)

No.	Message text	Description
		An attempt to create a socket for establishing a connection failed. The unicast routing program automatically restarts. [Explanation of message variables] None. [Action] Take appropriate action by following the rtm aborted log.
36	bgp_listen_start: listen: <error string>	Error (local device)
		Preparation for accepting a connection failed. The unicast routing program automatically restarts. [Explanation of message variables] <error string>: Error cause [Action] Take appropriate action by following the rtm aborted log.
37	bgp_set_peer_if: BGP peer <bgp name> [(<description>)] interface not found. Leaving peer idled	Warning (local device)
		The interface connected to the relevant peer was not found. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] Check the configuration.
38	bgp_set_peer_if: BGP peer <bgp name> [(<description>)] local address <ipv4 address> not on shared net. Leaving peer idled	Warning (local device)
		The local address used for establishing a connection to the relevant peer is not in the same network. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer <ipv4 address>: Local address used for establishing a connection [Action] Check the configuration.
39	bgp_pp_timeout: Peer <bgpp name> timed out waiting for OPEN	Warning (remote device or network)
		The timer for waiting for an OPEN message from the relevant peer timed out. [Explanation of message variables] <bgpp name>: Connection target peer name [Action] Check the unicast routing program (BGP4) in the peer.
40	bgp_peer_init: BGP peer <bgp name> [(<description>)] local address <ipv4 address> not found. Leaving peer idled	Warning (local device)
		The interface for the local address used for establishing a connection to the relevant peer is not found. [Explanation of message variables] <bgp name>: Connection target peer name

No.	Message text	Description
		<description>: Description name of the connection target peer <ipv4 address>: Local address used for establishing a connection [Action] Check the configuration.
41	bgp_recv_v4_update: Peer <bgp name> [(<description>)]: Strange message header length <length>	Error (remote device)
		The message length in the message header of a message received from the relevant peer is invalid. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Message length of the received message header [Action] Check the unicast routing program (BGP4) in the peer.
42	bgp_recv_v4_update: Peer <bgp name> [(<description>)] unrecognized message type <type>	Error (remote device)
		The message type of a message received from the relevant peer is invalid. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <type>: Message type [Action] Check the unicast routing program (BGP4) in the peer.
43	bgp_recv_v4_update: Received OPEN message from <bgp name> [(<description>)], state is ESTABLISHED	Warning (remote device or network)
		An OPEN message was received from the relevant peer in the ESTABLISHED status. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] The connection has become unstable. If this error occurs frequently, check the cause of the instability.
44	bgp_recv_v4_update: Peer <bgp name> [(<description>)] UPDATE length <length> too small	Error (remote device)
		The length of the UPDATE message from the relevant peer is too short. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received data length [Action] Check the unicast routing program (BGP4) in the peer.

No.	Message text	Description
45	bgp_recv_v4_update: Peer <bgp name> [(<description>)] UPDATE unreachable prefix length <length1> exceeds packet length <length2>	Error (remote device)
		The prefix length of unreachable route information of the UPDATE message from the relevant peer exceeds the packet length. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length1>: Prefix length of unreachable route information in the received message <length2>: Received packet length [Action] Check the unicast routing program (BGP4) in the peer.
46	bgp_recv_v4_update: Peer <bgp name> [(<description>)] UPDATE zero attribute length followed by <length> bytes of garbage	Error (remote device)
		The attribute length of the UPDATE message from the relevant peer is 0 even though actual data exists. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Actual data length [Action] Check the unicast routing program (BGP4) in the peer.
47	bgp_recv_v4_update: Peer <bgp name> [(<description>)] UPDATE path attribute length <length1> too large (<length2> bytes remaining)	Error (remote device)
		The path attribute length of the UPDATE message from the relevant peer is too long compared to the actual path attribute length. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length1>: Path attribute length of the received message <length2>: Actual data length [Action] Check the unicast routing program (BGP4) in the peer.
48	bgp_recv_v4_update: Peer <bgp name> [(<description>)] UPDATE no next hop found	Error (remote device)
		The next hop attribute is not found in the UPDATE message from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.
49	bgp_recv_v4_update:	Error (remote device)

No.	Message text	Description
	External peer <bgp name> [(<description>)] UPDATE included LOCALPREF attribute	The LOCALPREF attribute is included in the UPDATE message from the relevant external peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.
50	bgp_recv_v4_update: Peer <bgp name> [(<description>)] UPDATE no LOCALPREF attribute found	Error (remote device)
		The LOCALPREF attribute is not found in the UPDATE message from the relevant internal peer. [Explanation of message variables] <bgp name>: Source peer number <description>: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.
51	bgp_recv_v4_update: Peer <bgp name> [(<description>)] UPDATE has path attributes but no reachable prefixes!	Error (remote device)
		The UPDATE message from the relevant peer has path attributes but has no reachability information. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] Check the unicast routing program (BGP4) in the peer.
52	bgp_recv_v4_unreach: Peer <bgp name> [(<description>)] UPDATE: Invalid unreachable prefix length <length>	Error (remote device)
		The prefix length of unreachable route information of the UPDATE message received from the relevant peer is invalid. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Prefix length in received messages [Action] Check the unicast routing program (BGP4) in the peer.
53	bgp_recv_v4_unreach: Peer <bgp name> [(<description>)] UPDATE: Prefix length <length1> exceeds unreachable prefix data remaining (<length2> bytes)	Error (remote device)
		The prefix length of unreachable route information of the UPDATE message received from the relevant peer exceeds the prefix data of unreachable route information. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length1>: Prefix length in received messages <length2>: Actual data length [Action] Check the unicast routing program (BGP4) in the peer.

No.	Message text	Description
54	bgp_recv_v4_unreach: Peer <bgp name> [(<description>)] UPDATE: Ignoring unreachable route with two or more labels (<length1> of <length2>)	Warning (remote device) Routes of unreachable route information that has multiple labels of the UPDATE message received from the relevant peer are ignored. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length1> of <length2>: The location of invalid information in the message [Action] Check the unicast routing program (BGP4) in the peer.
55	bgp_recv_v4_unreach: Peer <bgp name> [(<description>)] UPDATE: Ignoring unreachable route with RD 0 prefix (<length1> of <length2>)	Error (remote device) Routes of unreachable route information that has RD 0 of the UPDATE message received from the relevant peer are ignored. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length1> of <length2>: The location of invalid information in the message [Action] Check the unicast routing program (BGP4) in the peer.
56	bgp_recv_v4_unreach: Peer <bgp name> [(<description>)] UPDATE: Ignoring invalid unreachable route <ipv4 address>/<mask> (<length1> of <length2>)	Error (remote device) Invalid routes of unreachable route information of the UPDATE message received from the relevant peer are ignored. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <ipv4 address>: Destination address of unreachable route information <mask>: Network mask of unreachable route information <length1> of <length2>: The location of invalid information in the message [Action] Check the unicast routing program (BGP4) in the peer.
57	bgp_recv_v4_reach: Peer <bgp name> [(<description>)] AS <as1> received path with first AS <as2>	Error (remote device) The AS path whose next- hop AS number is <as2> was received from the peer whose AS number is <as1>. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <as1>: AS number of the source peer <as2>: Next-hop AS number in the received message [Action] Check the unicast routing program (BGP4) in the peer.

No.	Message text	Description
58	bgp_recv_v4_reach: Peer <bgp name> [(<description>)] UPDATE: Invalid prefix length <length>	Error (remote device)
		The prefix length of the UPDATE message received from the relevant peer is invalid. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Prefix length in received messages [Action] Check the unicast routing program (BGP4) in the peer.
59	bgp_recv_v4_reach: Peer <bgp name> [(<description>)] UPDATE: Prefix length <length1> exceeds prefix data remaining (<length2> bytes)	Error (remote device)
		The prefix length of the UPDATE message received from the relevant peer exceeds the actual prefix length. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length1>: Prefix length in received messages <length2>: Actual prefix length [Action] Check the unicast routing program (BGP4) in the peer.
60	bgp_recv_v4_reach: Peer <bgp name> [(<description>)] UPDATE: Ignoring route with two or more labels (<length1> of <length2>)	Warning (remote device)
		Routes that have multiple labels of the UPDATE message received from the relevant peer are ignored. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length1> of <length2>: The location of invalid information in the received message. [Action] Check the unicast routing program (BGP4) in the peer.
61	bgp_recv_v4_reach: Peer <bgp name> [(<description>)] UPDATE: Ignoring route with RD 0 prefix (<length1> of <length2>)	Error (remote device)
		Routes that have RD 0 of the UPDATE message received from the relevant peer are ignored. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length1> of <length2>: The location of invalid information in the received message. [Action] Check the unicast routing program (BGP4) in the peer.

No.	Message text	Description
62	bgp_recv_v4_reach: Peer <bgp name> [(<description>)] UPDATE:Included invalid route <ipv4 address>/<mask> (<length1> of <length2>)	Error (remote device)
		The UPDATE message received from the relevant peer includes invalid routes. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <ipv4 address>: Destination address <mask>: Network mask <length1> of <length2>: The location of invalid information in the received message. [Action] Check the unicast routing program (BGP4) in the peer.
63	bgp_recv_v4_reach: Ignoring network 0 route <ipv4 address>/<mask> from peer <bgp name> [(<description>)] (<length1> of <length2>)	Warning (remote device)
		Routes addressed to network 0 from the relevant peer are ignored. [Explanation of message variables] <ipv4 address>: Destination address <mask>: Network mask <bgp name>: Source peer name <description>: Description name of the source peer <length1> of <length2>: The location of invalid information in the received message. [Action] Check the unicast routing program (BGP4) in the peer.
64	bgp_recv_v4_reach: Ignoring loopback route from peer <bgp name> [(<description>)] (<length1> of <length2>)	Warning (remote device)
		Loopback routes from the relevant peer are ignored. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length1> of <length2>: The location of invalid information in the received message. [Action] Check the unicast routing program (BGP4) in the peer.
65	bgp_recv_mp_unreach: Peer <bgp name> [(<description>)] UPDATE: Invalid length of MP_UNREACH_NLRI attribute(<length>) : No address family	Error (remote device)
		The length of the MP_UNREACH_NLRI attribute for the UPDATE message received from the peer is invalid. No address family exists. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received MP_UNREACH_NLRI attribute length [Action] Check the unicast routing program (BGP4) in the peer.

No.	Message text	Description
66	bgp_recv_mp_unreach: Peer <bgp name> [(<description>)] UPDATE: Invalid address family (<address family>) in MP_UNREACH_NLRI attribute	Error (remote device)
		The address family of the MP_UNREACH_NLRI attribute for the UPDATE message received from the peer is invalid. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <address family>: Address family information of the received MP_UNREACH_NLRI attribute [Action] Check the unicast routing program (BGP4) in the peer.
67	bgp_recv_mp_reach: Peer <bgp name> [(<description>)] UPDATE: Invalid length of MP_REACH_NLRI attribute(<length>) : No address family	Error (remote device)
		The length of the MP_REACH_NLRI attribute for the UPDATE message received from the peer is invalid. No address family exists. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4) in the peer.
68	bgp_recv_mp_reach: Peer <bgp name> [(<description>)] UPDATE: Invalid address family(<address family>) in MP_REACH_NLRI attribute	Error (remote device)
		The address family of the MP_REACH_NLRI attribute for the UPDATE message received from the peer is invalid. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <address family>: Address family information of the received MP_REACH_NLRI attribute [Action] Check the unicast routing program (BGP4) in the peer.
69	bgp_recv_mp_reach: Peer <bgp name> [(<description>)] UPDATE: Invalid length of MP_REACH_NLRI attribute(<length>) : No nexthop length	Error (remote device)
		The length of the MP_REACH_NLRI attribute for the UPDATE message received from the peer is invalid. No next hop length exists. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4) in the peer.

No.	Message text	Description
70	bgp_recv_mp_reach: Peer <bgp name> [(<description>)] UPDATE: Invalid nexthop length(<length>) in MP_REACH_NLRI attribute	Error (remote device) The next hop length of the MP_REACH_NLRI attribute for the UPDATE message received from the peer is invalid. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Next hop length of the received MP_REACH_NLRI attribute [Action] Check the unicast routing program (BGP4) in the peer.
71	bgp_recv_mp_reach: Peer <bgp name> [(<description>)] UPDATE: Invalid length of MP_REACH_NLRI attribute(<length>) : No nexthop	Error (remote device) The length of the MP_REACH_NLRI attribute for the UPDATE message received from the peer is invalid. No next hop exists. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4) in the peer.
72	bgp_recv_mp_reach: Peer <bgp name> [(<description>)] UPDATE: Invalid rd of nexthop (<rd1>:<rd2>) in MP_REACH_NLRI attribute	Error (remote device) The next hop RD of the MP_REACH_NLRI attribute for the UPDATE message received from the peer is invalid. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <rd1>:<rd2>: Next hop RD of the received MP_REACH_NLRI attribute [Action] Check the unicast routing program (BGP4) in the peer.
73	bgp_recv_mp_reach: Peer <bgp name> [(<description>)] UPDATE: Invalid length of MP_REACH_NLRI attribute(<length>) : No reserved	Error (remote device) The length of the MP_REACH_NLRI attribute for the UPDATE message received from the peer is invalid. No reserved field exists. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4) in the peer.

No.	Message text	Description
74	bgp_recv_mp_reach: Peer <bgp name> [(<description>)] UPDATE: Invalid length of MP_REACH_NLRI attribute(<length>) : No snpa length	Error (remote device)
		The length of the MP_REACH_NLRI attribute for the UPDATE message received from the peer is invalid. No SNPA length exists. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4) in the peer.
75	bgp_recv_mp_reach: Peer <bgp name> [(<description>)] UPDATE: Invalid length of MP_REACH_NLRI attribute(<length>) : No snpa	Error (remote device)
		The length of the MP_REACH_NLRI attribute for the UPDATE message received from the peer is invalid. No SNPA exists. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4) in the peer.
76	bgp_peer_established: Peer <bgp name> [(<description>)] connection established	Information (local or remote device)
		A BGP4 connection was established with the relevant peer. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] None.
77	bgp_ifachange: Peer <bgp name> [(<description>)]: Closed connection by changing interface state	Information (local or remote device)
		A BGP4 connection was closed due to a change in the interface state. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] Check the cause of the change in the interface state.
78	bgp_terminate: Peer <bgp name> [(<description>)]: Closed connection by terminating bgp	Information (local device)
		A BGP4 connection was closed due to the termination of a BGP4 task. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] Check the cause of the termination of BGP4 task.

No.	Message text	Description
79	bgp_peer_delete: Peer <bgp name> [(<description>)]: Closed connection by changing configuration	Information (local device) A BGP4 connection was closed due to a change in the configuration (deletion of peer information). [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] None.
80	bgp_init: Peer <bgp name> [(<description>)]: Closed connection by changing configuration	Information (local device) A BGP4 connection was closed due to a change in the configuration. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] None.
81	bgp_peer_clear: Peer <bgp name> [(<description>)]: Closed connection by clearing peer	Information (local device) A BGP4 connection was closed by entering the "clear ip bgp" command. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] None.
82	bgp_pp_recv: Peer <bgp name> in graceful-restart failed to retain stale routes, deleting all the stale routes from the peer	Error (remote device) A peer that executed a graceful restart failed to save the forwarding path. All the paths learned from the relevant peer will be deleted. [Explanation of message variables] <bgp name>: Connection target peer name [Action] Check the unicast routing program (BGP4) in the peer.
83	bgp_recv_open: Peer <bgp name> in graceful-restart failed to retain stale routes, deleting all the stale routes from the peer	Error (remote device) A peer that executed a graceful restart failed to save the forwarding path. All the paths learned from the relevant peer will be deleted. [Explanation of message variables] <bgp name>: Connection target peer name [Action] Check the unicast routing program (BGP4) in the peer.

No.	Message text	Description
84	bgp_restart_timeout: Peer <bgp name> [(<description>)]: Timed out waiting for reconnect.	Error (local or remote device)
		A graceful restart failed. A connection to the peer router could not be established within the restart-time specified by the peer router. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] Check if a communication can be established with the peer router. Check if BGP is running on the peer router. If the peer router is running, increase the restart-time value of the peer router so that the peer router can recover and establish a connection.
85	bgp_restart_timeout: Peer <bgp name> [(<description>)]: Timed out waiting for End-Of-RIB marker from restart router.	Error (remote device)
		A graceful restart failed. End-Of-RIB could not be received from the peer router. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] Check if BGP is running on the relevant peer router. If it is running, increase the stalepath-time value.
86	bgp_peer_established: Peer <bgp name> [(<description>)] connection established with graceful restart.	Information (local or remote device)
		A BGP connection with the relevant peer was re-established. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] None.
87	bgp_receive_End-Of-RIB: End-Of-RIB marker received from <bgp name> [(<description>)].	Information (local device)
		End-Of-RIB was received. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] None.
88	bgp_send_End-Of-RIB: End-Of-RIB marker sent to <bgp name> [(<description>)].	Information (local device)
		End-Of-RIB was sent. [Explanation of message variables] <bgp name>: Target peer name <description>: Description name of the destination peer [Action] None.

No.	Message text	Description
89	BGP: NOTIFICATION sent to <bgp name> [(<description>)]: code <code> (<code string>) [sub-code <subcode> (<subcode string>)] [value <value>] [data <data>]	Warning (remote device) A NOTIFICATION message was sent to the relevant peer. [Explanation of message variables] <bgp name>: Target peer name <description>: Description name of the destination peer <code> (<code string>), <subcode> (<subcode string>): The following error codes and subcodes: 1. Error code 1 (Message Header Error) • Error subcode 1 (lost connection synchronization) • Error subcode 2 (bad length) • Error subcode 3 (bad message type) 2. Error code 2 (Open Message Error) • Error subcode 0 (unspecified error) • Error subcode 1 (unsupported version) • Error subcode 2 (bad AS number) • Error subcode 3 (bad BGP ID) • Error subcode 4 (unsupported optional parameter) • Error subcode 6 (unacceptable holdtime) 3. Error code 3 (Update Message Error) • Error subcode 1 (invalid attribute list) • Error subcode 2 (unknown well known attribute) • Error subcode 3 (missing well known attribute) • Error subcode 4 (attribute flags error) • Error subcode 5 (bad attribute length) • Error subcode 6 (bad ORIGIN attribute) • Error subcode 9 (error with optional attribute) • Error subcode 10 (bad address or prefix field) • Error subcode 11 (AS path attribute problem) 4. Error code 4 (Hold Timer Expired Error) 5. Error code 5 (Finite State Machine Error) 6. Error code 6 (Cease) • If the <code> value is invalid, "invalid" is displayed for <code string>. If the <subcode> value is invalid, "unknown" is displayed for <subcode string>. • Information in the data field of the Notification message is displayed for <value> or <data>. <value>: Decimal representation <data>: Hexadecimal representation [Action] Check the network configuration and peer configuration. If there is no problem with them, check the unicast routing program (BGP4) in the peer.

No.	Message text	Description
90	BGP: NOTIFICATION received from <bgp name> [(<description>)]: code <code> (<code string>) [subcode <subcode> (<subcode string>)] [value <value>] [data <data>]	Warning (local device) A NOTIFICATION message was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <code> (<code string>), <subcode> (<subcode string>): The following error codes and subcodes: 1. Error code 1 (Message Header Error) • Error subcode 1 (lost connection synchronization) • Error subcode 2 (bad length) • Error subcode 3 (bad message type) 2. Error code 2 (Open Message Error) • Error subcode 0 (unspecified error) • Error subcode 1 (unsupported version) • Error subcode 2 (bad AS number) • Error subcode 3 (bad BGP ID) • Error subcode 4 (unsupported optional parameter) • Error subcode 6 (unacceptable holdtime) • Error subcode 7 (unsupported capability) 3. Error code 3 (Update Message Error) • Error subcode 1 (invalid attribute list) • Error subcode 2 (unknown well known attribute) • Error subcode 3 (missing well known attribute) • Error subcode 4 (attribute flags error) • Error subcode 5 (bad attribute length) • Error subcode 6 (bad ORIGIN attribute) • Error subcode 7 (AS loop detected) • Error subcode 8 (invalid NEXT_HOP) • Error subcode 9 (error with optional attribute) • Error subcode 10 (bad address or prefix field) • Error subcode 11 (AS path attribute problem) 4. Error code 4 (Hold Timer Expired Error) 5. Error code 5 (Finite State Machine Error) 6. Error code 6 (Cease) • If the <code> value is invalid, "invalid" is displayed for <code string>. If the <subcode> value is invalid, "unknown" is displayed for <subcode string>. • Information in the data field of the Notification message is displayed for <value> or <data>.

No.	Message text	Description
		<value>: Decimal representation <data>: Hexadecimal representation [Action] Check the network configuration and the configuration.
91	BGP: No MD5 digest from <source ipv4>+<port no.> to <destination ipv4>+<port no.> [VRF <vrf id>]	Warning (remote device) The MD5 authentication option is not set for the TCP segment received by BGP4 connection. This operation message is output according to the following conditions: 1. The messages from the first to the 16th event are output. 2. After 17 times from the beginning of the event occurrence, this message is output once every 256 times the event occurs. 3. If an event occurs 3 minutes or more after the last event occurred, this message is output depending on 1 and 2 above. Note that the above number of messages include the count of "BGP: Invalid MD5 digest from <source ipv4> + <port no.> to <destination ipv4> + <port no.>". [Explanation of message variables] <source ipv4>: Source IPv4 address <port no.>: TCP port number <destination ipv4>: Destination IPv4 address <vrf id>: VRF ID [Action] Check whether the MD5 authentication is set in BGP4 of the remote device. If it is not set, set the MD5 authentication so that it matches. If the setting matches, check whether TCP segments are sent from a peer other than the source BGP4 peer.
92	BGP: Invalid MD5 digest from <source ipv4>+<port no.> to <destination ipv4>+<port no.> [VRF <vrf id>]	Warning (local device or remote device) The MD5 authentication option for TCP segments received by BGP4 connection is invalid. This operation message is output according to the following conditions: 1. The messages from the first to the 16th event are output. 2. After 17 times from the beginning of the event occurrence, this message is output once every 256 times the event occurs. 3. If an event occurs 3 minutes or more after the last event occurred, this message is output depending on 1 and 2 above. Note that the above number of messages includes the count of "BGP: No MD5 digest from <source ipv4> + <port no.> to <destination ipv4> + <port no.>". [Explanation of message variables] <source ipv4>: Source IPv4 address <port no.>: TCP port number <destination ipv4>: Destination IPv4 address

No.	Message text	Description
		<vrf id>: VRF ID [Action] Check if the MD5 authentication keys match in BGP4 of the local and remote devices. If the MD5 authentication keys do not match, set them so that they do match. If the MD5 authentication keys match, check if TCP segments are sent from a peer other than the source BGP4 peer.
93	BGP: Number of prefix received from <bgp name> [(<description>)]: reached <routes1>, limit <routes2>	Warning (remote device)
		The number of paths (active routes and inactive routes) learned from the relevant peer exceeded the threshold. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <routes1>: Number of paths learned from peers <routes2>: Maximum number of paths learned from peers [Action] If the number of paths learned from the peer further increases, check the number of the paths advertised by the peer.
94	BGP: Number of prefix received from <bgp name> [(<description>)]: <routes1> exceed limit <routes2>	Warning (remote device)
		The number of paths (active routes and inactive routes) learned from the relevant peer exceeded the maximum value. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <routes1>: Number of paths learned from peers <routes2>: Maximum number of paths learned from peers [Action] Check the number of the paths advertised by the relevant peer.
95	BGP: Peer <bgp name> [(<description>)]: Closed connection by maximum-prefix	Information (remote device)
		BGP4 connection was closed due to the limitation of the number of learned paths. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] Check the number of the paths advertised by the relevant peer. To reconnect the peer, make sure that the number of paths advertised by the peer is equal to or less than the maximum value, and then enter the "clear ip bgp" command.
96	BGP: Peer <bgp name> [(<description>)] UPDATE included attribute type code (0) [- AS Path (<as number>): <as-path>]	Warning (remote device)
		An UPDATE message including the path attribute of type code 0 was received from the relevant peer.

No.	Message text	Description
		This operation message is not output again on the same peer for an hour after the previous output. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <as number>: Number of AS numbers <aspath>: AS paths, in the following format: • AS sequential number: AS_SEQ • {AS sequential number}: AS_SET • (AS sequential number): AS_CONFED_SEQUENCE Note that, the entire AS path might not be output because there is a limit to the number of characters that can be output in an operation message. [Action] Check the unicast routing program (BGP4) in the peer.
97	bgp_pp_recv: Peer <bgp name> as receiving-speaker failed to retain stale routes, the packets forwarded to the peer may be discarded.	Warning (remote device)
		A peer acting as a receiving router failed to save the forwarding path. Packets forwarded to the target peers may be discarded. [Explanation of message variables] <bgp name>: Connection target peer name [Action] During the graceful restart negotiation, non-forwardable state was notified. Investigate whether a failure has occurred on the peer router.
98	BGP: Completed the learning from receiving-speakers	Information (local device)
		Route learning from the receiving router has been completed. [Explanation of message variables] None. [Action] None.
99	BGP: Start advertisement, giving up learning from several receiving-speakers	Information (local device)
		Interrupt the route learning from some receiving routers and start the route advertisement. [Explanation of message variables] None. [Action] None.
100	bgp_recv_open: Peer <bgp name> as receiving-speaker failed to retain stale routes, the packets forwarded to the peer may be discarded.	Warning (remote device)

No.	Message text	Description
		A peer acting as a receiving router failed to save the forwarding path. Packets forwarded to the target peers may be discarded. [Explanation of message variables] <bgp name>: Connection target peer name [Action] During the graceful restart negotiation, non-forwardable state was notified. Investigate whether a failure has occurred on the peer router.
101	BGP: A peer connection closed because of a BFD state change. (peer = <bgp name>[(<description>)])	Information (local device)
		The target peer connection was disconnected due to a change in the BFD session status. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] Investigate the BFD session status.

3.2.4 Common to IPv4 unicast routing protocols

The following table describes the event information common to IPv4 unicast routing protocols (RTM).

Table 3-5: Event information common to IPv4 unicast routing protocols

No.	Message text	Description
1	*** Give up gdump. Because of no enough memory.	Warning (local device)
		Dump collection was stopped because the remaining memory capacity of the system temporarily fell below the preset value while unicast routing program control information dumps were being collected by the "dump protocols unicast" command. [Explanation of message variables] None. [Action] There is not enough memory to execute the command. Review the capacity limit.
2	The number of IPv4 unicast routes on global network exceeded the limit.	Warning (local device)
		The number of IPv4 unicast routes on the global network has exceeded the maximum. [Explanation of message variables] None. [Action] 1. Delete unnecessary routes. 2. Review the maximum number of routes that was specified in the configuration.

No.	Message text	Description
3	The number of IPv4 unicast routes on VRF <vrf id> exceeded the limit.	Warning (local device)
		The number of IPv4 unicast routes on VRF <vrf id> has exceeded the maximum. [Explanation of message variables] <vrf id>: VRF ID [Action] 1. Delete unnecessary routes. 2. Review the maximum number of routes that was specified in the configuration.
4	The number of IPv4 unicast routes on global network exceeded the warning threshold.	Information (local device)
		The number of IPv4 unicast routes on the global network has exceeded the warning threshold value. [Explanation of message variables] None. [Action] When adding routes, make sure that the number of added routes does not exceed the maximum.
5	The number of IPv4 unicast routes on VRF <vrf id> exceeded the warning threshold.	Information (local device)
		The number of IPv4 unicast routes on VRF <vrf id> has exceeded the warning threshold value. [Explanation of message variables] <vrf id>: VRF ID [Action] When adding routes, make sure that the number of added routes does not exceed the maximum.
6	Rtm: Graceful Restart terminated because this system failed to retain the routes.	Warning (local device)
		Graceful restart failed because the route could not be retained. [Explanation of message variables] None. [Action] Investigate whether the unicast routing program restarts during the graceful restart.

3.3 IPv6 routing protocol information (RTM)

This section explains IPv6 routing protocol event information.

3.3.1 RIPng

The following table gives the event information for IPv6 routing protocol information (RTM).

Table 3-6: IPv6 routing protocol (RIPng) event information

No.	Message text	Description
1	ripng_recv: Bad metric(<metric>) for net <prefix> from <source address>	Error (remote device)
		Route information that has an invalid metric value (0, or 17 or larger) was received. [Explanation of message variables] <metric>: Metric value of the route information <prefix>: Route information destination prefix <source address>: Source gateway address [Action] Check the unicast routing program (RIPng) for the source gateway.
2	ripng_recv: Bad prefixlen(<pefixlen>) for net <prefix> from <source address>	Error (remote device)
		Route information that has an invalid prefix length was received. [Explanation of message variables] <pefixlen>: Prefix length of the route information <prefix>: Route information destination <source address>: Source gateway address [Action] Check the unicast routing program (RIPng) for the source gateway.
3	ripng_recv: Ignoring RIPng <ripng command> packet from <source address> - ignoring invalid version packet	Error (remote device)
		A received RIPng packet was ignored because the version field was invalid. [Explanation of message variables] <ripng command>: Received message type • Request, Response <source address>: Source gateway address [Action] Check the unicast routing program (RIPng) for the source gateway.
4	ripng_recv: Packet hoplimit is <hop limit> hop limit must be 255	Error (remote device)
		A received RIPng packet was ignored because the hop limit was invalid. [Explanation of message variables] <hop limit>: Received hop limit [Action] Check the unicast routing program (RIPng) for the source gateway.

No.	Message text	Description
5	ripng_init: Old copy of rtm is running	Error (local device)
		Unicast routing program might already be running. The unicast routing program automatically restarts. [Explanation of message variables] None. [Action] Take appropriate action by following the rtm aborted log.
6	ripng_recv: Ignoring RIPng <ripng command> from <source address> - source address is not link-local	Error (remote device)
		A received RIPng packet was ignored because the source address was not a link-local address. [Explanation of message variables] <ripng command>: Received message type <source address>: Source gateway [Action] Check the unicast routing program (RIPng) for the source gateway.
7	ripng_recv: Ignoring RIPng <ripng command> from <source address> - source port is not valid	Error (remote device)
		A received RIPng packet was ignored because the source port was invalid. [Explanation of message variables] <ripng command>: Received message type <source address>: Source gateway [Action] Check the unicast routing program (RIPng) for the source gateway.
8	ripng_recv: Ignoring RIPng <ripng command> packet from <source address> - invalid or not implemented command	Error (remote device)
		A received packet was ignored because the command was invalid or not implemented. [Explanation of message variables] <ripng command>: Received message type <source address>: Source gateway [Action] Check the unicast routing program (RIPng) for the source gateway.
9	ripng_recv: Ignoring RIPng packet from <source address> - too short packet (<size>)	Error (remote device)
		A received packet was ignored because the packet length was shorter than the RIPng header. [Explanation of message variables] <source address>: Source gateway <size>: Packet length [Action] Check the unicast routing program (RIPng) for the source gateway.

No.	Message text	Description
10	ripng_recv: Ignoring RIPng request packet from <source address> - the routing entries of improper length	Error (remote device)
		A received request packet was ignored because route information of invalid length was included. [Explanation of message variables] <source address>: Source gateway [Action] Check the unicast routing program (RIPng) for the source gateway.
11	ripng_recv: Ignoring a routing entry of improper length - packet from <source address>	Error (remote device)
		Route information of invalid length was ignored. [Explanation of message variables] <source address>: Source gateway [Action] Check the unicast routing program (RIPng) for the source gateway.
12	RIPng: The total number of RIPng targets is more than the maximum permitted	Error (local device)
		The total number of RIPng targets (neighboring) exceeds the maximum number permitted. [Explanation of message variables] None. [Action] Check, and if necessary, revise the RIPng settings so that the maximum number of neighboring routers does not exceed the capacity limit.

3.3.2 OSPFv3 [SL-L3A]

The following table gives the event information for IPv6 routing protocol information (RTM).

Table 3-7: IPv6 routing protocol (OSPFv3) event information

No.	Message text	Description
1	OSPFv3 SENT <source address> (<interface name>) -> <destination address>: <error string>.	Warning (local device)
		An attempt to send an OSPFv3 packet failed. [Explanation of message variables] <source address>: Source IPv6 address <interface name>: Interface name <destination address>: Destination IPv6 address <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.

No.	Message text	Description
2	OSPFv3: Helper to adjacency <router id> [(VRF <vrf id>)] failed because network topology is changed.	Warning (local device or network)
		The helper router behavior stopped because the topology was changed. [Explanation of message variables] <router id>: Neighboring router's router ID <vrf id>: VRF ID [Action] None.
3	OSPFv3: Helper to adjacency <router id> [(VRF <vrf id>)] failed because restart time is up.	Information (remote device)
		The helper router behavior stopped because the waiting time for restart elapsed. [Explanation of message variables] <router id>: Neighboring router's router ID <vrf id>: VRF ID [Action] Check if the neighboring router has stopped the restart. If it has not stopped, adjust the restart time of the neighboring router.
4	OSPFv3 RECV [Area <area id>] RouterID <source id> [(<interface name>)] -> <destination address>: <log type>.	Warning (local device or remote device)
		A received OSPFv3 packet was invalid. However, multicast packets received from broadcast-type interfaces that have not been set as OSPFv3 interfaces are discarded without log acquisition. [Explanation of message variables] <area id>: Area ID <source id>: Source router ID <interface name>: Interface name <destination address>: Destination IPv6 address <log type>: One of the following log types: • IP: received my own packet • bad packet type • bad version • bad checksum • packet too small • packet size > ip length • unknown neighbor • area mismatch • bad virtual link • interface down • HELLO: hello timer mismatch • HELLO: dead timer mismatch • HELLO: extern option mismatch

No.	Message text	Description
		• DD: extern option mismatch • HELLO: router id confusion • DD: router id confusion • DD: MTU mismatch • LS ACK: Unknown LSA type • LS REQ: empty request • LS REQ: bad request • LS UPD: LSA checksum bad • LS UPD: Unknown LSA type [Action] The action to be taken depends on the type of the log. • IP: received my own packet • bad packet type • bad version • bad checksum • packet too small • packet size > ip length A neighboring router is sending an invalid packet. Check the unicast routing program (OSPFv3) of the neighboring router. • unknown neighbor Non-Hello packets were received from the neighboring router that is not recognized by Hello, but no action is required. • area mismatch • bad virtual link If packets are received from the new neighboring router, modify the area settings. In other cases, no action is required. • interface down None. • HELLO: hello timer mismatch • HELLO: dead timer mismatch Modify the OSPFv3 interface settings. • HELLO: extern option mismatch • DD: extern option mismatch Modify the stub area settings. • HELLO: router id confusion • DD: router id confusion Modify the router ID settings. • DD: MTU mismatch An attempt to exchange route information might fail because the MTU length does not match the neighboring router. Match the MTU length. • LS ACK: Unknown LSA type • LS REQ: empty request • LS REQ: bad request • LS UPD: LSA checksum bad • LS UPD: Unknown LSA type A neighboring router is sending an invalid packet. Check the unicast routing program (OSPFv3) of the neighboring router.

No.	Message text	Description
5	OSPFv3: Conflict between LSDB <lsid> and route <prefix> /<prefixlen> - Export to OSPFASE Bypassed.	Error (local device) There is a conflict between LSDB <lsid> and the route. The unicast routing program automatically restarts. [Explanation of message variables] <lsid>: LSID of LSA <prefix>: Route information destination address <prefixlen >: Prefix length of the route information [Action] Take appropriate action by following the rtm aborted log.
6	OSPFv3: Lost adjacency <router id> with interfaceID <id> (<interface name>) because no Hello received recently.	Warning (remote device or network) Adjacency was terminated because Hello packets that should be sent periodically from the neighboring router were not received during a given interval. This occurs when the neighboring router is deactivated, or if a problem occurs in communication between the Switch and the neighboring router. [Explanation of message variables] <router id>: Neighboring router's router ID <id>: ID of the interface of the neighboring router <interface name>: Interface name [Action] If this warning occurs frequently, shorten the interval for sending Hello packets (hellointerval) or extend the maximum interval for receiving Hello packets (routerdeadinterval).
7	OSPFv3: Lost adjacency <router id> with interfaceID <id> (<interface name>) because neighbor didn't receive my Hello recently.	Warning (remote device or network) Adjacency was terminated because the neighboring router no longer recognizes the Switch. This occurs when the neighboring router is restarted or Hello packets sent by the Switch are not properly received by the neighboring router. [Explanation of message variables] <router id>: Neighboring router's router ID <id>: ID of the interface of the neighboring router <interface name>: Interface name [Action] If this warning occurs frequently, extend the interval for sending Hello packets (hellointerval) and the maximum interval for receiving Hello packets (routerdeadinterval).
8	OSPFv3: Lost adjacency <router id1> with interfaceID <id> (<interface name>) due to bad LS Request (<lsid> <router id2> <ls type>).	Error (remote device) The neighboring router was lost due to an invalid LS request. [Explanation of message variables] <router id1>: Neighboring router's router ID <id>: ID of the interface of the neighboring router

No.	Message text	Description
		<interface name>: Interface name <lsid>: LSID of LSA <router id2>: LSA advertising router ID <ls type>: LSA LS type code [Action] Check the unicast routing program (OSPFv3) of the neighboring router.
9	OSPFv3: Lost adjacency <router id> with interfaceID <id> (<interface name>) due to sequence mismatch (<sequence1> versus <sequence2>).	Warning (local device or remote device)
		A neighboring router was lost due to a sequence (or option) mismatch. [Explanation of message variables] <router id>: Neighboring router's router ID <id>: ID of the interface of the neighboring router <interface name>: Interface name <sequence1>: Sequence number in control data <sequence2>: Sequence number in the DD message [Action] If this warning occurs frequently, extend the interval for retransmitting OSPFv3 packets (retransmitinterval).
10	OSPFv3: Adjacency <router id> interface <interface name> is established.	Information (local or remote device)
		A connection with the OSPFv3 neighboring router was successfully established. [Explanation of message variables] <router id>: Neighboring router's router ID <interface name>: Interface name [Action] None.
11	OSPFv3: Checksum failed at LSA type <ls type> ID <lsid> adv-router <router id> in this system's LSDB that belongs to Area <area id>, Domain <domain id> [on VRF <vrf id>].	Error (local device)
		LSDB checksum is invalid. The unicast routing program automatically restarts. [Explanation of message variables] <ls type>: LSA LS type code <lsid>: LSID of LSA <router id>: LSA advertising router ID <area id>: LSA area ID <domain id>: LSA domain ID <vrf id>: VRF ID [Action] Take appropriate action by following the rtm aborted log.
12	OSPFv3: Recovered from stub router (in [(VRF <vrf id>)] domain <domain id>).	Information (local device)
		The stub router behavior will now end. [Explanation of message variables] <vrf id>: VRF ID

No.	Message text	Description
		<domain id>: OSPFv3 domain ID [Action] None.
13	OSPFv3: Graceful restart failed (in [(VRF <vrf id>)] domain <domain id>) because adjacency <router id> doesn't help me.	Warning (remote device or network)
		Graceful restart failed because the neighboring router is not working as a helper router. [Explanation of message variables] <vrf id>: VRF ID <domain id>: OSPFv3 domain ID <router id>: Neighboring router's router ID [Action] Check the graceful restart configuration of the neighboring router.
14	OSPFv3: Graceful restart failed (in [(VRF <vrf id>)] domain <domain id>) because adjacency <router id> gives up me.	Warning (remote device or network)
		Graceful restart failed because the neighboring router stopped working as a helper router. [Explanation of message variables] <vrf id>: VRF ID <domain id>: OSPFv3 domain ID <router id>: Neighboring router's router ID [Action] If this error frequently occurs, check the OSPF status of the neighboring router and the cause of the helper function stopping.
15	OSPFv3: Graceful restart failed (in [(VRF <vrf id>)] domain <domain id>) because restart time is up.	Warning (local device)
		Graceful restart failed because the reconnection and LSA synchronization with all neighboring routers connected before restart were not possible within the restart time. [Explanation of message variables] <vrf id>: VRF ID <domain id>: OSPFv3 domain ID [Action] Check the restart time configuration.
16	OSPFv3: Graceful restart finished successfully (in [(VRF <vrf id>)] domain <domain id>).	Information (local device)
		Graceful restart was successful. [Explanation of message variables] <vrf id>: VRF ID <domain id>: OSPFv3 domain ID [Action] None.

3.3.3 BGP4+ [SL-L3A]

The following table gives the event information for IPv6 routing protocol information (RTM).

Table 3-8: IPv6 routing protocol (BGP4+) event information

No.	Message text	Description
1	bgp4+_check_auth: Synchronization failure with BGP task <task name>	Error (remote device)
		The value of the header marker of the message received by BGP4+ task is invalid. [Explanation of message variables] <task name>: BGP4+ task name [Action] Check the unicast routing program (BGP4+) in the peer.
2	bgp4+_trace: Unsupported BGP version <version>!!!	Error (local device)
		The BGP version number in control data was invalid. The unicast routing program automatically restarts. [Explanation of message variables] <version>: BGP version number in control data [Action] Take appropriate action by following the rtm aborted log.
3	bgp4+_log_notify: Notify message received from <bgp name> [(<description>)] is truncated (length <length>)	Error (remote device)
		The length of the NOTIFICATION message received from the relevant peer was invalid. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received data length [Action] Check the unicast routing program (BGP4+) in the peer.
4	bgp4+_send: Sending <length> bytes to <bgp name> [(<description>)] blocked (no spooling requested): <error string>	Warning (local device)
		An attempt to send a message to the relevant peer failed because the socket buffer became full. [Explanation of message variables] <length>: Send request message length <bgp name>: Target peer name <description>: Description name of the destination peer <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
5	bgp4+_send: Sending <length> bytes to <bgp name> [(<description>)] failed: <error string>	Warning (local device)
		An attempt to send a message to the relevant peer has failed. [Explanation of message variables] <length>: Send request message length <bgp name>: Target peer name <description>: Description name of the destination peer <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.

No.	Message text	Description
6	bgp4+_send: Sending <length> bytes to <bgp name> [(<description>)]: Connection closed	Warning (local device, remote device, or network) Sending of the message to the peer failed because the connection was disconnected. [Explanation of message variables] <length>: Send request message length <bgp name>: Target peer name <description>: Description name of the destination peer [Action] If this error occurs frequently, check the cause of the disconnection.
7	bgp4+_send: Sending to <bgp name> [(<description>)] looping: <error string>	Warning (local device) An attempt to send a message to the relevant peer has timed out. [Explanation of message variables] <bgp name>: Target peer name <description>: Description name of the destination peer <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
8	bgp4+_send_open: Internal error! peer <bgp name> [(<description>)], version <version>	Error (local device) The BGP version number of the OPEN message to be sent to the relevant peer was invalid. The unicast routing program automatically restarts. [Explanation of message variables] <bgp name>: Target peer name <description>: Description name of the destination peer <version>: BGP version number in the send message [Action] Take appropriate action by following the rtm aborted log.
9	bgp4+_path_attr_error from <routine>: Update error subcode <code> (<error string>) for peer <bgp name> [(<description>)] detected. <length> bytes error data - 1st five: <error data>	Error (remote device) An error was detected in the UPDATE message received from the relevant peer. [Explanation of message variables] <routine>: Internal routine name <code> (<error string>): Error cause <bgp name>: Source peer name <description>: Description name of the source peer <length>: Error data length <error data>: First five bytes of error data [Action] Check the unicast routing program (BGP4+) in the peer.

No.	Message text	Description
10	bgp4+_recv: Read from peer <bgp name> [(<description>)] failed: <error string>	Warning (local device)
		An attempt to receive a message from the relevant peer failed. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
11	bgp4+_recv: Peer <bgp name> [(<description>)]: Received unexpected EOF	Warning (local device, remote device, or network)
		An attempt to receive a message from the relevant peer failed due to disconnection. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] If this error occurs frequently, check the cause of the disconnection.
12	bgp4+_read_message: Peer <bgp name> [(<description>)]: <message type> message arrived with length <length>	Error (remote device)
		An invalid-length message was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <message type>: Received message type • invalid, Open, Update, Notification, KeepAlive <length>: Received data length [Action] Check the unicast routing program (BGP4+) in the peer.
13	bgp4+_read_message: Peer <bgp name> [(<description>)]: <message type1> arrived, expected <message type2> [or <message type2>]	Error (remote device)
		A message whose message type is inappropriate for the current state was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <message type1>: Received message type • invalid, Open, Update, Notification, KeepAlive <message type2>: Message type appropriate for the current state • invalid, Open, Update, Notification, KeepAlive [Action] Check the unicast routing program (BGP4+) in the peer.
14	bgp4+_get_open:	Error (remote device)

No.	Message text	Description
	Peer <bgp name> [(<description>)]: Received short version <version> message (<length> octets)	An invalid-length OPEN message was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <version>: BGP version number in the received message <length>: Received data length [Action] Check the unicast routing program (BGP4+) in the peer.
15	bgp4+_get_open: Received unsupported version <version> message from peer <bgp name> [(<description>)]	Warning (remote device)
		An OPEN message that has an unsupported BGP version was received from a peer. [Explanation of message variables] <version>: BGP version number of received messages <bgp name>: Source peer name <description>: Description name of the source peer [Action] Make sure that the peer supports BGP version 4.
16	bgp4+_get_open: Peer <bgp name> [(<description>)]: Hold time too small (<hold time>)	Error (remote device)
		An OPEN message whose hold time is less than three seconds was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <hold time>: Hold time in the received message [Action] Check the peer configuration.
17	bgp4+_get_open: Peer <bgp name> [(<description>)]: Invalid BGP4+ identifier <router id>	Error (remote device)
		An OPEN message that has an invalid BGP4+ identifier was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <router id>: BGP4+ identifier in the received message [Action] Check the unicast routing program (BGP4+) in the peer.
18	bgp4+_get_open: Peer <bgp name> [(<description>)]: Unsupported optional parameter <option>	Error (remote device)
		An OPEN message that contains an invalid option code was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer

No.	Message text	Description
		<option>: Option code in the received message [Action] Check the unicast routing program (BGP4+) in the peer.
19	bgp4+_recv_open: Peer <bgp name> [(<description>)] claims AS <as1>, <as2> configured	Warning (local device or remote device)
		An OPEN message that has a different AS number than the configured AS number was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <as1>: AS number of the received message <as2>: AS number of the peer in the configuration [Action] Check the configuration.
20	bgp4+_recv_open: Peer <bgp name> [(<description>)] accepted mismatched versions: Peer <version1> this system <version2>	Warning (remote device)
		A KEEPALIVE message that has a mismatched BGP version number was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <version1>: Remote BGP version number <version2>: Local BGP version number [Action] Make sure that the peer supports BGP4+.
21	bgp4+_pp_recv: No group for <bgpp name> found, dropping peer	Warning (local device or remote device)
		An OPEN message was received from a peer that was not set. [Explanation of message variables] <bgpp name>: Source peer name [Action] Check the configuration.
22	bgp4+_pp_recv: Rejecting connection from <bgp name> [(<description>)], peer in state <state>	Warning (remote device or network)
		An OPEN message was received from the relevant peer during the Idle, OpenConfirm, or Established status. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <state>: Peer status • Idle, OpenConfirm, Established [Action] The connection has become unstable. If this error occurs frequently, check the cause of the instability.

No.	Message text	Description
23	bgp4+_pp_recv: Dropping <bgpp name> version <version>, <bgp name> [(<description>)] wants version 4	Warning (remote device)
		An OPEN message that has an unsupported BGP version was received from a peer. [Explanation of message variables] <bgpp name>, <bgp name>: Source peer name <version>: BGP version number of received messages <description>: Description name of the source peer [Action] Check the BGP version supported by the peer.
24	bgp4+_pp_recv: Peer <bgp name> [(<description>)] sent unexpected extra data, probably insane	Error (remote device)
		Unnecessary data is appended to the message from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.
25	bgp4+_check_capability_match: Capability of peer <bgp name> [(<description>)] is unmatched	Warning (remote device)
		The capability settings specified for the Switch are not specified for the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] Check the configuration.
26	bgp4+_write_flush: Sending <length1> (sent <length2>) bytes to <bgp name> [(<description>)] failed: <error string>	Warning (local device)
		An attempt to send a message to the relevant peer has failed. [Explanation of message variables] <length1>: Send request data length <length2>: Sent data length <bgp name>: Target peer name <description>: Description name of the destination peer <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
27	bgp4+_write_flush: Sending <length1> (sent <length2>) bytes to <bgp name> [(<description>)]: Connection closed	Warning (local device, remote device, or network)
		Sending of the message to the peer failed because the connection was disconnected. [Explanation of message variables] <length1>: Send request data length <length2>: Sent data length

No.	Message text	Description
		<bgp name>: Target peer name <description>: Description name of the destination peer [Action] If this error occurs frequently, check the cause of the disconnection.
28	bgp4+_write_flush: Sending to <bgp name> [(<description>)] (sent <length1>, <length2> remain[s]) looping: <error string>	Warning (local device)
		An attempt to send a message to the relevant peer has timed out. [Explanation of message variables] <bgp name>: Target peer name <description>: Description name of the destination peer <length1>: Sent data length <length2>: Length of the data that remains unsent <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
29	bgp4+_peer_connected: task_get_addr_local(<bgp name> [(<description>)]): <error string>	Warning (local device)
		Extraction of the local address used for establishing a connection to the relevant peer failed. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
30	bgp4+_connect_start: Peer <bgp name> [(<description>)] local address <ipv6 address> unavailable, connection failed	Warning (local device)
		An attempt to establish a connection failed because the local address used for establishing a connection to the relevant peer could not be used (bind failure). [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer <ipv6 address>: Local address used for peering [Action] If this error frequently occurs, determine the cause of the error.
31	bgp4+_traffic_timeout: Holdtime expired for <bgp name> [(<description>)]	Warning (remote device or network)
		A hold timeout for the relevant peer occurred. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] Check the unicast routing program (BGP4+) in the peer.
32	bgp4+_traffic_timeout:	Warning (local device)

No.	Message text	Description
	Error sending KEEPALIVE to <bgp name> [(<description>)]: <error string>	An attempt to send a KEEPALIVE message to the relevant peer failed. [Explanation of message variables] <bgp name>: Target peer name <description>: Description name of the destination peer <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
33	bgp4+_listen_accept: accept(<socket>): <error string>	Warning (local device)
		An attempt to accept the connection failed. [Explanation of message variables] <socket>: Socket descriptor number <error string>: Error cause [Action] If this error frequently occurs, determine the cause of the error.
34	bgp4+_listen_accept: bgp4+_get_peer_if() failed, terminating!!	Error (local device)
		Extraction of the link-local address used for establishing a connection failed. The connection will be closed. [Explanation of message variables] None. [Action] If this error frequently occurs, check the unicast routing program (BGP4+) in the peer.
35	bgp4+_listen_accept: task_get_addr_local() failed, terminating!!	Error (local device)
		Extraction of the local address used for establishing a connection failed. The connection will be closed. [Explanation of message variables] None. [Action] If this error frequently occurs, check the unicast routing program (BGP4+) in the peer.
36	bgp4+_listen_start: Couldn't get BGP listen socket!!	Error (local device)
		An attempt to create a socket for establishing a connection failed. The unicast routing program automatically restarts. [Explanation of message variables] None. [Action] Take appropriate action by following the rtm aborted log.
37	bgp4+_listen_start: listen: <error string>	Error (local device)
		Preparation for accepting a connection failed. The unicast routing program automatically restarts. [Explanation of message variables]

No.	Message text	Description
		<error string>: Error cause [Action] Take appropriate action by following the rtm aborted log.
38	bgp4+_set_peer_if: BGP peer <bgp name> [(<description>)] interface not found. Leaving peer idled	Warning (local device) The interface connected to the relevant peer was not found. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] Check the configuration.
39	bgp4+_set_peer_if: BGP peer <bgp name> [(<description>)] local address <ipv6 address> not on shared net. Leaving peer idled	Warning (local device) The local address used for establishing a connection to the relevant peer is not in the same network. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer <ipv6 address>: Local address used for establishing a connection [Action] Check the configuration.
40	bgp4+_pp_timeout: Peer <bgpp name> timed out waiting for OPEN	Warning (remote device or network) The timer for waiting for an OPEN message from the relevant peer timed out. [Explanation of message variables] <bgpp name>: Connection target peer name [Action] Check the unicast routing program (BGP4+) in the peer.
41	bgp4+_peer_init: BGP peer <bgp name> [(<description>)] local address <ipv6 address> not found. Leaving peer idled	Warning (local device) The interface for the local address used for establishing a connection to the relevant peer is not found. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer <ipv6 address>: Local address used for establishing a connection [Action] Check the configuration.
42	bgp4+_recv_update: Peer <bgp name> [(<description>)]: Strange message header length <length>	Error (remote device) The message length in the message header of a message received from the relevant peer is invalid. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer

No.	Message text	Description
		<length>: Message length of the received message header [Action] Check the unicast routing program (BGP4+) in the peer.
43	bgp4+_recv_update: Peer <bgp name> [(<description>)] unrecognized message type <type>	Error (remote device)
		The message type of the UPDATE message received from the relevant peer is invalid. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <type>: Message type [Action] Check the unicast routing program (BGP4+) in the peer.
44	bgp4+_recv _update: Received OPEN message from <bgp name> [(<description>)], state is ESTABLISHED	Warning (remote device or network)
		An OPEN message was received from the relevant peer in the ESTABLISHED status. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] The connection has become unstable. If this error occurs frequently, check the cause of the instability.
45	bgp4+_recv _update: Peer <bgp name> [(<description>)] UPDATE length <length> too small	Error (remote device)
		The length of the UPDATE message from the relevant peer is too short. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received data length [Action] Check the unicast routing program (BGP4+) in the peer.
46	bgp4+_recv_update: Peer <bgp name> [(<description>)] UPDATE unreachable prefix length <length1> exceeds packet length <length2>	Error (remote device)
		The prefix length of unreachable route information of the UPDATE message from the relevant peer exceeds the packet length. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length1>: Prefix length of unreachable route information in the received message <length2>: Received packet length [Action] Check the unicast routing program (BGP4+) in the peer.

No.	Message text	Description
47	bgp4+_recv_update: Peer <bgp name> [(<description>)] UPDATE unreachable prefix length <length> too long	Error (remote device) The prefix length of unreachable route information of the UPDATE message from the relevant peer exceeds 128 bits. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Prefix length in received messages [Action] Check the unicast routing program (BGP4+) in the peer.
48	bgp4+_recv_update: Peer <bgp name> [(<description>)] UPDATE prefix length <length1> exceeds unreachable prefix data remaining (<length2> bytes)	Error (remote device) The prefix length of unreachable route information of the UPDATE message received from the relevant peer exceeds the prefix data of unreachable route information. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length1>: Prefix length in received messages <length2>: Actual data length [Action] Check the unicast routing program (BGP4+) in the peer.
49	bgp4+_recv_update: Peer <bgp name> [(<description>)] UPDATE zero attribute length followed by <length> bytes of garbage	Error (remote device) The attribute length of the UPDATE message from the relevant peer is 0 even though actual data exists. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Actual data length [Action] Check the unicast routing program (BGP4+) in the peer.
50	bgp4+_recv_update: Peer <bgp name> [(<description>)] UPDATE path attribute length <length1> too large (<length2> bytes remaining)	Error (remote device) The path attribute length of the UPDATE message from the relevant peer is too long compared to the actual path attribute length. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length1>: Path attribute length of the received message <length2>: Actual data length [Action] Check the unicast routing program (BGP4+) in the peer.

No.	Message text	Description
51	bgp4+_recv_update: Peer <bgp name> [(<description>)] UPDATE no next hop found	Error (remote device)
		The next hop attribute is not found in the UPDATE message from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.
52	bgp4+_recv_update: External peer <bgp name> [(<description>)] UPDATE included LOCALPREF attribute	Error (remote device)
		The LOCALPREF attribute is included in the UPDATE message from the relevant external peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.
53	bgp4+_recv_update: Peer <bgp name> [(<description>)] UPDATE no LOCALPREF attribute found	Error (remote device)
		The LOCALPREF attribute is not found in the UPDATE message from the relevant internal peer. [Explanation of message variables] <bgp name>: Source peer number <description>: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.
54	bgp4+_recv_update: Peer <bgp name> [(<description>)] UPDATE has path attributes but no reachable prefixes!	Error (remote device)
		The UPDATE message from the relevant peer has path attributes but does not have the corresponding route information. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.
55	bgp4+_recv_update: Peer <bgp name> [(<description>)] AS <as1> received path with first AS <as2>	Error (remote device)
		The AS path whose next- hop AS number is <as2> was received from the peer whose AS number is <as1>. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <as1>: AS number of the source peer <as2>: Next-hop AS number in the received message [Action] Check the unicast routing program (BGP4+) in the peer.

No.	Message text	Description
56	bgp4+_recv_update: Ignores prefix from peer <bgp name> [(<description>)] in RFC-1771's NLRI field	Warning (remote device)
		Route information in a format that complies with RFC 1771 instead of RFC 2858 was ignored. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] Check the unicast routing program (BGP4+) in the peer.
57	bgp4+_recv_reach: Peer <bgp name> [(<description>)] UPDATE: Invalid length of MP_REACH_NLRI attribute(<length>) : No address family	Error (remote device)
		The length of the MP_REACH_NLRI attribute for the UPDATE message from the peer is invalid. No address family exists. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4+) in the peer.
58	bgp4+_recv_reach: Peer <bgp name> [(<description>)] UPDATE: Invalid length of MP_REACH_NLRI attribute(<length>) : No nexthop length	Error (remote device)
		The length of the MP_REACH_NLRI attribute for the UPDATE message from the peer is invalid. No next hop length exists. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4+) in the peer.
59	bgp4+_recv_reach: Peer <bgp name> [(<description>)] UPDATE: Invalid length of MP_REACH_NLRI attribute(<length>) : No nexthop	Error (remote device)
		The length of the MP_REACH_NLRI attribute for the UPDATE message from the peer is invalid. No next hop exists. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4+) in the peer.
60	bgp4+_recv_reach: Peer <bgp name> [(<description>)] UPDATE: Invalid length of MP_REACH_NLRI attribute(<length>) : No reserved	Error (remote device)
		The length of the MP_REACH_NLRI attribute for the UPDATE message from the peer is invalid. No reserved field exists. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4+) in the peer.

No.	Message text	Description
61	bgp4+_recv_reach: Peer <bgp name> [(<description>)] UPDATE: Invalid length of MP_REACH_NLRI attribute(<length>) : No snpa length	Error (remote device) The length of the MP_REACH_NLRI attribute for the UPDATE message from the peer is invalid. No SNPA length exists. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4+) in the peer.
62	bgp4+_recv_reach: Peer <bgp name> [(<description>)] UPDATE: Invalid length of MP_REACH_NLRI attribute(<length>) : No snpa	Error (remote device) The length of the MP_REACH_NLRI attribute for the UPDATE message from the peer is invalid. No SNPA exists. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4+) in the peer.
63	bgp4+_recv_reach: Peer <bgp name> [(<description>)] UPDATE multi-protocol prefix length <length1> exceeds prefix data remaining (<length2> bytes)	Error (remote device) The prefix length of the route of the UPDATE message from the relevant peer is too long compared to the remaining data. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length1>: Prefix length in received messages <length2>: Actual data length [Action] Check the unicast routing program (BGP4+) in the peer.
64	bgp4+_recv_reach: Peer <bgp name> [(<description>)] UPDATE multi-protocol prefix length <length> too long	Error (remote device) The prefix length of the route of the UPDATE message from the relevant peer exceeds 128 bits. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received data length [Action] Check the unicast routing program (BGP4+) in the peer.

No.	Message text	Description
65	bgp4+_recv_reach: Peer <bgp name> [(<description>)] bad next hop address length <length>	Error (remote device) The next hop address length of the route from the relevant peer is invalid. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Next hop address length [Action] Check the unicast routing program (BGP4+) in the peer.
66	bgp4+_recv_reach: Peer <bgp name> [(<description>)] next hop <ipv6 address> improper, ignoring routes in this update	Error (remote device) The next hop address of the route from the relevant peer is not in the same network. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <ipv6 address>: Next hop address [Action] Check the unicast routing program (BGP4+) in the peer.
67	bgp4+_recv_reach: Peer <bgp name> [(<description>)] unknown family/subfamily <family>/<subfamily>	Error (remote device) Route information other than IPv6 unicast was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <family>: Address family <subfamily>: Sub address family [Action] Check the unicast routing program (BGP4+) in the peer.
68	bgp4+_recv_unreach: Peer <bgp name> [(<description>)] UPDATE: Invalid length of MP_UNREACH_NLRI attribute(<length>) : No address family	Error (remote device) The length of the MP_UNREACH_NLRI attribute for the UPDATE message from the peer is invalid. No address family exists. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Received MP_UNREACH_NLRI attribute length [Action] Check the unicast routing program (BGP4+) in the peer.

No.	Message text	Description
69	bgp4+_recv_unreach: Peer <bgp name> [(<description>)] UPDATE prefix length <length> exceeds unreachable multi-protocol prefix data remaining (<length> bytes)	Error (remote device) The prefix length of unreachable route information of the UPDATE message from the relevant peer exceeds the data length of remaining unreachable route information. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Next hop address length [Action] Check the unicast routing program (BGP4+) in the peer.
70	bgp4+_recv_unreach: Peer <bgp name> [(<description>)] UPDATE unreachable multi-protocol prefix length <length> too long	Error (remote device) The prefix length of unreachable route information of the UPDATE message from the relevant peer exceeds 128 bits. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <length>: Prefix length in received messages [Action] Check the unicast routing program (BGP4+) in the peer.
71	bgp4+_recv_unreach: Peer <bgp name> [(<description>)] unknown family/subfamily <family>/<subfamily>	Error (remote device) Unreachable route information other than IPv6 unicast was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <family>: Address family <subfamily>: Sub address family [Action] Check the unicast routing program (BGP4+) in the peer.
72	bgp4+_peer_established: Peer <bgp name> [(<description>)] connection established	Information (local or remote device) A BGP4+ connection was established with the relevant peer. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] None.
73	bgp4+_ifachange: Peer <bgp name> [(<description>)]: Closed connection by changing interface state	Information (local or remote device) A BGP4+ connection was closed due to a change in the interface state. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] Check the cause of the change in the interface state.

No.	Message text	Description
74	bgp4+_terminate: Peer <bgp name> [(<description>)]: Closed connection by terminating bgp4+	Information (local device) A BGP4+ connection was closed due to the termination of a BGP4+ task. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] Check the cause of the termination of BGP4+ task.
75	bgp4+_peer_delete: Peer <bgp name> [(<description>)]: Closed connection by changing configuration	Information (local device) A BGP4+ connection was closed due to a change in the configuration (deletion of peer information). [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] None.
76	bgp4+_init: Peer <bgp name> [(<description>)]: Closed connection by changing configuration	Information (local device) A BGP4+ connection was closed due to a change in the configuration. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] None.
77	bgp4+_peer_clear: Peer <bgp name> [(<description>)]: Closed connection by clearing peer	Information (local device) A BGP4+ connection was closed by entering the "clear ipv6 bgp" command. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] None.
78	bgp4+_pp_recv: Peer <bgp name> in graceful-restart failed to retain stale routes, deleting all the stale routes from the peer	Error (remote device) A peer that executed a graceful restart failed to save the forwarding path. All the paths learned from the relevant peer will be deleted. [Explanation of message variables] <bgp name>: Connection target peer name [Action] Check the unicast routing program (BGP4+) in the peer.

No.	Message text	Description
79	bgp4+_recv_open: Peer <bgp name> in graceful-restart failed to retain stale routes, deleting all the stale routes from the peer	Error (remote device) A peer that executed a graceful restart failed to save the forwarding path. All the paths learned from the relevant peer will be deleted. [Explanation of message variables] <bgp name>: Connection target peer name [Action] Check the unicast routing program (BGP4+) in the peer.
80	bgp4+_restart_timeout: Peer <bgp name> [(<description>)]: Timed out waiting for reconnect.	Error (local or remote device) A graceful restart failed. A connection to the peer router could not be established within the restart-time specified by the peer router. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] Check if a communication can be established with the peer router. Check if BGP4+ is running on the peer router. If the peer router is running, increase the restart-time value of the peer router so that the peer router can recover and establish a connection.
81	bgp4+_restart_timeout: Peer <bgp name> [(<description>)]: Timed out waiting for End-Of-RIB marker from restart router.	Error (remote device) A graceful restart failed. End-Of-RIB could not be received from the peer router. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] Check if BGP4+ is running on the relevant peer router. If it is running, increase the stalepath-time value.
82	bgp4+_peer_established: Peer <bgp name> [(<description>)] connection established with graceful restart.	Information (local or remote device) A BGP connection with the relevant peer was re-established. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] None.
83	bgp4+_receive_End-Of-RIB: End-Of-RIB marker received from <bgp name> [(<description>)].	Information (local device) End-Of-RIB was received. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer [Action] None.

No.	Message text	Description
84	bgp4+_send_End-Of-RIB: End-Of-RIB marker sent to <bgp name> [(<description>)].	Information (local device) End-Of-RIB was sent. [Explanation of message variables] <bgp name>: Target peer name <description>: Description name of the destination peer [Action] None.
85	BGP4+: NOTIFICATION sent to <bgp name> [(<description>)]: code <code> (<code string>) [subcode <subcode> (<subcode string>)] [value <value>] [data <data>]	Warning (remote device) A NOTIFICATION message was sent to the relevant peer. [Explanation of message variables] <bgp name>: Target peer name <description>: Description name of the destination peer <code> (<code string>), <subcode> (<subcode string>): The following error codes and subcodes: 1. Error code 1 (Message Header Error) • Error subcode 1 (lost connection synchronization) • Error subcode 2 (bad length) • Error subcode 3 (bad message type) 2. Error code 2 (Open Message Error) • Error subcode 0 (unspecified error) • Error subcode 1 (unsupported version) • Error subcode 2 (bad AS number) • Error subcode 3 (bad BGP ID) • Error subcode 4 (unsupported optional parameter) • Error subcode 6 (unacceptable holdtime) 3. Error code 3 (Update Message Error) • Error subcode 1 (invalid attribute list) • Error subcode 2 (unknown well known attribute) • Error subcode 3 (missing well known attribute) • Error subcode 4 (attribute flags error) • Error subcode 5 (bad attribute length) • Error subcode 6 (bad ORIGIN attribute) • Error subcode 9 (error with optional attribute) • Error subcode 10 (bad address or prefix field) • Error subcode 11 (AS path attribute problem) 4. Error code 4 (Hold Timer Expired Error) 5. Error code 5 (Finite State Machine Error) 6. Error code 6 (Cease) • If the <code> value is invalid, "invalid" is displayed for <code string>. If the <subcode> value is invalid, "unknown" is displayed for <subcode string>. • Information in the data field of the Notification message is displayed for <value> or <data>.

No.	Message text	Description
		<value>: Decimal representation <data>: Hexadecimal representation [Action] Check the network configuration and peer configuration. If there is no problem with them check the unicast routing program (BGP4+) in the peer.
86	BGP4+: NOTIFICATION received from <bgp name> [(<description>)]: code <code> (<code string>) [subcode <subcode> (<subcode string>)] [value <value>] [data <data>]	Warning (local device)
		A NOTIFICATION message was received from the relevant peer. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <code> (<code string>), <subcode> (<subcode string>): The following error codes and subcodes: 1. Error code 1 (Message Header Error) • Error subcode 1 (lost connection synchronization) • Error subcode 2 (bad length) • Error subcode 3 (bad message type) 2. Error code 2 (Open Message Error) • Error subcode 0 (unspecified error) • Error subcode 1 (unsupported version) • Error subcode 2 (bad AS number) • Error subcode 3 (bad BGP ID) • Error subcode 4 (unsupported optional parameter) • Error subcode 6 (unacceptable holdtime) • Error subcode 7 (unsupported capability) 3. Error code 3 (Update Message Error) • Error subcode 1 (invalid attribute list) • Error subcode 2 (unknown well known attribute) • Error subcode 3 (missing well known attribute) • Error subcode 4 (attribute flags error) • Error subcode 5 (bad attribute length) • Error subcode 6 (bad ORIGIN attribute) • Error subcode 7 (AS loop detected) • Error subcode 8 (invalid NEXT_HOP) • Error subcode 9 (error with optional attribute) • Error subcode 10 (bad address or prefix field) • Error subcode 11 (AS path attribute problem) 4. Error code 4 (Hold Timer Expired Error) 5. Error code 5 (Finite State Machine Error) 6. Error code 6 (Cease) • If the <code> value is invalid, "invalid" is displayed for <code string>. If the <subcode> value is invalid, "unknown" is displayed for <subcode string>. • Information in the data field of the Notification message is displayed for <value> or <data>.

No.	Message text	Description
		<value>: Decimal representation <data>: Hexadecimal representation [Action] Check the network configuration and the configuration.
87	BGP4+: No MD5 digest from <source ipv6>+<port no.> to <destination ipv6>+<port no.> [VRF <vrf id>]	Warning (remote device) The MD5 authentication option is not set for the TCP segment received by BGP4+ connection. This operation message is output according to the following conditions: 1. The messages from the first to the 16th event are output. 2. After 17 times from the beginning of the event occurrence, this message is output once every 256 times the event occurs. 3. If an event occurs 3 minutes or more after the last event occurred, this message is output depending on 1 and 2 above. Note that the above number of messages includes the count of BGP4+: Invalid MD5 digest from <source ipv6> + <port no.> to <destination ipv6> + <port no.>. [Explanation of message variables] <source ipv6>: Source IPv6 address <port no.>: TCP port number <destination ipv6>: Destination IPv6 address <vrf id>: VRF ID [Action] Check whether the MD5 authentication is set in BGP4+ of the remote device. If it is not set, set the MD5 authentication so that it matches. If the setting matches, check whether TCP segments are sent from a peer other than the source BGP4+ peer.
88	BGP4+: Invalid MD5 digest from <source ipv6>+<port no.> to <destination ipv6>+<port no.> [VRF <vrf id>]	Warning (local device or remote device) The MD5 authentication option for TCP segments received by BGP4+ connection is invalid. This operation message is output according to the following conditions: 1. The messages from the first to the 16th event are output. 2. After 17 times from the beginning of the event occurrence, this message is output once every 256 times the event occurs. 3. If an event occurs 3 minutes or more after the last event occurred, this message is output depending on 1 and 2 above. Note that the above number of messages includes the count of BGP4+: No MD5 digest from <source ipv6> + <port no.> to <destination ipv6> + <port no.>. [Explanation of message variables] <source ipv6>: Source IPv6 address <destination ipv6>: Destination IPv6 address

No.	Message text	Description
		<port no.>: TCP port number <vrf id>: VRF ID [Action] Check if the MD5 authentication keys match in BGP4+ of the local and remote devices. If the MD5 authentication keys do not match, set them so that they do match. If the MD5 authentication keys match, check if TCP segments are sent from a peer other than the source BGP4+ peer.
89	BGP4+: Number of prefix received from <bgp name> [(<description>)]: reached <routes1>, limit <routes2>	Warning (remote device)
		The number of paths (active routes and inactive routes) learned from the relevant peer exceeded the threshold. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <routes1>: Number of paths learned from peers <routes2>: Maximum number of paths learned from peers [Action] If the number of paths learned from the peer further increases, check the number of the paths advertised by the peer.
90	BGP4+: Number of prefix received from <bgp name> [(<description>)]: <routes1> exceed limit <routes2>	Warning (remote device)
		The number of paths (active routes and inactive routes) learned from the relevant peer exceeded the maximum value. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <routes1>: Number of paths learned from peers <routes2>: Maximum number of paths learned from peers [Action] Check the number of the paths advertised by the relevant peer.
91	BGP4+: Peer <bgp name> [(<description>)]: Closed connection by maximum-prefix	Information (remote device)
		BGP4+ connection was closed due to the limitation of the number of learned paths. [Explanation of message variables] <bgp name>: Connection target peer name <description>: Description name of the connection target peer [Action] Check the number of the paths advertised by the relevant peer. To reconnect the peer, make sure that the number of paths advertised by the peer is equal to or less than the maximum value, and then enter the "clear ipv6 bgp" command.

No.	Message text	Description
92	BGP4+: Peer <bgp name> [(<description>)] UPDATE included attribute type code (0) [- AS Path (<as number>): <aspath>]	Warning (remote device) An UPDATE message including the path attribute of type code 0 was received from the relevant peer. This operation message is not output again on the same peer for an hour after the previous output. [Explanation of message variables] <bgp name>: Source peer name <description>: Description name of the source peer <as number>: Number of AS numbers <aspath>: AS paths, in the following format: • AS sequential number: AS_SEQ • {AS sequential number}: AS_SET • (AS sequential number): AS_CONFED_SEQUENCE Note that, the entire AS path might not be output because there is a limit to the number of characters that can be output in an operation message. [Action] Check the unicast routing program (BGP4+) in the peer.
93	bgp4+_pp_recv: Peer <bgp name> as receiving-speaker failed to retain stale routes, the packets forwarded to the peer may be discarded.	Warning (remote device) A peer acting as a receiving router failed to save the forwarding path. Packets forwarded to the target peers may be discarded. [Explanation of message variables] <bgp name>: Connection target peer name [Action] During the graceful restart negotiation, non-forwardable state was notified. Investigate whether a failure has occurred on the peer router.
94	BGP4+: Completed the learning from receiving-speakers	Information (local device) Route learning from the receiving router has been completed. [Explanation of message variables] None. [Action] None.
95	BGP4+: Start advertisement, giving up learning from several receiving-speakers	Information (local device) Interrupt the route learning from some receiving routers and start the route advertisement. [Explanation of message variables] None. [Action] None.

No.	Message text	Description
96	bgp4+_recv_open: Peer <bgp name> as receiving-speaker failed to retain stale routes, the packets forwarded to the peer may be discarded.	Warning (remote device)
		A peer acting as a receiving router failed to save the forwarding path. Packets forwarded to the target peers may be discarded. [Explanation of message variables] <bgp name>: Connection target peer name [Action] During the graceful restart negotiation, non-forwardable state was notified. Investigate whether a failure has occurred on the peer router.

3.3.4 Common to IPv6 unicast routing protocols

The following table describes the event information common to IPv6 unicast routing protocols (RTM).

Table 3-9: Event information common to IPv6 unicast routing protocols

No.	Message text	Description
1	*** Give up gdump. Because of no enough memory.	Warning (local device)
		Dump collection was stopped because the remaining memory capacity of the system temporarily fell below the preset value while unicast routing program control information dumps were being collected by the "dump protocols unicast" command. [Explanation of message variables] None. [Action] There is not enough memory to execute the command. Review the capacity limit.
2	The number of IPv6 unicast routes on global network exceeded the limit.	Warning (local device)
		The number of IPv6 unicast routes on the global network has exceeded the maximum. [Explanation of message variables] None. [Action] 1. Delete unnecessary routes. 2. Review the maximum number of routes that was specified in the configuration.
3	The number of IPv6 unicast routes on VRF <vrf id> exceeded the limit.	Warning (local device)
		The number of IPv6 unicast routes on VRF <vrf id> has exceeded the maximum. [Explanation of message variables] <vrf id>: VRF ID [Action] 1. Delete unnecessary routes. 2. Review the maximum number of routes that was specified in the configuration.

No.	Message text	Description
4	The number of IPv6 unicast routes on global network exceeded the warning threshold.	Information (local device)
		The number of IPv6 unicast routes on the global network has exceeded the warning threshold value. [Explanation of message variables] None. [Action] When adding routes, make sure that the number of added routes does not exceed the maximum.
5	The number of IPv6 unicast routes on VRF <vrf id> exceeded the warning threshold.	Information (local device)
		The number of IPv6 unicast routes on VRF <vrf id> has exceeded the warning threshold value. [Explanation of message variables] <vrf id>: VRF ID [Action] When adding routes, make sure that the number of added routes does not exceed the maximum.
6	Rtm: Graceful Restart terminated because this system failed to retain the routes.	Warning (local device)
		Graceful restart failed because the route could not be retained. [Explanation of message variables] None. [Action] Investigate whether the unicast routing program restarts during the graceful restart.

3.4 IPv6 routing information (RTM)

3.4.1 RA

The following table describes the event information for IPv6 routing information (RTM).

Table 3-10: IPv6 routing (RA) event information

No.	Message text	Description
1	rs_input: Cannot locate interface for RS from <address1> to <address2>	Error (local device)
		The router solicitation was ignored because an interface corresponding to the received router solicitation is not found. [Explanation of message variables] <address1>: Router solicitation sender address <address2>: Router solicitation destination address [Action] If this error frequently occurs, check the status of the interface.
2	rs_input: ND option check failed for an RS from <address> on <interface name>	Error (remote device)
		The router solicitation was ignored because the ND option check for the router solicitation from the relevant address failed. [Explanation of message variables] <address>: Router solicitation sender address <interface name>: Name of interface for receiving router solicitation [Action] Check the router solicitation setting in the router solicitation sender terminal.
3	rs_input: RS from unspecified src on <interface name> has a link-layer address option	Error (remote device)
		The router solicitation was ignored because the link-layer address option has been set for router solicitation from unspecified address (::). [Explanation of message variables] <interface name>: Name of interface for receiving router solicitation [Action] Check the router solicitation setting in the router solicitation sender terminal.
4	rs_input: RS received on non advertising interface(<interface name>)	Warning (local device)
		The router solicitation was ignored because the router solicitation was received by the interface that does not advertise routers. [Explanation of message variables] <interface name>: Name of interface for receiving router solicitation [Action] If it is necessary to respond to the router solicitation, enable router advertisement in the interface.

No.	Message text	Description
5	rs_input: RS with invalid hop limit(<hop limit>) received from <address> on <interface name>	Error
		The router solicitation was ignored because the hop limit of the received router solicitation packet is not the correct value (255). [Explanation of message variables] <hop limit>: Hop limit value of the received router solicitation message <address>: Router solicitation sender address <interface name>: Name of interface for receiving router solicitation [Action] Check the settings of the terminal that sends a router request.
6	rs_input: RS with invalid ICMP6 code(<code>) received from <address> on <interface name>	Error
		The router solicitation was ignored because the ICMP6 code of the received router solicitation packet is not the correct value (0). [Explanation of message variables] <code>: ICMP6 code value of the received router solicitation message <address>: Router solicitation sender address <interface name>: Name of interface for receiving router solicitation [Action] Check the settings of the terminal that sends a router request.
7	rs_input: RS from <address> on <interface name> does not have enough length (len = <length>)	Error
		The router solicitation was ignored because the received router solicitation packet is short. [Explanation of message variables] <address>: Router solicitation sender address <interface name>: Name of interface for receiving router solicitation <length>: Received router solicitation packet length [Action] Check the settings of the terminal that sends a router request.
8	nd6_options: bad ND option length(0) (type = <type>)	Error (remote device)
		The length of the ND option is invalid. [Explanation of message variables] <type>: Received ND option type number [Action] Take action to correct the rs_input and ra_input errors that were output together.
9	ra_output: Cannot send RA for I/F <interface name> (lack of active linklocal addr)	Error (local device)
		Router advertisements cannot be sent because there is no valid link-local address in the relevant interface. [Explanation of message variables] <interface name>: Name of interface for sending router advertisements [Action] If this error frequently occurs, check the status of the interface.

No.	Message text	Description
10	ra_output: Cannot send RA for I/F <interface name>	Error (local device)
		Router advertisements cannot be sent from the relevant interface. [Explanation of message variables] <interface name>: Name of interface for sending router advertisements [Action] If this error frequently occurs, check the status of the interface.
11	ra_output: not send RA for I/F <interface name> (linkmtu <value own> is greater than the physical interface MTU <phymtu>)	Warning (local device)
		Router advertisements are not output because the specified value exceeds the MTU length of the relevant interface. [Explanation of message variables] <interface name>: Name of interface for sending router advertisements <value own>: MTU option value of the local system <phymtu>: Physical MTU length of the interface [Action] Check the settings of the router that sends router advertisements.

3.5 IPv4 multicast routing information (MRP)

3.5.1 PIM-SM

The following table describes the event information for IPv4 routing information (MRP).

Table 3-11: IPv4 multicast routing (PIM-SM) event information

No.	Message text	Description
1	IGMP: received packet too short (<length> bytes) for IP header [on VRF <vrf id>]	Error (remote device)
		A packet smaller than the IP header was received. [Explanation of message variables] <length>: Received packet size <vrf id>: VRF ID [Action] A remote device is sending an invalid packet. Check the IPv4 multi-cast communication program of the remote device.
2	IGMP: received packet (<length1> bytes) from <source address> shorter than header + data length (<length2> + <length3> bytes) [on VRF <vrf id>]	Error (remote device)
		A packet smaller than the data length specified in the IP header was received. [Explanation of message variables] <length1>: Received packet size <source address>: Source IPv4 address <length2>: Received IP header size <length3>: Received IP packet data size <vrf id>: VRF ID [Action] A remote device is sending an invalid packet. Check the IPv4 multi-cast communication program of the remote device.
3	IGMP: received IP data field too short (<length> bytes) for IGMP header, from <source address> to <destination address> [on VRF <vrf id>]	Error (remote device)
		A packet smaller than an IGMP header length (8) was received. [Explanation of message variables] <length>: Received IP packet data size <source address>: Source IPv4 address <destination address>: Destination IPv4 address <vrf id>: VRF ID [Action] A remote device is sending an invalid packet. Check the IPv4 multi-cast communication program of the remote device.

No.	Message text	Description
4	IGMP: ignoring packet from <source address> to <destination address> [on VRF <vrf id>] - invalid igmp header checksum (data '<data>', length '<length>')	Error (remote device)
		A received IGMP packet was ignored because of an IGMP header checksum error. [Explanation of message variables] <source address>: Source IPv4 address <destination address>: Destination IPv4 address <vrf id>: VRF ID <data>: Contents of the first byte (packet type) of IGMP received data <length>: IGMP received data length [Action] A remote device is sending an invalid packet. Check the IPv4 multi-cast communication program of the remote device.
5	IGMP: ignoring <packet> from <source address> to <destination address> [on VRF <vrf id>] - invalid group address '<group address>'	Error (remote device)
		A received IGMP packet was ignored because the group address in the packet was invalid. [Explanation of message variables] <packet>: Packet type • "Group Membership Report", "Group Leave Report" <source address>: Source IPv4 address <destination address>: Destination IPv4 address <vrf id>: VRF ID <group address>: Received group address [Action] A remote device is sending an invalid packet. Check the IPv4 multi-cast communication program of the remote device.
6	IGMP: Querier was changed on interface <interface name> [of VRF <vrf id>] - new querier <querier ip address> (was <old querier ip address>)	Event (local device)
		The querier router changed on the interface. [Explanation of message variables] <interface name>: Interface name <vrf id>: VRF ID <querier ip address>: Querier IPv4 address <old querier ip address>: Previous querier IPv4 address [Action] None.
7	PIM: received packet too short (<length> bytes) for IP header [on VRF <vrf id>]	Error (remote device)
		A packet smaller than the IP header was received. [Explanation of message variables] <length>: Received packet size <vrf id>: VRF ID [Action] A remote device is sending an invalid packet. Check the IPv4 multicast routing program (PIM-SM) of the remote device.

No.	Message text	Description
8	PIM: received packet (<length1> bytes) from <source address> shorter than header + data length (<length2> + <length3> bytes) [on VRF <vrf id>]	Error (remote device) A packet smaller than the data length specified in the IP header was received. [Explanation of message variables] <length1>: Received packet size <source address>: Source IPv4 address <length2>: Received IP header size <length3>: Received IP packet data size <vrf id>: VRF ID [Action] A remote device is sending an invalid packet. Check the IPv4 multicast routing program (PIM-SM) of the remote device.
9	PIM: received IP data field too short (<length> bytes) for PIM header, from <source address> to <destination address> [on VRF <vrf id>]	Error (remote device) A packet smaller than an PIM header length (4) was received. [Explanation of message variables] <length>: Received IP packet data size <source address>: Source IPv4 address <destination address>: Destination IPv4 address <vrf id>: VRF ID [Action] A remote device is sending an invalid packet. Check the IPv4 multicast routing program (PIM-SM) of the remote device.
10	PIM: ignoring packet from <source address> to <destination address> [on VRF <vrf id>] - invalid pim header checksum (data '<data>', length '<length>')	Error (remote device) A received PIM packet was ignored because of an PIM header checksum error. [Explanation of message variables] <source address>: Source IPv4 address <destination address>: Destination IPv4 address <vrf id>: VRF ID <data>: Contents of the first byte (packet type) of PIM received data <length>: PIM received data length [Action] A remote device is sending an invalid packet. Check the IPv4 multicast routing program (PIM-SM) of the remote device.
11	PIM: ignoring <packet> message from <source address> to <destination address> [on VRF <vrf id>] - packet too short (<length> bytes)	Error (remote device) A received PIM packet was ignored because the packet size was smaller than the minimum packet length. [Explanation of message variables] <packet>: Packet type

No.	Message text	Description
		• "Register", "Register-Stop", "Join/Prune", "Assert", "Bootstrap", "Candidate-RP-Advertisement" <source address>: Source IPv4 address <destination address>: Destination IPv4 address <vrf id>: VRF ID <length>: PIM received data length [Action] A remote device is sending an invalid packet. Check the IPv4 multicast routing program (PIM-SM) of the remote device.
12	PIM: ignoring <packet> message from <source address> to <destination address> [on VRF <vrf id>] - invalid encoded unicast address (<cause>)	Error (remote device)
		A received PIM packet was ignored because the encoding unicast address in the packet was invalid. [Explanation of message variables] <packet>: Packet type • "Register-Stop", "Join/Prune", "Assert", "Bootstrap", "Candidate-RP-Advertisement" <source address>: Source IPv4 address <destination address>: Destination IPv4 address <vrf id>: VRF ID <cause>: Detailed cause • address family '<value>': The address family <value> is invalid (other than 1). • encoding type '<value>': The encoding type <value> is invalid (other than 0). • source address '<address>': The source IPv4 address <address> is invalid. • upstream neighbor address '<address>': The upstream neighbor IPv4 address <address> is invalid. • BSR address '<address>': The BSR address <address> is invalid. • RP address '<address>': The rendezvous point address <address> is invalid. [Action] A remote device is sending an invalid packet. Check the IPv4 multicast routing program (PIM-SM) of the remote device.
13	PIM: ignoring <packet> message from <source address> to <destination address> [on VRF <vrf id>] - invalid encoded source address (<cause>)	Error (remote device)
		A received PIM packet was ignored because the encoding sender IPv4 address in the packet was invalid. [Explanation of message variables] <packet>: Packet type • "Join/Prune" <source address>: Source IPv4 address <destination address>: Destination IPv4 address <vrf id>: VRF ID

No.	Message text	Description
		<cause>: Detailed cause • address family '<value>': The address family <value> is invalid (other than 1). • encoding type '<value>': The encoding type <value> is invalid (other than 0). [Action] A remote device is sending an invalid packet. Check the IPv4 multicast routing program (PIM-SM) of the remote device.
14	PIM: ignoring <packet> message from <source address> to <destination address> [on VRF <vrf id>] - invalid encoded group address (<cause>)	Error (remote device) A received PIM packet was ignored because the encoding group address in the packet was invalid. [Explanation of message variables] <packet>: Packet type • "Register-Stop", "Join/Prune", "Assert", "Bootstrap", "Candidate-RP-Advertisement" <source address>: Source IPv4 address <destination address>: Destination IPv4 address <vrf id>: VRF ID <cause>: Detailed cause • address family '<value>': The address family <value> is invalid (other than 1). • encoding type '<value>': The encoding type <value> is invalid (other than 0). • mask length '<value>': The group mask length <value> is invalid (not in the range from 4 to 32). • group address '<address>': The group address <address> is invalid. [Action] A remote device is sending an invalid packet. Check the IPv4 multicast routing program (PIM-SM) of the remote device.
15	PIM: ignoring Hello message from <source address> [on VRF <vrf id>] - invalid holdtime option length (<length>)	Error (remote device) A received PIM packet was ignored because the length of the holdtime option in the Hello packet was invalid (other than 2). [Explanation of message variables] <source address>: Source IPv4 address <vrf id>: VRF ID <length>: Received holdtime option length [Action] A remote device is sending an invalid packet. Check the IPv4 multicast routing program (PIM-SM) of the remote device.

No.	Message text	Description
16	PIM: ignoring Hello message from <source address> [on VRF <vrf id>] - no holdtime option	Error (remote device)
		A received PIM packet was ignored because the holdtime option was not included in the Hello packet. [Explanation of message variables] <source address>: Source IPv4 address <vrf id>: VRF ID [Action] A remote device is sending an invalid packet. Check the IPv4 multicast routing program (PIM-SM) of the remote device.
17	PIM: ignoring Register message from <source address> to <destination address> [on VRF <vrf id>] - invalid inner source address '<inner source address>'	Error (remote device)
		A received PIM packet was ignored because the source IPv4 address of IP packets encapsulated by the Register packet was invalid. [Explanation of message variables] <source address>: Source IPv4 address <destination address>: Destination IPv4 address <vrf id>: VRF ID <inner source address>: Encapsulated source IPv4 address [Action] The source multi-cast data is sending invalid packets. Check the IPv4 multi-cast communication program sent from the source multi-cast data.
18	PIM: ignoring Register message from <source address> to <destination address> [on VRF <vrf id>] - invalid inner group address '<inner group address>'	Error (remote device)
		A received PIM packet was ignored because the group address of IP packets encapsulated by the Register packet was invalid. [Explanation of message variables] <source address>: Source IPv4 address <destination address>: Destination IPv4 address <vrf id>: VRF ID <inner group address>: Encapsulated group address [Action] The source multi-cast data is sending invalid packets. Check the IPv4 multi-cast communication program sent from the source multi-cast data. If the encapsulated group address is in the range from PIM to SSM, check the PIM-SSM setting of the remote device.
19	PIM: ignoring Bootstrap message from <source address> to <destination address> [on VRF <vrf id>] - invalid hash mask length '<value>'	Error (remote device)
		A received PIM packet was ignored because the hash mask length in the Bootstrap packet was invalid (33 or more). [Explanation of message variables] <source address>: Source IPv4 address <destination address>: Destination IPv4 address <vrf id>: VRF ID <value>: Hash mask length specified for the received packet

No.	Message text	Description
		[Action] A remote device is sending an invalid packet. Check the IPv4 multicast routing program (PIM-SM) of the remote device.
20	PIM: BSR information was changed [on VRF <vrf id>] - lost BSR information	Warning (remote device)
		BSR information was cleared because advertisements from the Bootstrap router were lost. [Explanation of message variables] <vrf id>: VRF ID [Action] Check the reason why advertisements from the Bootstrap router were lost.
21	PIM: BSR information was changed [on VRF <vrf id>] - new BSR address <ip address>	Event (local device)
		BSR address was changed. [Explanation of message variables] <vrf id>: VRF ID <ip address>: BSR address If the BSR address is the Switch, "(this system)" is displayed after the IPv4 address. [Action] None.
22	PIM: Learning of IPv4 multicast routing entries started because a master switch switchover occurred. (aging time = <time> seconds)	Event (local device)
		Learning of IPv4 multicast route information has started due to the switch status changing from backup to master in a stack configuration (learning time is <time> seconds). [Explanation of message variables] <time> Relearning period for IPv4 multicast route information [Action] None.
23	PIM: Learning of IPv4 multicast routing entries finished after a master switch switchover occurred.	Event (local device)
		Learning of IPv4 multicast route information has finished due to the switch status changing from backup to master in a stack configuration. [Explanation of message variables] None. [Action] None.

3.6 IPv6 multicast routing information (MR6)

3.6.1 IPv6 PIM-SM

The following table describes the event information for IPv6 routing information (MR6).

Table 3-12: IPv6 multicast routing (PIM-SM) event information

No.	Message text	Description
1	MLD: ignoring <packet> from <source address> [on VRF <vrf id>] - invalid scope <group address>	Error (remote device)
		MLD packets were ignored because the scope of group addresses included in the packets were invalid (node-local or link-local). [Explanation of message variables] <packet>: Packet type • "Multicast Listener Query", "Multicast Listener Report", "Multicast Listener Done", "MLDv2 Multicast Listener Report" <source address>: Source IPv6 address <vrf id>: VRF ID <group address>: MLD group address [Action] A remote device is sending an invalid packet. Check the IPv6 multi-cast communication program of the remote device.
2	MLD: ignoring <packet> from <source address> [on VRF <vrf id>] - message received from a non linklocal address	Error (remote device)
		MLD packets that have non-link-local addresses in the source were ignored. [Explanation of message variables] <packet>: Packet type • "Multicast Listener Query" <source address>: Source IPv6 address <vrf id>: VRF ID [Action] A remote device is sending an invalid packet. Check the IPv6 multi-cast communication program of the remote device.
3	MLD: Querier was changed on interface <interface name> [of VRF <vrf id>] - new querier <querier ipv6 address> (was <old querier ipv6 address>)	Event (local device)
		The querier router changed on the interface. [Explanation of message variables] <interface name>: Interface name <vrf id>: VRF ID <querier ipv6 address>: Querier IPv6 address • If the querier IPv6 address is the Switch, "(this system)" is displayed. <old querier ipv6 address>: Previous querier IPv6 address • If the previous querier IPv6 address is the Switch, "(this system)" is displayed. [Action] None.

No.	Message text	Description
4	PIM: ignoring <packet> message from <source address> [on VRF <vrf id>] - packet too short (<length> bytes)	Error (remote device) A received PIM packet was ignored because the packet size was smaller than the minimum packet length. [Explanation of message variables] <packet>: Packet type • "Hello", "Register", "Register-Stop", "Join/Prune", "Assert", "Bootstrap", "Candidate-RP-Advertisement" <source address>: Source IPv6 address <vrf id>: VRF ID <length>: PIM received data length [Action] A remote device is sending an invalid packet. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.
5	PIM: ignoring <packet> message from <source address> [on VRF <vrf id>] - invalid encoded unicast address (<cause>)	Error (remote device) A received PIM packet was ignored because the encoding unicast address in the packet was invalid. [Explanation of message variables] <packet>: Packet type • "Hello", "Register-Stop", "Join/Prune", "Assert", "Bootstrap", "Candidate-RP-Advertisement" <source address>: Source IPv6 address <vrf id>: VRF ID <cause>: Detailed cause • address family '<value>': The address family <value> is invalid (other than 2). • encoding type '<value>': The encoding type <value> is invalid (other than 0). • source address '<address>': The source address <address> is invalid. • upstream neighbor address '<address>': The upstream neighboring address <address> is invalid. • BSR address '<address>': The BSR address <address> is invalid. • RP address '<address>': The rendezvous point address <address> is invalid. [Action] A remote device is sending an invalid packet. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.

No.	Message text	Description
6	PIM: ignoring <packet> message from <source address> [on VRF <vrf id>] - invalid encoded source address (<cause>)	Error (remote device)
		A received PIM packet was ignored because the encoding source address was invalid. [Explanation of message variables] <packet>: Packet type • "Join/Prune" <source address>: Source IPv6 address <vrf id>: VRF ID <cause>: Detailed cause • address family '<value>': The address family <value> is invalid (other than 2). • encoding type '<value>': The encoding type <value> is invalid (other than 0). [Action] A remote device is sending an invalid packet. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.
7	PIM: ignoring <packet> message from <source address> [on VRF <vrf id>] - invalid encoded group address (<cause>)	Error (remote device)
		A received PIM packet was ignored because the encoding group address in the packet was invalid. [Explanation of message variables] <packet>: Packet type • "Register-Stop", "Join/Prune", "Assert", "Bootstrap", "Candidate-RP-Advertisement" <source address>: Source IPv6 address <vrf id>: VRF ID <cause>: Detailed cause • address family '<value>': The address family <value> is invalid (other than 2). • encoding type '<value>': The encoding type <value> is invalid (other than 0). • mask length '<value>': The group mask length <value> is invalid (not in the range from 8 to 128). • group address '<address>': The group address <address> is invalid. [Action] A remote device is sending an invalid packet. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.
8	PIM: ignoring Hello message from <source address> [on VRF <vrf id>] - invalid holdtime option length (<length>)	Error (remote device)
		A received PIM packet was ignored because the length of the holdtime option in the Hello packet was invalid (other than 2). [Explanation of message variables]

No.	Message text	Description
		<source address>: Source IPv6 address <vrf id>: VRF ID <length>: Received holdtime option length [Action] A remote device is sending an invalid packet. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.
9	PIM: ignoring Hello message from <source address> [on VRF <vrf id>] - no hold-time option	Error (remote device)
		A received PIM packet was ignored because the holdtime option was not included in the Hello packet. [Explanation of message variables] <source address>: Source IPv6 address <vrf id>: VRF ID [Action] A remote device is sending an invalid packet. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.
10	PIM: ignoring Register message from <source address> [on VRF <vrf id>] - invalid inner source address '<inner source address>'	Error (remote device)
		A received PIM packet was ignored because the source address of IPv6 packets encapsulated by the Register packet was invalid. [Explanation of message variables] <source address>: Source IPv6 address <vrf id>: VRF ID <inner source address>: Encapsulated source address [Action] The source multi-cast data is sending invalid packets. Check the IPv6 multi-cast communication program sent from the source multi-cast data.
11	PIM: ignoring Register message from <source address> [on VRF <vrf id>] - invalid inner source address scope '<inner source address>'	Error (remote device)
		A received PIM packet was ignored because the scope of the source address of IPv6 packets encapsulated by the Register packet was invalid. [Explanation of message variables] <source address>: Source IPv6 address <vrf id>: VRF ID <inner source address>: Encapsulated source address [Action] The source multi-cast data is sending invalid packets. Check the IPv6 multi-cast communication program sent from the source multi-cast data.

No.	Message text	Description
12	PIM: ignoring Register message from <source address> [on VRF <vrf id>] - invalid inner group address '<inner group address>'	Error (remote device)
		A received PIM packet was ignored because the group address of IPv6 packets encapsulated by the Register packet was invalid. [Explanation of message variables] <source address>: Source IPv6 address <vrf id>: VRF ID <inner group address>: Encapsulated group address [Action] The source multi-cast data is sending invalid packets. Check the IPv6 multi-cast communication program sent from the source multi-cast data.
13	PIM: ignoring Register message from <source address> [on VRF <vrf id>] - invalid inner group address scope '<inner group address>'	Error (remote device)
		A received PIM packet was ignored because the scope of the group address of IPv6 packets encapsulated by the Register packet was invalid. [Explanation of message variables] <source address>: Source IPv6 address <vrf id>: VRF ID <inner group address>: Encapsulated group address [Action] The source multi-cast data is sending invalid packets. Check the IPv6 multi-cast communication program sent from the source multi-cast data.
14	PIM: ignoring Register message from <source address> [on VRF <vrf id>] - invalid inner IP version '<version>'	Error (remote device)
		A received PIM packet was ignored because the version of IPv6 packets encapsulated by the Register packet was not version 6. [Explanation of message variables] <source address>: Source IPv6 address <vrf id>: VRF ID <version>: Encapsulated IP packet version [Action] The source multi-cast data is sending invalid packets. Check the IPv6 multi-cast communication program sent from the source multi-cast data.
15	PIM: ignoring Bootstrap message from <source address> [on VRF <vrf id>] - invalid hash mask length '<value>'	Error (remote device)
		A received PIM packet was ignored because the hash mask length in the Bootstrap packet was invalid (129 or more). [Explanation of message variables] <source address>: Source IPv6 address <vrf id>: VRF ID <value>: Hash mask length specified for the received packet [Action] A remote device is sending an invalid packet. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.

No.	Message text	Description
16	PIM: ignoring Bootstrap message from <source address> [on VRF <vrf id>] - invalid BSR address '<ipv6 address>'	Error (remote device)
		A received PIM packet was ignored because the BSR address in the Bootstrap packet was invalid. [Explanation of message variables] <source address>: Source IPv6 address <vrf id>: VRF ID <ipv6 address>: BSR address [Action] A remote device is sending an invalid packet. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.
17	PIM: ignoring Bootstrap message from <source address> [on VRF <vrf id>] - cannot find a route to the BSR(<ipv6 address>)	Warning (local device)
		A received PIM packet was ignored because the unicast route to the BSR address in the Bootstrap was not found. [Explanation of message variables] <source address>: Source IPv6 address <vrf id>: VRF ID <ipv6 address>: BSR address [Action] Check whether the route to the BSR address in the Bootstrap packet exists.
18	PIM: ignoring Candidate-RP-Advertisement message from <source address> [on VRF <vrf id>] - non global address(<ipv6 address>) as RP	Error (remote device)
		A received PIM packet was ignored because the rendezvous point address included in the Candidate-RP-Advertisement packet was invalid. [Explanation of message variables] <source address>: Source IPv6 address <vrf id>: VRF ID <ipv6 address>: Rendezvous point address [Action] A remote device is sending an invalid packet. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.
19	PIM: BSR information was changed [on VRF <vrf id>] - lost BSR information	Warning (remote device)
		BSR information was cleared because advertisements from the Bootstrap router were lost. [Explanation of message variables] <vrf id>: VRF ID [Action] Check the reason why advertisements from the Bootstrap router were lost.

No.	Message text	Description
20	PIM: BSR information was changed [on VRF <vrf id>] - new BSR address <ipv6 address>	Event (local device)
		BSR address was changed. [Explanation of message variables] <vrf id>: VRF ID <ipv6 address>: BSR address If the BSR address is the Switch, "(this system)" is displayed after the IPv6 address. [Action] None.
21	PIM: Add interface <interface name> [of VRF <vrf id>] to the output interface list of (S,G)=(<source address>, <group address>)	Event (local device)
		Interface <interface name> was added to the output interface list of the multicast routing cache (S, G) (this message is output to syslog only). [Explanation of message variables] <interface name>: Interface name <vrf id>: VRF ID <source address>: Source IPv6 address <group address>: IPv6 group address [Action] None.
22	PIM: Delete interface <interface name> [of VRF <vrf id>] from the output interface list of (S,G)=(<source address>, <group address>)	Event (local device)
		Interface <interface name> was deleted from the output interface list of the multicast routing cache (S, G) (this message is output to syslog only). [Explanation of message variables] <interface name>: Interface name <vrf id>: VRF ID <source address>: Source IPv6 address <group address>: IPv6 group address [Action] None.

3.7 BFD information (BFD)

The following table describes the event information for BFD information (BFD).

Table 3-13: BFD event information

No.	Message text	Description
1	The number of BFD sessions exceeded the limit.	Event (local device)
		The number of BFD session exceeds the capacity limit. [Explanation of message variables] None. [Action] Because the number of BFD session has reached the upper limit, BFD monitoring for the excess will not be performed. Run without exceeding the capacity limit. To enable the target BFD monitoring, delete unnecessary BFD monitoring settings, and then execute the "clear bfd session" command with the all parameter.
2	BFD sessions could not be set because an error occurred.	Event (local device)
		The BFD session setting failed. [Explanation of message variables] None. [Action] Make sure that the Switch can communicate with the partner device. To enable the target BFD monitoring, review the settings and then execute the "clear bfd session" command with the all parameter.
3	BFD packets cannot be sent because no valid loopback interface address has been set. (remote address = <address>[, VRF = <vrf id>], session index = <index>)	Event (local device)
		BFD packets cannot be sent because a valid loopback interface address is not set. [Explanation of message variables] <address> IPv4 address of remote system <vrf id>: VRF ID <index> BFD session number [Action] Set a valid IP address to the loopback interface.
4	BFD packets cannot be sent because no valid next hop exists. (remote address = <address>[, VRF = <vrf id>], session index = <index>)	Event (local device)
		The BFD packet cannot be sent because there is no valid next hop. [Explanation of message variables] <address> IPv4 address of remote system <vrf id>: VRF ID <index> BFD session number [Action] Check the state of the interface.

No.	Message text	Description
5	The BFD session status changed. (remote address = <address>[, VRF = <vrf id>], session index = <index>, state = <old state> to <new state>[, diagnostic code = <diag code>])	Event (local device) The BFD session status was changed. [Explanation of message variables] <address> IPv4 address of remote system <vrf id>: VRF ID <index> BFD session number <old state> Session status before change • Down: Down • Init: Establishment being requested • Up: Up • AdminDown: Administrative down <new state> Session status after change <diag code> Diagnostic code from the remote system (when session status after change is down or administratively down) • Control Detection Time Expired • Neighbor Signaled Session Down • Path Down • Administratively Down [Action] If the change is not intended, check the operation of the Switch and the communication status with the remote device based on the diagnostic code. • If Control Detection Time Expired is displayed, valid BFD packets are not received from the remote system during the failure detection time. • If Neighbor Signaled Session Down is displayed, the remote system has notified you that the BFD session is down. • If Path Down is displayed, the sending interface or route is down. • If Administratively Down is displayed, it is administratively down. Administrative down indicates that the Switch is intentionally suppressed due to its operating status. After reviewing the capacity limit, communication status, and settings, execute the "clear bfd session" command.
6	No BFD packets were received from the remote system during the failure detection period. (remote address = <address>[, VRF = <vrf id>], session index = <index>)	Event (local device) No BFD packet was received within the failure detection time. [Explanation of message variables] <address> IPv4 address of remote system <vrf id>: VRF ID <index> BFD session number [Action] Check the status of the communication with the remote device. If there is no problem, check the configuration of the Switch and the settings of the remote system, and set the minimum receiving interval of the Switch to be longer than the minimum sending interval of the remote system.