AX3640S/AX3630S Software Manual

Message and Log Reference

For Version 11.10

AX36S-S008X-H0

■ Relevant products

This manual applies to the models in the AX3640S and AX3630S series of switches. It also describes the functionality of version 11.10 of the software. The described functionality is that supported by the software OS-L3A-A/OS-L3A and OS-L3L-A/OS-L3L, and by optional licenses.

■ Export restrictions

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

■ Trademarks

Cisco is a registered trademark of Cisco Systems, Inc. in the United States and other countries.

Ethernet is a registered trademark of Xerox Corporation.

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

IPX is a trademark of Novell, Inc.

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

Octpower is a registered trademark of NEC Corporation.

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

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

VitalQIP and VitalQIP Registration Manager are trademarks of Alcatel-Lucent.

VLANaccessClient is a trademark of NEC Soft, Ltd.

VLANaccessController and VLANaccessAgent are trademarks of NEC Corporation.

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

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

■ Reading and storing this manual

Before you use the equipment, carefully read the manual and make sure that you understand all safety precautions.

After reading the manual, keep it in a convenient place for easy reference.

■ Notes

Information in this document is subject to change without notice.

■ Editions history

December 2012 (Edition 18) AX36S-S008X-H0

■ Copyright

History of Amendments

[For version 11.7]

Summary of amendments

Item	Changes
Checking a log	• A description of the tracking object log was added.
Event location = SOFTWARE	• A log message related to the policy-based routing was added. • Log messages related to the tracking functionality of the policy-based routing were added.
Tracking Object Log	• This chapter was added.

[For version 11.6]

Descriptions of AX3650S series switches were moved to the AX3800S/AX3650S Software Manual.

[For version 11.5]

Summary of amendments

Item	Changes
RIP	• A description of VRF was added.
OSPF	• A description of VRF was added.
BGP4	• A description of VRF was added.
Common to IPv4 unicast routing protocols	• Log messages related to VRF were added.
OSPFv3	• A description of VRF was added.
BGP4+	• A description of VRF was added.
Common to IPv6 unicast routing protocols	• Log messages related to VRF were added.
IPv4 multicast routing information (MRP)	• Log messages related to VRF were added.
IPv6 multicast routing information (MR6)	• Log messages related to VRF were added.
Event location = ACCESS	• A description of VRF was added.
Event location = IP	• Log messages related to VRF were added.
Event location = SOFTWARE	• A description of VRF was added. • Log messages related to IPv4 multi-cast were added. • Log messages related to IPv6 multi-cast were added. • Log messages related to Switch management were added.
Event location = EQUIPMENT	• Log messages related to Switch management were added.
Event location = FAN	• A description of AX3650 series switches was added.

[For version 11.4]

Summary of amendments

Item	Changes
Event location = VLAN (Ring Protocol)	• Log messages related to multi-fault monitoring functionality were added.
Event location = SOFTWARE	• Log messages related to IPv6 DHCP relays were added. • Log messages related to power saving functionality were added. • Log messages related to DHCP snooping were added.

Item	Changes
Event location = ULR	• Log messages related to automatic preemption functionality were added.

[For version 11.2]

Summary of amendments

Item	Changes
Event location = VLAN (Ring Protocol)	• Log messages related to path switchback suppression functionality were added.
Event location = SOFTWARE	• Log messages related to VRRP tracking functionality were added.
Event location = ULR	• This subsection was added.

[For version 11.1]

Summary of amendments

Item	Changes
RIP	• Log messages related to authentication were added.
Event location = VLAN (CFM)	• This subsection was added.

[For version 11.0]

Summary of amendments

Item	Changes
Event location = VLAN	• Log messages for clearing the MAC address table by receiving ordinary Flush Request frames were added.
Event location = SOFTWARE	• Log messages related to setting the maximum number of multi paths were added.

[For version 10.8]

Summary of amendments

Item	Changes
Event location = VLAN	• The log message for message ID 25100031 was deleted.
Event location = VLAN (GSRP)	• Log messages for when the automatic master wait time elapsed were added.
Event location = SOFTWARE	• The descriptions of log messages related to IEEE 802.1X were changed. • The descriptions of log messages related to Web authentication were changed. • The descriptions of log messages related to MAC authentication were changed. • Log messages related to packet queuing addressed to CPU were added.
Event location = SOFTWARE (VLAN authentication)	• The descriptions of log messages related to authentication VLAN were changed.

[For version 10.7]

Summary of amendments

Item	Changes
BGP4	• Log messages related to BGP4 were added.

Item	Changes
BGP4+	• Log messages related to BGP4+ were added.
PIM-SM	• Log messages related to registering packets were changed.
Event location = VLAN	• The descriptions related to running the Ring Protocol and Multiple Spanning Tree together were changed.
Event location = VLAN (GSRP)	• The descriptions related to running the Ring Protocol and GSRP together were changed.
Event location = VLAN (L2 loop detection)	• This subsection was added.
Event location = SOFTWARE	• Log messages related to detecting L2 loops were added.

[For version 10.6]

Summary of amendments

Item	Changes
Event location = SOFTWARE	• Log messages related to MAC authentication were added.

[For version 10.4]

Summary of amendments

Item	Changes
Event location = VLAN (Ring Protocol)	• This subsection was added.
Event location = SOFTWARE	• Log messages related to sFlow statistics were added. • Log messages related to Ring Protocol were added.

[For version 10.3]

Summary of amendments

Item	Changes
Event location = ACCESS	• Log messages related to local command authorization were added. • Part of additional information of upper four digits for RADIUS or TACACS+ was changed.
Event location = VLAN	• Log messages when using the root guard functionality and receiving BPDU were added.
Event location = SOFTWARE	• Log messages related to IEEE 802.3ah/UDLD were added. • Log messages related to multi-cast were added. • Log messages related to Web authentication were added.
Event location = SOFTWARE (authentication VLAN)	• Log messages related to authentication VLAN were added.
Event location = PORT	• Log messages related to IEEE 802.3ah/UDLD were added. • Log messages related to detecting unidirectional link failures were added.

[For version 10.2]

Summary of amendments

Item	Changes
Code information for logs	• The identifier of the event location was changed from LINE to PORT.

Item	Changes
OSPF	• A new log message (item number 12) was added.
BGP4	• New log messages (item numbers 89 to 95 and 100 to 102) were added.
OSPFv3	• A new log message (item number 12) was added.
BGP4+	• New log messages (item numbers 86 to 92 and 97 to 99) were added.
Event location = CONFIG	• The message identifier for item numbers 1 to 3 were changed. • A new log message (item number 4) was added.
Event location = VLAN	• The log message for message identifier 20110030 was deleted. • New log messages (item numbers 37, 38, 45, and 46) were added. • In the message, `NIF` was changed to `NIF No.` and `Line` was changed to `Port No.`.
Event location = MAC	• In the message, `NIF` was changed to `NIF No.` and `Line` was changed to `Port No.`.
Event location = SOFTWARE	• Log messages for message identifiers 00005007 and 00005017 were deleted. • New log messages (item numbers 13, 14, 15, 42, 43, 44, 69, 93, 94, 116, and 117) were added. • The message identifier for item numbers 85 and 113 were changed.
Event location = PORT	• The identifier of the event location was changed from LINE to PORT. • New log messages (item numbers 2, 4, and 22 to 30) were added. • Log messages for item numbers 1, 3, 6 to 17, 19 to 21, and 31 to 33 were changed.
Event location = PS	• New log messages (item numbers 1, 3, and 6) were added.
Event location = EQUIPMENT	• A new log message (item number 1) was added.
Event location = FAN	• This subsection was added.

Preface

Applicable products and software versions

This manual applies to the models in the AX3640S and AX3630S series of switches. It also describes the functionality of version 11.10 of the software. The described functionality is that supported by the software OS-L3A-A/OS-L3A and OS-L3L-A/OS-L3L, and by optional licenses.

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

Unless otherwise noted, this manual describes the functions applicable to both the AX3640S and AX3630S series of switches, and functionalities common to each software. For functionalities that are not common to both AX3640S and AX3630S series switches, and functionalities not common to OS-L3A-A/OS-L3A and OS-L3L-A/OS-L3L are indicated as follows:

[AX3640S]:

The description applies to AX3640S switches.

[AX3630S]:

The description applies to AX3630S switches.

[OS-L3A]:

The description applies to OS-L3A-A/OS-L3A for the AX3640S and AX3630S series of switches.

The functions supported by optional licenses are indicated as follows:

[OP-DH6R]:

The description applies to the OP-DH6R optional license.

[OP-OTP]:

The description applies to the OP-OTP optional license.

[OP-VAA]:

The description applies to the OP-VAA optional license.

Corrections to the manual

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

Intended readers

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

Readers must have an understanding of the following:

- The basics of network system management

Manual URL

You can view this manual on our website at:

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

Reading sequence of the manuals

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

● **Unpacking the switch and the basic settings for initial installation**

Quick Start Guide (AX36S-Q001X)

● **Determining the hardware facility conditions and how to handle the hardware**

Hardware Instruction Manual (AX36S-H001X)

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

Configuration Guide Vol.1 (AX36S-S001X)
Vol.2 (AX36S-S002X)
Vol.3 (AX36S-S003X)

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

Configuration Command Reference Vol. 1 (AX36S-S004X)
Vol. 2 (AX36S-S005X)

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

Operation Command Reference Vol. 1 (AX36S-S006X)
Vol. 2 (AX36S-S007X)

● **Understanding messages and logs**

Message and Log Reference (AX36S-S008X)

● **Understanding the MIB**

MIB Reference (AX36S-S009X)

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

Troubleshooting Guide (AX36S-T001X)

Conventions: The terms "Switch" and "switch"

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

AX3640S series switch

AX3630S 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
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second (can also appear as bps)
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4

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

RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SFP+	Enhanced Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VAA	VLAN Access Agent
VLAN	Virtual LAN
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

Conventions: KB, MB, GB, and TB

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

Contents

Chapter

1. Operation Messages and Logs

This chapter explains how to use the failed part, operation messages, and logs to identify the location of errors that have occurred.

1.1 Checking operation messages

The Switch outputs information to be reported to the administrator, such as activity status and failure information, to an operation terminal as operation messages. Operation messages are also stored internally as operation log data. Using this log data, you can manage the switch operating status.

1.1.1 Message types

The table below describes the types of output messages and gives references for those messages. Among these messages, the routing protocol event information, and failure and event information that is output by the switch model is called an operation message.

Table 1-1: Message types and references

Message type	Description	Reference
Configuration error messages	Messages output for input of configuration command	*Error Messages on Configuration Editing* in the manual *Configuration Command Reference*
Command response messages	Messages output for command input	*Response Messages* section of each command in the manual *Operation Command Reference*
Operation messages	Routing protocol event information	*2. Routing Event Information*
	Device failure information and event information	*3. Device Failure and Event Information*

1.1.2 Contents of operation messages

Routing protocol event information includes both functional items output as operation messages and items not output as operation messages. Items not output as operation messages are also recorded in operation logs. The following table describes the support status of operation messages.

Table 1-2: Support status of operation messages

Category	Function item	Operation messages
Routing protocol event information	IPv4 routing information	Y
	IPv4 multicast routing information	N
	IPv6 routing information	Y
	IPv6 multicast routing information	N
Device failure and event information	Failure information for each event location	Y
	Error information per event location of the switch.	Y

Legend:

Y: Message is displayed

N: Message is not displayed

1.1.3 Format of operation messages

(1) Routing protocol event information

The following shows the format of routing protocol event information.

Figure 1-1: Format of routing protocol event information

```
mm/dd hh:mm:ss       ttttttttttttt...ttttttttttttt
      1                          2
```

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.

(2) Device failure and event information

The following shows the format of device failure and event information.

Figure 1-2: Format of switch failure and event information

```
mm/dd hh:mm:ss  ee  kkkkkkkk  [iii...iii]  xxxxxxxx  yyyy:yyyyyyyyyyyy  ttt...ttt
      1          2      3          4           5            6              7
```

1. Time: Displays the date and time when the event indicated in the message occurred.
2. Event level
3. Event location or function
4. Event interface ID. Whether this information is displayed depends on the event location.
5. Message ID
6. Additional information
7. Message text

Code information such as the event level, and event location or function included in the message are the same as the log. For details, see *1.2.4 Format of the reference log*.

1.1.4 Outputting operation messages

(1) Routing protocol event information

Routing protocol event information reports the operating status of IPv4 and IPv6 routing protocols. To output messages to the operation terminal screen, use commands. The table below describes the commands that can be used. Note that multicast routing protocols do not display messages but only collect them in operation logs.

Table 1-3: Messages output as routing protocol event information

Category	Command name	Description
IPv4 routing information	debug protocols unicast	Starts message display
	no debug protocols unicast	Stops message display
IPv4 multicast routing information	--	No message is displayed
IPv6 routing information	debug protocols unicast	Starts message display
	no debug protocols unicast	Stops message display
IPv6 multicast routing information	--	No message is displayed

Legend: --: Not applicable.

(2) Device failure and event information

All messages for device failure and event information are output to the operation terminal screen.

Depending on the error severity or event contents, the information is classified into seven event levels, ranging from `E3` to `E9`. 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 Checking a log

1.2.1 Log type

The Switch acquires two types of logs: operation log and reference log. The operation log acquires entered commands, operation event information, and command response messages and operation information selected to be output as operation messages to the operation terminal. This information is acquired as log data in chronological order. The reference log acquires statistics for device failure and event information within the operation message.

The following table describes the features of the operation log and reference log.

Table 1-4: Features 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.
Maintenance information that is to be acquired	• Entered commands • Command response messages • Routing protocol event information • Device failure and event information	• Device failure and event information
Number of acquired entries	• 1500 entries can be acquired. Within those, the first 1000 log entries are saved chronologically. • The remaining 500 entries consist of older entries whose log type is `KEY`, `RSP`, `ERR`, or `EVT`. • 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 entries exceeds 1000, whether old entries are deleted or saved depends on the log type. • Excess old entries whose log type is not `KEY`, `RSP`, `ERR`, or `EVT` are deleted. • Excess old entries whose log type is `KEY`, `RSP`, `ERR`, or `EVT` are saved as entries 1001 to 1500. If the number of logs entries exceeds 1500, old log entries are deleted.	• If the number of log entries exceeds 500 entries, entries that have a lower event level are deleted and the new entries are acquired. Note that new entries that have an event level of `E3` or `E4` are not acquired.

1.2.2 Log contents

The following table describes the information acquired in the operation log and reference log.

Table 1-5: Information acquired in the operation log and reference log

Category	Description	Operation log	Reference log	Reference
Entered commands	Commands entered from the operation terminal by operators.	Y	N	--

Category	Description	Operation log	Reference log	Reference
Command response messages	Messages output by switches to respond to entered commands.	Y	N	*Response Messages* section of each command in the manual *Operation Command Reference*
Routing protocol event information	IPv4 routing protocol information	Y	N	*2. Routing Event Information*
	IPv4 multicast routing information	Y	N	
	IPv6 routing protocol information	Y	N	
	IPv6 multicast routing information	Y	N	
Device failure and event information	Failure information for each event location	Y	Y	*3. Device Failure and Event Information*
	Error information per event location of the switch.	Y	Y	
Tracking object log **[AX3640S] [OS-L3A]**	Information for the tracking functionality of the policy-based routing	Y	N	*4. Tracking Object Log [AX3640S] [OS-L3A]*

Legend:

Y: Messages are displayed or log data is acquired.

N: Message is not displayed and log data is not acquired.

--: Not applicable.

1.2.3 Format of operation logs

Messages that are in operation are saved within the device. When log data is stored, it is formatted with a log type for output as operation messages to the screen.

(1) Routing protocol event information

The following describes the formats for entered commands, command response messages, and routing protocol event information.

Figure 1-3: Format of event information for entered commands, command response messages, and routing protocols

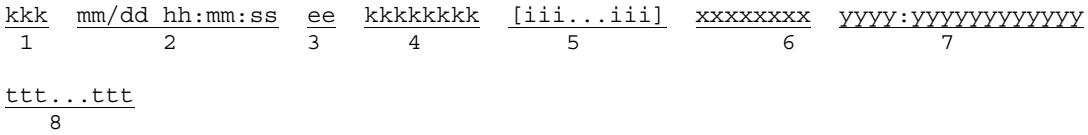
```
kkk   mm/dd hh:mm:ss     ttttttttttttt...ttttttttttttt
 1          2                        3
```

1. Log type: A 3-letter identification code applied for each provided functionality.
   - `KEY`: Operational information selected by entered commands.
   - `RSP`: Event information related to command response messages.
   - `RTM`, `MRP`, or `MR6`: Routing protocol event information
2. Time: Date and time that the event occurred.
3. Message text

(2) Device failure and event information

The following shows the format of device failure and event information.

Figure 1-4: Format of switch failure and event information

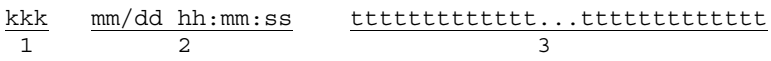


1. Log type: A 3-letter identification code applied for each provided functionality.
   - ERR: Error information for a switch event location
   - EVT: Event information for a switch event location
2. Time: Date and time that the event occurred.
3. Event level
4. Event location or function
5. Event interface ID. Whether this information is displayed depends on the event location.
6. Message ID
7. Additional information
8. Message text

(3) Tracking object log [AX3640S] [OS-L3A]

The figure below shows the format for tracking object logs.

Figure 1-5: Format of the tracking object log



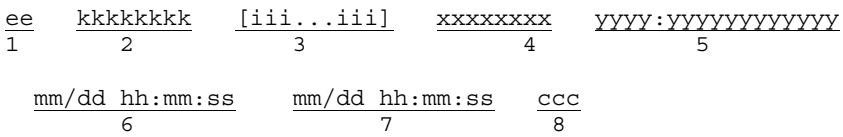
1. Log type: A 3-letter identification code applied for each provided functionality.
   - TRO: Event information for the tracking functionality of the policy-based routing
2. Time: Date and time that the event occurred.
3. Message text

1.2.4 Format of the reference log

Error information and event information related to the switch are saved as operation logs in the order they occurred, and are also saved as reference logs. Reference logs categorizes the information by message ID, and then records the event time of the first and last occurrences, and total number of occurrences.

The figure below describes the format of the reference log.

Figure 1-6: Format of the reference log



1. Event level (E9 to E3)
2. Event location or function

3. Event interface ID. Whether this information is displayed depends on the event location.
4. Message ID
5. Additional information
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.

1.2.5 Code information for logs

(1) Log type

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

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

The following table describes the correspondence between information acquired as logs and log types. Within the operation logs, event level is given to device failure and event information and reference logs.

Table 1-6: Correspondence between the information acquired as a log and log type

Information to be acquired	Log type	Description	Event level
Operational information selected by entered commands	KEY	Operational information selected by commands entered by an operator from an operation terminal	--
Event information related to command response messages	RSP	Event information related to messages output by a switch in response to commands	--
Routing protocol information	RTM	IPv4 or IPv6 routing information	--
	MRP	IPv4 multicast routing information	--
	MR6	IPv6 multicast routing information	--
Device failure and event information	ERR	Error information for a switch event location	E9 to E5
	EVT	Error information for a switch event location	E4, E3, R8 to R5
Layer 2 authentication information	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	--
DHCP snooping information	DSN	Information to be collected with DHCP snooping. Indicated as corresponding operation commands. • show ip dhcp snooping logging	--
Tracking object log **[AX3640S] [OS-L3A]**	TRO	Tracking functionality for policy-based routing	--

Legend: --: Not applicable.

(2) Event level

Events in the reference log 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	Display contents (type)	Description
9	E9 (fatal error)	This error stops the whole system. (The system might restart or operation might stop.)
8	E8 (critical error) R8 (recover from critical error)	This error stops a fan, the power, or part of the switch. • If this error is due to a hardware error, restarting the applicable hardware is involved.
7	E7 (software error) R7 (recover from software error)	This error stops part of the software.
6	E6 R6	Not used
5	E5 R5	Not used
4	E4 (network error)	Information related to lines (LAN)
3	E3 (warning)	This error is a warning.

Note that when an error whose event level is from E9 to E5 is recovered, a relevant operation message whose event level is from R8 to R5 is output. Also, when an error from E9 to E5 occurs, the operation log and reference log are automatically saved to the device memory as /usr/var/log/system.log and /usr/var/log/error.log.

(3) Event location

The reference log uses an ID to indicate the location or the functionality of the event that occurred. The following table describes the event locations.

Table 1-8: Event locations

#	ID	Event location or function
1	CONFIG	Configuration
2	ACCESS	Switch access permissions
3	IP	IP control functionality
4	VLAN	VLAN control functionality
5	MAC	MAC control functionality
6	SOFTWARE	Software control functionality
7	PORT	Port control functionality
8	ULR	Uplink redundancy control functionality
9	PS	Power control functionality
10	EQUIPMENT	Switch control functionality
11	FAN	Fan control functionality

(4) 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 1-9: Display format of the interface ID

Display format of the ID	Interface
GigabitEthernet <*nif no.*>/<*port no.*>	Ethernet interface with a maximum line speed of 1000 Mbit/s
TenGigabitEthernet <*nif no.*>/<*port no.*>	Ethernet interface with a maximum line speed of 10 Gbit/s

Legend:

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

<*port no.*>: Indicates the port number.

(5) Message identifier and additional information

This information contains a code that indicates the contents of the event that occurred. For details, see *3. Device Failure and Event Information*.

(6) Time of the first and last occurrences of the applicable event

This information indicates the time of the first and last occurrences of the applicable event.

(7) Number of occurrences of the applicable event

This information indicates the total number of occurrences of the applicable event if repeated. The total is the number of event occurrences counting 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.

1.2.6 Automatically saving and viewing logs

(1) Saving logs automatically

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 1-10: 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`

(2) Viewing logs and method for creating files

Operation logs and reference logs can be referenced by using the `show logging` command. These logs can also be retrieved as files by specifying redirection 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 1-11: 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>
>
```

(3) Acquiring logs from remote hosts

Logs can be acquired from remote hosts by using the syslog output functionality. However, the syslog output functionality might lose log information due to reasons such as frame-loss.

For details about the `syslog` output functionality, see *logging facility* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.

(4) Sending logs by using the email functionality

Log information can be sent to remote hosts or to PCs by using the email functionality. This functionality cannot receive emails. If a user replies to an email sent by this functionality, a transmission error occurs.

For details about the email functionality, see *logging email-from* in the manual *Configuration Command Reference Vol. 1 For Version 11.10* or *logging email-server* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.

Chapter

2. Routing Event Information

This chapter explains the contents of routing event information. Routing protocol event information reports the operating status of IPv4 and IPv6 routing protocols. To output messages to the operation terminal screen, use commands. Note that multicast routing protocols do not display messages but only collect them in operation logs.

2.1 IPv4 routing protocol information (RTM)

This section explains IPv4 routing protocol event information.

2.1.1 RIP

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

Table 2-1: IPv4 routing protocol (RIP) event information

#	Message text	Description
1	rip_recv_response: Bad metric (<*metric*>) for net <*destination address*> from <*source address*>	Error (remote device)
		Routing information that has an invalid metric (0, or 17 or larger) was received. [Explanation of message variables] <*metric*>: Metric of the routing information <*destination address*>: Routing information destination address <*source address*>: Source gateway [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*>	Error (remote device)
		Routing information that has an invalid network mask was received. [Explanation of message variables] <*mask*>: Routing information network mask <*destination address*>: Routing information destination address <*source address*>: Source gateway [Action] Check the unicast routing program (RIP) for the source gateway.
3	rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> - 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 [Action] Check the unicast routing program (RIP) for the source gateway.
4	rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> - reserved field not zero	Error (remote device)
		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 [Action] Check the unicast routing program (RIP) for the source gateway.

#	Message text	Description
5	rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> - 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*> - illegal authentication type rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> - illegal authentication key identifier (Key-ID <*key id*>) rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> - 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 <*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*> - 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 • `TraceOn`, `TraceOff` <*source address*>: Source gateway [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.

#	Message text	Description
9	rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> - 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*> - authentication failure [(Key-ID <*key id*>)] rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> - illegal authentication key identifier (Key-ID <*key id*>) rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> - 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 [Action] Check the unicast routing program (RIP) for the source gateway.
10	rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> - 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*> - authentication failure [(Key-ID <*key id*>)] rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> - illegal authentication type rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> - 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 <*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.

#	Message text	Description
11	rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> - 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. Note that the above number of messages includes the count of the following messages: rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> - authentication failure [(Key-ID <*key id*>)] rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> - illegal authentication type rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> - 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 <*key id*>: Key identifier [Action] Check the unicast routing program (RIP) for the source gateway.

2.1.2 OSPF [OS-L3A]

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

Table 2-2: IPv4 routing protocol (OSPF) event information

#	Message text	Description
1	OSPF SENT <*source address*> -> <*destination address*> : <*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 <*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*> failed because restart time is up.	Information (remote device)
		The helper router operations 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 [Action] Check if the neighboring router has stopped the restart operation. If it has not stopped, adjust the restart time of the neighboring router.

#	Message text	Description
3	OSPF: Helper to adjacency <*router id*> address <*address*> failed because network topology is changed.	Warning (local device or network)
		The helper router operations stopped because the topology was changed. [Explanation of message variables] <*router id*>: Neighboring router's router ID <*address*>: Neighboring router's IPv4 address [Action] None.
4	OSPF RECV [Area <*area id*>] <*source address*> -> <*destination address*> : <*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 <*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 • 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.

#	Message text	Description
		• 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 The 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. • 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 The 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*>: Routing information destination address <*mask1*>: Routing 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.

#	Message text	Description
6	OSPF: Lost adjacency <*router id*> address <*address*>(<*interface name*>) due to sequence mismatch (<*sequence1*> versus <*sequence2*>)	Warning (local device or remote device)
		The 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 <*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.

#	Message text	Description
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*>.	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 [Action] Take appropriate action by following the `rtm aborted` log.
12	OSPF: Recovered from stub router (in domain <*domain id*>).	Information (local device)
		The stub router operation will now end. [Explanation of message variables] <*domain id*>:OSPF domain ID [Action] None.

2.1.3 BGP4 [OS-L3A]

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

Table 2-3: IPv4 routing protocol (BGP4) event information

#	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.

#	Message text	Description
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: 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 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.

#	Message text	Description
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 <*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.

#	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.
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.

#	Message text	Description
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.
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 state. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Description name of the source peer <*state*>: Peer state • `Idle`, `OpenConfirm`, `Established` [Action] The connection has become unstable. If this error occurs frequently, check the cause of the instability.

#	Message text	Description
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.
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.

#	Message text	Description
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*>: Length of the sent data <*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: Peer <*bgp name*> [(<*description*>)] local address <*ipv4 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 <*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.

#	Message text	Description
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)
		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 establish 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.

#	Message text	Description
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 <*description*>: Description name of the connection target peer <*ipv4 address*>: Local address used for establish 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 receive from the relevant peer in the ESTABLISHED state. [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.

#	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 routing 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 routing 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*>: Entity 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: 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.

#	Message text	Description
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 routing 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 routing information of the UPDATE message received from the relevant peer exceeds the prefix data of unreachable routing information. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Description name of the source peer <*length1*>: Prefix length in received messages <*length2*>: Entity data length [Action] Check the unicast routing program (BGP4) in the peer.
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 routing 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.

#	Message text	Description
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 routing 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 routing 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 routing information <*mask*>: Network mask of unreachable routing 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.
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.

#	Message text	Description
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.
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.

#	Message text	Description
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.
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 relevant 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.

#	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.
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.

#	Message text	Description
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.
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.

#	Message text	Description
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.
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.

#	Message text	Description
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.
89	BGP: 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*>. <*value*>: Decimal representation <*data*>: Hexadecimal representation

#	Message text	Description
		[Action] Check the network configuration and peer configuration. If there is no problem with them, check the unicast routing program (BGP4) in the peer.
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*>. <*value*>: Decimal representation <*data*>: Hexadecimal representation [Action] Check the network configuration and peer configuration.
91	BGP:	Warning (remote device)

#	Message text	Description
	No MD5 digest from <*source ipv4*>+<*port no.*> to <*destination ipv4*>+<*port no.*>	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 when 1 or 2 above occurs. Note that the above number of messages includes 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 [Action] Check whether the MD authentication is set in BGP4 of the remote system. If it is not set, set the MD 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:	Warning (local device or remote device)
	Invalid MD5 digest from <*source ipv4*>+<*port no.*> to <*destination ipv4*>+<*port no.*>	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 when 1 or 2 above occurs. 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 [Action] Check if the MD5 authentication keys match in BGP4 of the local and remote systems. 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:	Warning (remote device)
	Number of prefix received from <*bgp name*> [(<*description*>)]: reached <*routes1*>, limit <*routes2*>	The number of paths (active paths and inactive paths) 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:	Warning (remote device)

#	Message text	Description
	Number of prefix received from <*bgp name*> [(<*description*>)]: <*routes1*> exceed limit <*routes2*>	The number of paths (active paths and inactive paths) 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*>): <*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.

2.1.4 Event information common to the IPv4 unicast routing protocols

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

Table 2-4: Event information common to unicast routing protocols

#	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.

2.2 IPv6 routing protocol information (RTM)

This section explains IPv6 routing protocol event information.

2.2.1 RIPng

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

Table 2-5: IPv6 routing protocol (RIPng) event information

#	Message text	Description
1	ripng_recv: Bad metric (<*metric*>) for net <*prefix*> from <*source address*>	Error (remote device)
		Routing information that has an invalid metric (0, or 17 or larger) was received. [Explanation of message variables] <*metric*>: Metric of the routing information <*prefix*>: Routing 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)
		Routing information that has an invalid prefix length was received. [Explanation of message variables] <*pefixlen*>: Prefix length of the routing information <*prefix*>: Routing 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.
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.

#	Message text	Description
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.
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 routing 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)
		Routing 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.

#	Message text	Description
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 RIP settings so that the maximum number of neighboring routers does not exceed the capacity limit.

2.2.2 OSPFv3 [OS-L3A]

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

Table 2-6: IPv6 routing protocol (OSPFv3) event information

#	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.
2	OSPFv3: Helper to adjacency <*router id*> failed because network topology is changed.	Warning (local device or network)
		The helper router operations stopped because the topology was changed. [Explanation of message variables] <*router id*>: Neighboring router's router ID [Action] None.
3	OSPFv3: Helper to adjacency <*router id*> failed because restart time is up.	Information (remote device)
		The helper router operations stopped because the waiting time for restart elapsed. [Explanation of message variables] <*router id*>: Neighboring router's router ID [Action] Check if the neighboring router has stopped the restart operation. 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:

#	Message text	Description
		• 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 • 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 The 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.

#	Message text	Description
		• DD: MTU mismatch An attempt to exchange routing 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 The neighboring router is sending an invalid packet. Check the unicast routing program (OSPFv3) of the neighboring router.
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*>: Routing information destination address <*prefixlen* >: Prefix length of the routing 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`).

#	Message text	Description
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 <*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)
		The 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*>.	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 [Action] Take appropriate action by following the `rtm aborted` log.
12	OSPFv3: Recovered from stub router (in domain <*domain id*>).	Information (local device)
		The stub router operation will now end. [Explanation of message variables] <*domain id*>: OSPFv3 domain ID [Action] None.

2.2.3 BGP4+ [OS-L3A]

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

Table 2-7: IPv6 routing protocol (BGP4+) event information

#	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 was 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.

#	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.
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.

#	Message text	Description
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: 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	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.

#	Message text	Description
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 <*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+.

#	Message text	Description
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 state. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Description name of the source peer <*state*>: Peer state • `Idle`, `OpenConfirm`, `Established` [Action] The connection has become unstable. If this error occurs frequently, check the cause of the instability.
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.

#	Message text	Description
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 <*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*>: Length of the sent data <*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.

#	Message text	Description
32	bgp4+_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	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] <*error string*>: Error cause [Action] Take appropriate action by following the `rtm aborted` log.

#	Message text	Description
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 establish 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 establish 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 <*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.

#	Message text	Description
44	bgp4+_recv _update: Received OPEN message from <*bgp name*> [(<*description*>)], state is ESTABLISHED	Warning (remote device or network)
		An OPEN message was receive from the relevant peer in the ESTABLISHED state. [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 routing 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 routing information in the received message <*length2*>: Received packet length [Action] Check the unicast routing program (BGP4+) in the peer.
47	bgp4+_recv_update: Peer <*bgp name*> [(<*description*>)] UPDATE unreachable prefix length <*length*> too long	Error (remote device)
		The prefix length of unreachable routing 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 routing information of the UPDATE message received from the relevant peer exceeds the prefix data of unreachable routing information. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Description name of the source peer <*length1*>: Prefix length in received messages <*length2*>: Entity data length [Action] Check the unicast routing program (BGP4+) in the peer.

#	Message text	Description
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*>: Entity data length [Action] Check the unicast routing program (BGP4+) in the peer.
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 routing 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.

#	Message text	Description
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.
56	bgp4+_recv_update: Ignores prefix from peer <*bgp name*> [(<*description*>)] in RFC-1771's NLRI field	Warning (remote device)
		Routing 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.

#	Message text	Description
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.
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*>: Entity 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.

#	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)
		Routing 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 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.
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 routing information of the `UPDATE` message from the relevant peer exceeds the data length of remaining unreachable routing 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.

#	Message text	Description
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 routing 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 routing 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.
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.

#	Message text	Description
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.
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.

#	Message text	Description
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.
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:

#	Message text	Description
		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.
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:

#	Message text	Description
		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*>. <*value*>: Decimal representation <*data*>: Hexadecimal representation [Action] Check the network configuration and peer configuration.
87	BGP4+: No MD5 digest from <*source ipv6*>+<*port no.*> to <*destination ipv6*>+<*port no.*>	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 when 1 or 2 above occurs. 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.*>.

#	Message text	Description
		[Explanation of message variables] <*source ipv6*>: Source IPv6 address <*port no.*>: TCP port number <*destination ipv6*>: Destination IPv6 address [Action] Check whether the MD authentication is set in BGP4+ of the remote system. If it is not set, set the MD 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.*>	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 when 1 or 2 above occurs. 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 <*port no.*>: TCP port number [Action] Check if the MD5 authentication keys match in BGP4+ of the local and remote systems. 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 paths and inactive paths) 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 paths and inactive paths) 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.

#	Message text	Description
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.
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.

2.2.4 Event information common to the IPv6 unicast routing protocols

See *2.1.4 Event information common to the IPv4 unicast routing protocols*.

2.3 IPv6 routing information (RTM)

2.3.1 RA

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

Table 2-8: IPv6 routing (RA) event information

#	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.
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.

#	Message text	Description
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	ra_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.
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.

2.4 IPv4 multicast routing information (MRP)

2.4.1 PIM-SM

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

Table 2-9: IPv4 multicast routing (PIM-SM) event information

#	Message text	Description
1	IGMP: received packet too short (<*length*> bytes) for IP header	Error (remote device)
		A packet smaller than the IP header was received. [Explanation of message variables] <*length*>: Received packet size [Action] A remote device is sending an invalid packet. Check the IPv4 multi-cast communication program of the partner device.
2	IGMP: received packet (<*length1*> bytes) from <*source address*> shorter than header + data length (<*length2*> + <*length3*> bytes)	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 [Action] A remote device is sending an invalid packet. Check the IPv4 multi-cast communication program of the partner device.
3	IGMP: received IP data field too short (<*length*> bytes) for IGMP header, from <*source address*> to <*destination address*>	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 [Action] A remote device is sending an invalid packet. Check the IPv4 multi-cast communication program of the partner device.
4	IGMP: ignoring packet from <*source address*> to <*destination address*> - 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 <*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 partner device.

#	Message text	Description
5	IGMP: ignoring <*packet*> from <*source address*> to <*destination address*> - 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 <*group address*>: Received group address [Action] A remote device is sending an invalid packet. Check the IPv4 multi-cast communication program of the partner device.
6	IGMP: Querier was changed on interface <*interface name*> - 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 <*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	Error (remote device)
		A packet smaller than the IP header was received. [Explanation of message variables] <*length*>: Received packet size [Action] A remote device is sending an invalid packet. Check the IPv4 multicast routing program (PIM-SM) of the remote device.
8	PIM: received packet (<*length1*> bytes) from <*source address*> shorter than header + data length (<*length2*> + <*length3*> bytes)	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 [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*>	Error (remote device)
		A packet smaller than the 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 [Action] A remote device is sending an invalid packet. Check the IPv4 multicast routing program (PIM-SM) of the remote device.

#	Message text	Description
10	PIM: ignoring packet from <*source address*> to <*destination address*> - invalid pim header checksum (data '<*data*>', length '<*length*>')	Error (remote device)
		A received PIM packet was ignored because of a PIM header checksum error. [Explanation of message variables] <*source address*>: Source IPv4 address <*destination address*>: Destination IPv4 address <*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*> - 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 • `Register`, `Register-Stop`, `Join/Prune`, `Assert`, `Bootstrap`, `Candidate-RP-Advertisement` <*source address*>: Source IPv4 address <*destination address*>: Destination IPv4 address <*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*> - 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 <*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 neighboring 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.

#	Message text	Description
13	PIM: ignoring <*packet*> message from <*source address*> to <*destination address*> - 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 <*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*> - 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 <*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*> - 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 <*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.

#	Message text	Description
16	PIM: ignoring Hello message from <*source address*> - 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 [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*> - 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 <*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*> - 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 <*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*> - 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 <*value*>: Hash mask length specified for the received packet [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 - lost BSR information	Warning (remote device)
		BSR information was cleared because advertisements from the Bootstrap router were lost. [Explanation of message variables] None. [Action] Check the reason why advertisements from the Bootstrap router were lost.

#	Message text	Description
21	PIM: BSR information was changed - new BSR address <*ip address*>	Event (local device)
		BSR address was changed. [Explanation of message variables] <*ip address*>: BSR address If the BSR address is the Switch, `(this system)` is displayed after the IPv4 address. [Action] None.

2.5 IPv6 multicast routing information (MR6)

2.5.1 IPv6 PIM-SM

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

Table 2-10: IPv6 multicast routing (PIM-SM) event information

#	Message text	Description
1	MLD: ignoring <*packet*> from <*source address*> - 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 <*group address*>: MLD group address [Action] A remote device is sending an invalid packet. Check the IPv6 multi-cast communication program of the partner device.
2	MLD: ignoring <*packet*> from <*source address*> - 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 [Action] A remote device is sending an invalid packet. Check the IPv6 multi-cast communication program of the partner device.
3	MLD: Querier was changed on interface <*interface name*> - 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 <*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.

#	Message text	Description
4	PIM: ignoring <*packet*> message from <*source address*> - 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 <*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*> - 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 <*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.
6	PIM: ignoring <*packet*> message from <*source address*> - 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 <*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.

#	Message text	Description
7	PIM: ignoring <*packet*> message from <*source address*> - 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 <*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*> - 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 IPv6 address <*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*> - 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 IPv6 address [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*> - 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 <*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.

#	Message text	Description
11	PIM: ignoring Register message from <*source address*> - 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 <*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.
12	PIM: ignoring Register message from <*source address*> - 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 <*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*> - 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 <*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*> - 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 <*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*> - 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 <*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.

#	Message text	Description
16	PIM: ignoring Bootstrap message from <*source address*> - 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 <*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*> - 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 <*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*> - 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 <*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 - lost BSR information	Warning (remote device)
		BSR information was cleared because advertisements from the Bootstrap router were lost. [Explanation of message variables] None. [Action] Check the reason why advertisements from the Bootstrap router were lost.
20	PIM: BSR information was changed - new BSR address <*ipv6 address*>	Event (local device)
		BSR address was changed. [Explanation of message variables] <*ipv6 address*>: BSR address If the BSR address is the Switch, `(this system)` is displayed after the IPv6 address. [Action] None.

#	Message text	Description
21	PIM: Add interface <*interface name*> 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 <*source address*>: Source IPv6 address <*group address*>: IPv6 group address [Action] None.
22	PIM: Delete interface <*interface name*> 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 <*source address*>: Source IPv6 address <*group address*>: IPv6 group address [Action] None.

Chapter

3. Device Failure and Event Information

This chapter describes the contents of device failure and event information. All messages for device failure and event information are output to the operation terminal screen. Depending on the error severity or event contents, the information is classified into seven event levels, ranging from `E3` to `E9`. 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.

3.1 Configuration

3.1.1 Event location = CONFIG

The following table describes device failure and event information when the event location is `CONFIG`.

Table 3-1: Device failure and event information when the event location is CONFIG

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
1	E3	CONFIG	09300001	0100	This system started with the default configuration file. because the startup configuration file is not found or broken.
	Operation started with the default settings because there is no startup configuration file or it cannot be read. [Explanation of message variables] None. [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.				
2	E3	CONFIG	09300002	0100	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. [Explanation of message variables] <*line number*>: Line number of the target configuration command <*error syntax*>: Syntax of the target configuration command [Action] Check the contents of the error.				
3	E3	CONFIG	09300007	0100	Configuration edit status forcedly finished.
	The configuration status was forced to switch from editable status to editing-completed status. [Explanation of message variables] None. [Action] Have all users in the configuration command mode exit from the configuration command mode, and then restart the editing.				
4	E3	CONFIG	09300008	0100	Cannot set the automatic setting configuration command.:<*command*>
	Automatic setting of the configuration command failed. [Explanation of message variables] <*command*>: Command name [Action] Manually set the corresponding command.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
5	E3	CONFIG	09600006	0100	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. [Explanation of message variables] <*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.				

3.2 Access

3.2.1 Event location = ACCESS

The following table describes device failure and event information when the event location is `ACCESS`.

Table 3-2: Device failure and event information when the event location is ACCESS

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
1	E3	ACCESS	00000001	0201 0205	Unknown host address <*ip address*>.
	An attempt to connect via telnet or FTP from <*ip address*> was not permitted. [Explanation of message variables] <*ip address*>: IPv4 address or IPv6 address [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.				
2	E3	ACCESS	00000002	0201 0205	Login incorrect <*user name*>.
	An attempt to log in by using the <*user name*> account was made, but the login was not allowed. [Explanation of message variables] <*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/`)				
3	E3	ACCESS	00000003	0201 0205	Login refused for too many users logged in.
	An attempt to connect via telnet was refused because too many users are logged in. [Explanation of message variables] None. [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.				

<table>
<tr><th rowspan="2">#</th><th>Event level</th><th>Event location</th><th>Message ID</th><th>Added info
Highest 4 digits</th><th>Message text</th></tr>
<tr><th colspan="5">Description</th></tr>
<tr><td rowspan="2">4</td><td>E3</td><td>ACCESS</td><td>00005002</td><td>0200</td><td>Login <<i>user name</i>> from <<i>host</i>> (<<i>term</i>>).</td></tr>
<tr><td colspan="5">A user logged in.
[Explanation of message variables]
<<i>user name</i>>: User name
<<i>host</i>>: Host ID
• For a remote operation terminal: IPv4 or IPv6 address
• For a console terminal: console
<<i>term</i>>: Terminal name
• For a remote operation terminal: ttyp0 or higher
• For a console terminal: tty00
[Action]
None.</td></tr>
<tr><td rowspan="2">5</td><td>E3</td><td>ACCESS</td><td>00005003</td><td>0200</td><td>Logout <<i>user name</i>> from <<i>host</i>> (<<i>term</i>>).</td></tr>
<tr><td colspan="5">A user logged out.
[Explanation of message variables]
<<i>user name</i>>: User name
<<i>host</i>>: Host ID
• For a remote operation terminal: IPv4 or IPv6 address
• For a console terminal: console
<<i>term</i>>: Terminal name
• For a remote operation terminal: ttyp0 or higher
• For a console terminal: tty00
[Action]
None.</td></tr>
<tr><td rowspan="2">6</td><td>E3</td><td>ACCESS</td><td>00010001</td><td>0204</td><td>SNMP agent program received packet from <<i>ip address</i>> with unexpected community name <<i>community name</i>>.</td></tr>
<tr><td colspan="5">The SNMP agent received a packet that had the unexpected community name <<i>community name</i>> from <<i>ip address</i>>.
[Explanation of message variables]
<<i>ip address</i>>: IPv4 or IPv6 address of the SNMP manager
<<i>community name</i>>: 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 <<i>ip address</i> >and <<i>community name</i>>. 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 <<i>ip address</i>>.
The Switch suppresses repeated output to the operation log of accesses from an invalid IP address or community. A maximum of 16 invalid IP address are saved and, for each saved IP address, one out of every 128 invalid access attempts is output to the log.</td></tr>
</table>

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
7	E3	ACCESS	00030001	0201 0205 0208 0209	Local authentication succeeded.
	Local authentication was performed and was successful for a user login request or request to change the administrator mode (`enable` command). [Explanation of message variables] None. [Action] None.				
8	E3	ACCESS	00030002	0201 0205 0208 0209	Local authentication failed.
	Local authentication was performed but authentication failed for a user login request or request to change the administrator mode (`enable` command). [Explanation of message variables] None. [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.				
9	E3	ACCESS	00030003	0201 0205 0208 0209	RADIUS authentication accepted from <*host*>.
	RADIUS authentication was performed successfully for a user login request or request to change the administrator mode (`enable` command). [Explanation of message variables] <*host*>: IP address or host name of the RADIUS server [Action] None.				
10	E3	ACCESS	00030004	0201 0205 0208 0209	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). [Explanation of message variables] <*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.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
11	E3	ACCESS	00030005	0201 0205 0208 0209	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. [Explanation of message variables] <*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.				
12	E3	ACCESS	00030006	0201 0205 0208 0209	RADIUS server configuration 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. [Explanation of message variables] None. [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.				
13	E3	ACCESS	00030007	0201 0205 0208 0209	Invalid response received from <*host*>.
	RADIUS or TACACS+ authentication was attempted for a user login request or request to change the administrator mode (`enable` command), but the response from RADIUS or TACACS+ server was invalid. [Explanation of message variables] <*host*>: IP address or host name of RADIUS or TACACS+ server [Action] Make sure that the same RADIUS or TACACS+ key is specified for the Switch and the RADIUS or TACACS+ server.				
14	E3	ACCESS	00030008	0201 0205 0208 0209	RADIUS authentication failed.
	RADIUS authentication failed for a user login request or request to change the administrator mode (`enable` command) [Explanation of message variables] None. [Action] If any other operation log messages for RADIUS authentication were output, refer to them.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
15	E3	ACCESS	0003000a	0201 0205 0208 0209	Can't communicate with RADIUS server (<*host*>).
	Communication with the RADIUS server failed. [Explanation of message variables] <*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.				
16	E3	ACCESS	0003000b	0201 0208	RADIUS authorization response with no contents.
	RADIUS command authorization was performed, but a command list was not properly obtained from the RADIUS server. [Explanation of message variables] None. [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).				
17	E3	ACCESS	00030013	0201 0205 0208 0209	TACACS+ authentication accepted from <*host*>.
	TACACS+ authentication was successfully performed for a user login request or request to change the administrator mode (`enable` command). [Explanation of message variables] <*host*>: IP address or host name of the TACACS+ server [Action] None.				
18	E3	ACCESS	00030014	0201 0205 0208 0209	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. [Explanation of message variables] <*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.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
19	E3	ACCESS	00030015	0201 0205 0208 0209	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. [Explanation of message variables] <*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.				
20	E3	ACCESS	00030016	0201 0205 0208 0209	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. [Explanation of message variables] None. [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.				
21	E3	ACCESS	00030018	0201 0205 0208 0209	TACACS+ authentication failed.
	TACACS+ authentication failed for a user login request or request to change the administrator mode (`enable` command). [Explanation of message variables] None. [Action] If any other operation log messages were output for TACACS+ authentication, refer to them.				
22	E3	ACCESS	0003001a	0201 0205 0208 0209	Can't communicate with TACACS+ server (<*host*>).
	Communication with the TACACS+ server failed. [Explanation of message variables] <*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.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
23	E3	ACCESS	0003001b	0201 0208	TACACS+ authorization response with no contents.
	TACACS+ command authorization was performed but a command list was not properly obtained from the TACACS+ server. [Explanation of message variables] None. [Action] Make sure that `class`, `allow-commands`, and `deny-commands` are properly set in the TACACS+-server settings (vendor-specific setting for the Switch).				
24	E3	ACCESS	0003001c	0201 0208	TACACS+ authorization 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. [Explanation of message variables] <*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.				
25	E3	ACCESS	0003001d	0201 0208	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. [Explanation of message variables] None. [Action] Make sure that settings for the command class (`username view-class`) and the command list (`username view`, `parser view`, `commands exec`) are set correctly for users authenticated using local login.				

3.3 Protocol

3.3.1 Event location = IP

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

Table 3-3: Device failure and event information when the event location is IP

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
1	E4	IP	26000001	0600	The ARP entry can't be registered at hardware tables. (<*ipv4 address*>)
	An ARP entry cannot be registered in the hardware tables. [Explanation of message variables] <*ipv4 address*>: IPv4 address of the ARP entry that cannot be registered in the hardware tables [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.				
2	E4	IP	26000002	0600	The ARP entry can't be deleted from hardware tables.
	An ARP entry cannot be deleted from the hardware tables. [Explanation of message variables] None. [Action] Replace the Switch.				
3	E4	IP	26000003	0600	The NDP entry can't be registered at hardware tables. (<*ipv6 address*>)
	An NDP entry cannot be registered in the hardware tables. [Explanation of message variables] <*ipv6 address*>: IPv6 address of NDP entry that cannot be registered in the hardware tables [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.				
4	E4	IP	26000004	0600	The NDP entry can't be deleted from hardware tables.
	An NDP entry cannot be deleted from the hardware tables. [Explanation of message variables] None. [Action] Replace the Switch.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
5	E4	IP	26000005	0600	IPv4 unicast routing information can't be registered at hardware tables. (<*ipv4 prefix*>/<*masklen*>)
	An IPv4 unicast routing table entry cannot be registered in the hardware tables. [Explanation of message variables] <*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 [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.				
6	E4	IP	26000006	0600	IPv4 unicast routing information can't be deleted from hardware tables.
	An IPv4 unicast routing table entry cannot be deleted from the hardware tables. [Explanation of message variables] None. [Action] Replace the Switch.				
7	E4	IP	26000007	0600	IPv4 multicast routing information can't be registered at hardware tables. (Source:<*ipv4 address*> Group:<*ipv4 address*>)
	An IPv4 multicast routing table entry cannot be registered in the hardware tables. [Explanation of message variables] <*ipv4 address*>: Source IPv4 address and group address of the IPv4 multicast routing table entry that cannot be registered in the hardware tables [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.				
8	E4	IP	26000008	0600	IPv4 multicast routing information can't be deleted from hardware tables.
	An IPv4 multicast routing table entry cannot be deleted from the hardware tables. [Explanation of message variables] None. [Action] Replace the Switch.				
9	E4	IP	26000009	0600	IPv6 unicast routing information can't be registered at hardware tables. (<*ipv6 prefix*>/<*prefixlen*>)
	An IPv6 unicast routing table entry cannot be registered in the hardware tables. [Explanation of message variables] <*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 [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.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
10	E4	IP	2600000a	0600	IPv6 unicast routing information can't be deleted from hardware tables.
	An IPv6 unicast routing table entry cannot be deleted from the hardware tables. [Explanation of message variables] None. [Action] Replace the Switch.				
11	E4	IP	2600000b	0600	IPv6 multicast routing information can't be registered at hardware tables. (Source:<*ipv6 address*> Group:<*ipv6 address*>)
	An IPv6 multicast routing table entry cannot be registered in the hardware tables. [Explanation of message variables] <*ipv6 address*>: Source address and group address of the IPv6 multicast routing table entry that cannot be registered in the hardware tables [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.				
12	E4	IP	2600000c	0600	IPv6 multicast routing information can't be deleted from hardware tables.
	An IPv6 multicast routing table entry cannot be deleted from the hardware tables. [Explanation of message variables] None. [Action] Replace the Switch.				
13	E4	IP	2600000d	0600	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. [Explanation of message variables] <*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.				
14	E4	IP	50000003	0600	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*>. [Explanation of message variables] <*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.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
15	E4	IP	50000006	0600	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. [Explanation of message variables] None. [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.				
16	E4	IP	50000013	0600	The number of pieces of the IPv4 unicast routing information exceeds the capacity of this system.
	The number of IPv4 unicast routing information entries exceeds the capacity limit of the Switch. [Explanation of message variables] None. [Action] 1. Delete unnecessary information from the IPv4 unicast routing information. 2. Review the network system configuration, and change it to a new system configuration by reducing IPv4 unicast routing information. 3. After implementing (1) or (2), specify `*` for the `clear ip route` command.				
17	E4	IP	51000006	0600	The number of pieces of the IPv4 Multicast Routing entry exceeds the capacity of this system.
	The number of IPv4 multicast routing information entries exceeds the capacity limit of the Switch. [Explanation of message variables] None. [Action] 1. Delete unnecessary information from the IPv4 multicast routing information. 2. Review the network system configuration, and change it to a new system configuration by reducing the IPv4 multicast routing information.				
18	E4	IP	60000002	0600	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. [Explanation of message variables] None. [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.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
19	E4	IP	60000003	0600	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. [Explanation of message variables] <*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 device. 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.				
20	E4	IP	60000008	0600	The number of pieces of the IPv6 unicast routing information exceeds the capacity of this system.
	The number of IPv6 unicast routing information entries exceed the capacity limit of the Switch. [Explanation of message variables] None. [Action] 1. Delete unnecessary information from the IPv6 unicast routing information. 2. Review the network system configuration, and change it to a new system configuration by reducing the IPv6 unicast routing information. 3. After implementing (1) or (2), specify `*` for the `clear ipv6 route` command.				
21	E4	IP	61000005	0600	The number of pieces of the IPv6 Multicast Routing entry exceeds the capacity of this system.
	The number of IPv6 multicast routing information entries exceed the capacity limit of the Switch. [Explanation of message variables] None. [Action] 1. Delete unnecessary information from the IPv6 multicast routing information. 2. Review the network system configuration, and change it to a new system configuration by reducing the IPv6 multicast routing information.				

3.3.2 Event location = VLAN

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

Table 3-4: Device failure and event information when the event location is VLAN

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
1	E3	VLAN	20110002	0700	STP(<*mode*>): This bridge becomes the Root Bridge.
	The Switch has become the root bridge. [Explanation of message variables] <*mode*>: Spanning Tree type • `single`: Single Spanning Tree • `PVST+:VLAN` <*vlan id*>: PVST+ Spanning Tree Protocol and VLAN ID [Action] None.				
2	E3	VLAN	20110003	0700	STP(<*mode*>): This bridge becomes the Designated Bridge.
	The Switch has become the designated bridge. [Explanation of message variables] <*mode*>: Spanning Tree type • `single`: Single Spanning Tree • `PVST+:VLAN` <*vlan id*>: PVST+ Spanning Tree Protocol and VLAN ID [Action] None.				
3	E3	VLAN	20110006	0700	STP(<*mode*>): Topology change detected - BPDU Timeout detected on the root port(<*nif no.*>/<*port no.*>).
	A BPDU timeout was detected on the root port. [Explanation of message variables] <*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 <*nif no.*>/<*port no.*>: NIF number/port number [Action] Check the line status.				
4	E3	VLAN	20110007	0700	STP(<*mode*>): Topology change detected - Topology Change Notification BPDU received on the port(<*nif no.*>/<*port no.*>).
	A topology change BPDU has been received. [Explanation of message variables] <*mode*>: Spanning Tree type • `single`: Single Spanning Tree • `PVST+:VLAN` <*vlan id*>: PVST+ Spanning Tree Protocol and VLAN ID • `MST`: Multiple Spanning Tree <*nif no.*>/<*port no.*>: NIF number/port number [Action] Check the line status.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
5	E3	VLAN	20110011	0700	STP(<*mode*>): Spanning Tree Protocol enabled - BPDU received on the Port Fast(<*nif no.*>/<*port no.*>).
	A port has become subject to the Spanning Tree Protocol because the port was set with the `PortFast` function and received a BPDU. [Explanation of message variables] <*mode*>: Spanning Tree type • `single`: Single Spanning Tree • `PVST+:VLAN` <*vlan id*>: PVST+ Spanning Tree Protocol and VLAN ID • `MST`: Multiple Spanning Tree <*nif no.*>/<*port no.*>: NIF number/port number [Action] Check the line status.				
6	E3	VLAN	20110012	0700	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. [Explanation of message variables] <*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.				
7	E3	VLAN	20110013	0700	STP (<*mode*>) : Topology change detected - Topology Change Notification BPDU received on the port(ChGr:<*channel group number*>).
	A topology change BPDU has been received. [Explanation of message variables] <*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.				
8	E3	VLAN	20110014	0700	STP (<*mode*>) : Spanning Tree Protocol enabled - BPDU received on the Port Fast(ChGr:<*channel group number*>).
	A port has become subject to the Spanning Tree Protocol because the port was set with the `PortFast` function and received a BPDU. [Explanation of message variables] <*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.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
9	E3	VLAN	20110022	0700	STP : Cleared MAC Address Table entry.
	A MAC Address Table entry was cleared because a topology change BPDU was received. [Explanation of message variables] None. [Action] None.				
10	E3	VLAN	20110023	0700	STP(<*mode*>): Topology change detected - BPDU Timeout detected on the alternate port(<*nif no.*>/<*port no.*>).
	A BPDU timeout was detected on the alternate port. [Explanation of message variables] <*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 <*nif no.*>/<*port no.*>: NIF number/port number [Action] Check the line status.				
11	E3	VLAN	20110024	0700	STP(<*mode*>): Topology change detected - BPDU Timeout detected on the backup port(<*nif no.*>/<*port no.*>).
	A BPDU timeout was detected on the backup port. [Explanation of message variables] <*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 <*nif no.*>/<*port no.*>: NIF number/port number [Action] Check the line status.				
12	E3	VLAN	20110025	0700	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. [Explanation of message variables] <*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.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
13	E3	VLAN	20110026	0700	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. [Explanation of message variables] <*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.				
14	E3	VLAN	20110027	0700	STP(MST): This bridge becomes the CIST Root Bridge.
	The Switch has become the CIST root bridge. [Explanation of message variables] None. [Action] None.				
15	E3	VLAN	20110028	0700	STP(CIST): This bridge becomes the CIST Regional Root Bridge.
	The Switch has become the CIST regional root bridge. [Explanation of message variables] None. [Action] None.				
16	E3	VLAN	20110029	0700	STP(MST Instance <*mst instance id*>): This bridge becomes the MSTI Regional Root Bridge.
	The Switch has become the MSTI regional root bridge. [Explanation of message variables] <*mst instance id*>: MST instance ID [Action] None.				
17	E3	VLAN	20110031	0700	STP(CIST): This bridge becomes the CIST Regional Designated Bridge.
	The Switch has become the CIST regional designated bridge. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
18	E3	VLAN	20110032	0700	STP(MST Instance <*mst instance id*>): This bridge becomes the MSTI Regional Designated Bridge.
	The Switch has become the MSTI regional designated bridge. [Explanation of message variables] <*mst instance id*>: MST instance ID [Action] None.				
19	E3	VLAN	21100001	0700	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. [Explanation of message variables] <*vlan id*>: VLAN ID <*ipv4 address*>: IPv4 address [Action] 1. Check the connection with the IGMP querier <*ipv4 address*>. 2. Check if the GMP querier change message (message ID is 21100002) was output. 3. If the connection with the IGMP querier cannot be checked, execute the configuration command `ip igmp snooping querier` to enable the IGMP querier function of the Switch.				
20	E3	VLAN	21100002	0700	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*>). [Explanation of message variables] <*vlan id*>: VLAN ID <*ipv4 address*>: IPv4 address [Action] None.				
21	E3	VLAN	21100003	0700	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. [Explanation of message variables] <*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.				
22	E3	VLAN	21100004	0700	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 (maximum: 500) of the switch. [Explanation of message variables] None. [Action] The number of entries exceeds the capacity limit. Review the system configuration and setting so that you can reduce the number of entries.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
23	E3	VLAN	20110042	0700	STP (<*mode*>) : Topology change detected - BPDU Timeout detected on the root port(VLID:<*link id*>).
	A BPDU timeout was detected on the root port. [Explanation of message variables] <*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.				
24	E3	VLAN	20110043	0700	STP (<*mode*>) : Topology change detected - Topology Change Notification BPDU received on the port(VLID:<*link id*>).
	A topology change BPDU has been received. [Explanation of message variables] <*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.				
25	E3	VLAN	20110044	0700	STP (<*mode*>) : Topology change detected - BPDU Timeout detected on the alternate port(VLID:<*link id*>).
	A BPDU timeout was detected on the alternate port. [Explanation of message variables] <*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.				
26	E3	VLAN	20110045	0700	STP (<*mode*>) : Topology change detected - BPDU Timeout detected on the backup port(VLID:<*link id*>).
	A BPDU timeout was detected on the backup port. [Explanation of message variables] <*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.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
27	E3	VLAN	20130019	0700	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. [Explanation of message variables] <*port list*>: Port range <*mac address*>: Device MAC address of the frame-sending source [Action] None.				
28	E3	VLAN	21200001	0700	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. [Explanation of message variables] <*vlan id*>: VLAN ID <*ipv6 address*>: IPv6 address [Action] 1. Check the connection with the MLD querier at <*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 configuration command `ipv6 mld snooping querier` to enable the MLD querier function of the Switch.				
29	E3	VLAN	21200002	0700	MLD snooping: MLD querier changed on VLAN <*vlan id*> - new MLD querier address <*ipv6 address*>.
	The MLD querier was changed to <*ipv6 address*> because a new MLD querier was identified on the VLAN (<*vlan id*>). [Explanation of message variables] <*vlan id*>: VLAN ID <*ipv6 address*>: IPv6 address [Action] None.				
30	E3	VLAN	21200003	0700	MLD snooping: IPv6 address not defined on VLAN <*vlan id*>, MLD querier function stopped.
	The MLD querier on VLAN (<*vlan id*>) was stopped because the IPv6 address was not set. [Explanation of message variables] <*vlan id*>: VLAN ID [Action] 1. Set the IPv6 address for the appropriate VLAN. 2. Execute the `show mld-snooping` command to check that the IPv6 address set for the appropriate VLAN is displayed.				
31	E3	VLAN	21200004	0700	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 (maximum: 500) of the switch. [Explanation of message variables] None. [Action] The number of entries exceeds the capacity limit. Review the system configuration and setting so that you can reduce the number of entries.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
32	E3	VLAN	2510001b	0700	Sum of number of VLAN on ports exceeded capacity.
	The total number of VLANs for each port exceed the capacity limit. [Explanation of message variables] None. [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 switch.				
33	E4	VLAN	20110008	0700	STP(<*mode*>): Port status becomes Forwarding on the port(<*nif no.*>/<*port no.*>).
	The port was placed in the forwarding status. [Explanation of message variables] <*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 <*nif no.*>/<*port no.*>: NIF number/port number [Action] None.				
34	E4	VLAN	20110009	0700	STP(<*mode*>): Port status becomes Blocking on the port(<*nif no.*>/<*port no.*>).
	The port was placed in the blocking status. [Explanation of message variables] <*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 <*nif no.*>/<*port no.*>: NIF number/port number [Action] None.				
35	E4	VLAN	20110010	0700	STP(<*mode*>): Port status becomes Down- BPDU received on the BPDU GUARD port(<*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. [Explanation of message variables] <*mode*>: Spanning Tree type • `single`: Single Spanning Tree • `PVST+:VLAN` <*vlan id*>: PVST+ Spanning Tree Protocol and VLAN ID • `MST`: Multiple Spanning Tree <*nif no.*>/<*port no.*>: NIF number/port number [Action] Check the line status.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
36	E4	VLAN	20110015	0700	STP (<*mode*>) : Port status becomes Forwarding on the port(ChGr:<*channel group number*>).
	The port was placed in the forwarding status. [Explanation of message variables] <*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.				
37	E4	VLAN	20110016	0700	STP (<*mode*>) : Port status becomes Blocking on the port(ChGr:<*channel group number*>).
	The port was placed in the blocking status. [Explanation of message variables] <*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.				
38	E4	VLAN	20110017	0700	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. [Explanation of message variables] <*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.				
39	E4	VLAN	20110037	0700	STP (<*mode*>) : Port status becomes Blocking on the port(<*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. [Explanation of message variables] <*mode*>: Spanning Tree type • `PVST+:VLAN` <*vlan id*>: PVST+ Spanning Tree Protocol and VLAN ID <*nif no.*>/<*port no.*>: NIF number/port number [Action] Check the settings of the remote device.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
40	E4	VLAN	20110038	0700	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. [Explanation of message variables] <*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 remote device.				
41	E4	VLAN	20110039	0700	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. [Explanation of message variables] None. [Action] Either review the network configuration, or use Single Spanning Tree or Multiple Spanning Tree.				
42	E4	VLAN	20110040	0700	STP(<*mode*>): Port status becomes Blocking - BPDU that priority is high was received on the ROOT GUARD port(<*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. [Explanation of message variables] <*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 <*nif no.*>/<*port no.*>: NIF number/port number [Action] Check the settings of the remote device.				
43	E4	VLAN	20110041	0700	STP(<*mode*>): Port status becomes Blocking - BPDU that priority is high was received on the ROOT GUARD port(ChGr:<*channel group number*>).
	A port was placed in the `Blocking` status because it was set with the root guard function and received a high-priority BPDU. [Explanation of message variables] <*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 remote device.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
44	E4	VLAN	20110047	0700	STP (<*mode*>) : Port status becomes Forwarding on the port(VLID:<*link id*>).
	The port was placed in the forwarding status. [Explanation of message variables] <*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.				
45	E4	VLAN	20110048	0700	STP (<*mode*>) : Port status becomes Blocking on the port(VLID:<*link id*>).
	The port was placed in the blocking status. [Explanation of message variables] <*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.				
46	E4	VLAN	21100005	0700	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. [Explanation of message variables] <*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.				
47	E4	VLAN	21200005	0700	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. [Explanation of message variables] <*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.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
48	E4	VLAN	25100001	0700	VLAN (<*vlan id*>) Status is Up.
	The VLAN status is UP. [Explanation of message variables] <*vlan id*>: VLAN ID [Action] None.				
49	E4	VLAN	25100002	0700	VLAN (<*vlan id*>) Status is Down.
	The VLAN status is DOWN. [Explanation of message variables] <*vlan id*>: VLAN ID [Action] Each line status check that belongs to VLAN.				
50	E4	VLAN	25100005	0700	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. [Explanation of message variables] <*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.				
51	E4	VLAN	25100006	0700	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. [Explanation of message variables] <*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.				
52	E4	VLAN	25100007	0700	Protocol based VLAN (<*vlan id*>) registration failed on the port(<*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. [Explanation of message variables] <*vlan id*>: VLAN ID <*nif no.*>/<*port no.*>: NIF number/port number [Action] Review the system configuration.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
53	E4	VLAN	25100008	0700	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. [Explanation of message variables] <*vlan id*>: VLAN ID [Action] Review the system configuration.				
54	E4	VLAN	25100021	0700	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. [Explanation of message variables] <*protocol name*>: Name of the protocol that you are attempting to add <*vlan id*>: VLAN ID [Action] Review the system configuration.				
55	E4	VLAN	25100022	0700	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. [Explanation of message variables] <*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.				

3.3.3 Event location = VLAN (Ring Protocol)

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

Table 3-5: Device failure and event information when the event location is VLAN (Ring Protocol)

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
1	E3	VLAN	20170001	0700	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 operation mode of the `Ring Protocol` configuration to the master mode. [Explanation of message variables] <*ring id*>: Ring ID [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
2	E3	VLAN	20170002	0700	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. [Explanation of message variables] <*ring id*>: Ring ID [Action] None.				
3	E3	VLAN	20170003	0700	AXRP <*ring id*> : cleared MAC address table by receiving flush request frames.
	A flush control frame was received, and the MAC address table was cleared. The switch outputs this message when it clears a MAC address table whose output target is a ring port. [Explanation of message variables] <*ring id*>: Ring ID [Action] None.				
4	E3	VLAN	20170005	0700	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. [Explanation of message variables] <*ring id*>: Ring ID [Action] None.				
5	E3	VLAN	20170014	0700	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. [Explanation of message variables] <*link id*>: Virtual link ID [Action] None.				
6	E3	VLAN	20170016	0700	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. [Explanation of message variables] <*ring id*>: Ring ID [Action] Either wait for the suppression-time timeout specified by the configuration command `preempt-delay`, or manually remove the path switchback suppression state with the command `clear axrp preempt-delay`.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
7	E3	VLAN	20170017	0700	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. [Explanation of message variables] <*ring id*>: Ring ID [Action] None.				
8	E3	VLAN	20170018	0700	AXRP <*ring id*> : activated multi fault state monitoring.
	Multi-fault monitoring of `Ring Protocol` started. [Explanation of message variables] <*ring id*>: Ring ID [Action] None.				
9	E3	VLAN	20170019	0700	AXRP <*ring id*> : detected multi fault recovery by receiving multi fault detection frames.
	Multi-fault monitoring of `Ring Protocol` detected recovery from multiple faults. The switch outputs this message when it receives a multi-fault monitoring frame at a shared node and detects recovery from multiple faults. [Explanation of message variables] <*ring id*>: Ring ID [Action] None.				
10	E3	VLAN	20170021	0700	AXRP (multi-fault-detection <*ring id*>) : cleared MAC address table by receiving flush frames.
	A multi-fault flush control frame was received, and the MAC address table was cleared. The switch outputs this message when it clears the MAC address table of a ring port that supports the ring ID that applies multi-fault monitoring. [Explanation of message variables] <*ring id*>: Ring ID [Action] None.				
11	E4	VLAN	20170004	0700	AXRP <*ring id*> : detected fault by health check timeout.
	Monitoring of the `Ring Protocol` state detected a fault. The switch outputs this message when it detects a health-check timeout at the master node. [Explanation of message variables] <*ring id*>: Ring ID [Action] A fault may be occurring at the link or the node in a corresponding ring. Check the link and the node states.				
12	E4	VLAN	20170020	0700	AXRP <*ring id*> : detected multi fault by multi fault detection timeout.
	Multi-fault monitoring of `Ring Protocol` detected multiple faults. The switch outputs this message when the multi-fault monitoring function detects a timeout at the shared node. [Explanation of message variables] <*ring id*>: Ring ID [Action] Multiple faults might be occurring in a corresponding ring. Check the link and the node states.				

3.3.4 Event location = VLAN (GSRP)

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

Table 3-6: Device failure and event information when the event location is VLAN (GSRP)

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
1	E3	VLAN	20130002	0700	GSRP <*gsrp group id*> VLAN group <*vlan group id*> : state transitioned to Backup.
	The GSRP state transitioned to Backup. The switch 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 state while the GSRP device has not identified the partner switch. [Explanation of message variables] <*gsrp group id*>: GSRP group ID <*vlan group id*>: VLAN group ID [Action] None.				
2	E3	VLAN	20130003	0700	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 state transitioned to Master because the switch has more active ports than the neighboring GSRP switch. [Explanation of message variables] <*gsrp group id*>: GSRP group ID <*vlan group id*>: VLAN group ID [Action] None.				
3	E3	VLAN	20130004	0700	GSRP <*gsrp group id*> VLAN group <*vlan group id*> : state transitioned to Master, because the priority was higher than neighbor's.
	The GSRP state transitioned to Master because the priority of the switch is higher than that of the neighboring GSRP switch. [Explanation of message variables] <*gsrp group id*>: GSRP group ID <*vlan group id*>: VLAN group ID [Action] None.				
4	E3	VLAN	20130005	0700	GSRP <*gsrp group id*> VLAN group <*vlan group id*> : state transitioned to Master, because the MAC address was larger than neighbor's.
	The GSRP state transitioned to Master because the MAC address of the switch is larger than that of the neighboring GSRP switch. [Explanation of message variables] <*gsrp group id*>: GSRP group ID <*vlan group id*>: VLAN group ID [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
5	E3	VLAN	20130008	0700	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 state transitioned from Master to Backup because the switch has fewer active ports than the neighboring GSRP switch. [Explanation of message variables] <*gsrp group id*>: GSRP group ID <*vlan group id*>: VLAN group ID [Action] None.				
6	E3	VLAN	20130009	0700	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 state transitioned from Master to Backup because the priority of the switch is lower than that for the neighboring GSRP switch. [Explanation of message variables] <*gsrp group id*>: GSRP group ID <*vlan group id*>: VLAN group ID [Action] None.				
7	E3	VLAN	20130010	0700	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 state transitioned from Master to Backup because the MAC address of the switch is smaller than that for the neighboring GSRP switch. [Explanation of message variables] <*gsrp group id*>: GSRP group ID <*vlan group id*>: VLAN group ID [Action] None.				
8	E3	VLAN	20130013	0700	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 state is Master. [Explanation of message variables] <*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.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
9	E3	VLAN	20130015	0700	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. [Explanation of message variables] <*port list*>: Port range <*gsrp group id*>: GSRP group ID <*vlan group id*>: VLAN group ID <*mac address*>: MAC address [Action] None.				
10	E3	VLAN	20130017	0700	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`. [Explanation of message variables] <*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.				
11	E4	VLAN	20130006	0700	GSRP <*gsrp group id*> VLAN group <*vlan group id*> : state transitioned to Master, because "set gsrp master" command was executed.
	The GSRP state transitioned to Master because the `set gsrp master` command was executed. [Explanation of message variables] <*gsrp group id*>: GSRP group ID <*vlan group id*>: VLAN group ID [Action] None.				
12	E4	VLAN	20130007	0700	GSRP <*gsrp group id*> VLAN group <*vlan group id*> : state transitioned to Master, because the direct link failure was detected.
	The GSRP state transitioned to Master because a direct link failure was detected. The switch outputs this message when the `direct-down` parameter is set in the GSRP configuration command `no-neighbor-to-master`, and GSRP state transitioned to Master because a direct link down was detected while in the Backup (neighbor unknown) state. [Explanation of message variables] <*gsrp group id*>: GSRP group ID <*vlan group id*>: VLAN group ID [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
13	E4	VLAN	20130011	0700	GSRP <*gsrp group id*> VLAN group <*vlan group id*> : state transitioned to Backup(No Neighbor).
	The GSRP state transitioned to Backup (neighbor unknown). [Explanation of message variables] <*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.				
14	E4	VLAN	20130012	0700	GSRP <*gsrp group id*> VLAN group <*vlan group id*> : state transitioned from Backup(No Neighbor) to Backup.
	The GSRP state transitioned from Backup (neighbor unknown) to Backup. [Explanation of message variables] <*gsrp group id*>: GSRP group ID <*vlan group id*>: VLAN group ID [Action] None.				
15	E4	VLAN	20130014	0700	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 state is Backup (Lock). [Explanation of message variables] <*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.				
16	E4	VLAN	20130016	0700	GSRP <*gsrp group id*> VLAN group <*vlan group id*> : state transitioned from Master to Backup, because the double Master detected.
	The GSRP state of the switch and neighboring machine are both Master, so both transitioned to Backup. [Explanation of message variables] <*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.				
17	E4	VLAN	20130018	0700	GSRP <*gsrp group id*> VLAN group <*vlan group id*> : state transitioned to Master, because forced shift time was expired.
	The GSRP state transitioned to Master due to elapsing of the time set for the automatic master transition wait time. [Explanation of message variables] <*gsrp group id*>: GSRP group ID <*vlan group id*>: VLAN group ID [Action] None.				

3.3.5 Event location = VLAN (L2 loop detection)

The following table describes device failure and event information when the event location is VLAN (L2 loop detection).

Table 3-7: Device failure and event information when the event location is VLAN (L2 loop detection)

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
1	E4	VLAN	20800001	0700	L2LD : Port(<*nif no.*>/<*port no.*>) inactivated because of loop detection from port(<*nif no.*>/<*port no.*>).
	The active port has been blocked because a loop failure was detected. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number [Action] Check the network configuration.				
2	E4	VLAN	20800002	0700	L2LD : Port(<*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. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] Check the network configuration.				
3	E4	VLAN	20800003	0700	L2LD : ChGr(<*channel group number*>) inactivated because of loop detection from port(<*nif no.*>/<*port no.*>).
	The active port has been blocked because a loop failure was detected. [Explanation of message variables] <*channel group number*>: Channel group number <*nif no.*>/<*port no.*>: NIF number/port number [Action] Check the network configuration.				
4	E4	VLAN	20800004	0700	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. [Explanation of message variables] <*channel group number*>: Channel group number [Action] Check the network configuration.				
5	E4	VLAN	20800005	0700	L2LD : Port(<*nif no.*>/<*port no.*>) loop detection from port(<*nif no.*>/<*port no.*>).
	A loop failure was detected. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number [Action] Check the network configuration.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
6	E4	VLAN	20800006	0700	L2LD : Port(<*nif no.*>/<*port no.*>) loop detection from ChGr(<*channel group number*>).
	A loop failure was detected. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] Check the network configuration.				
7	E4	VLAN	20800007	0700	L2LD : ChGr(<*channel group number*>) loop detection from port(<*nif no.*>/<*port no.*>).
	A loop failure was detected. [Explanation of message variables] <*channel group number*>: Channel group number <*nif no.*>/<*port no.*>: NIF number/port number [Action] Check the network configuration.				
8	E4	VLAN	20800008	0700	L2LD : ChGr(<*channel group number*>) loop detection from ChGr(<*channel group number*>).
	A loop failure was detected. [Explanation of message variables] <*channel group number*>: Channel group number [Action] Check the network configuration.				
9	E4	VLAN	20800009	0700	L2LD : Port(<*nif no.*>/<*port no.*>) activate by automatic restoration of the L2loop detection function.
	The port state `inactive` was cleared due to automatic recovery of the L2 loop detection function. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number [Action] None.				
10	E4	VLAN	20800010	0700	L2LD : ChGr(<*channel group number*>) activate by automatic restoration of the L2loop detection function.
	The port state `inactive` was cleared due to automatic recovery of the L2 loop detection function. [Explanation of message variables] <*channel group number*>: Channel group number [Action] None.				
11	E4	VLAN	20800011	0700	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. [Explanation of message variables] None. [Action] Decrease the number of ports sending L2 loop detection frames.				

3.3.6 Event location = VLAN (CFM)

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

Table 3-8: Device failure and event information when the event location is VLAN (CFM)

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
1	E4	VLAN	20900003	0700	MD Level <*level*> MA <*no.*>: detected on fault of OtherCCM in MEP <*mepid*>.
	The relevant MEP detected a fault (OtherCCM). [Explanation of message variables] <*level*>: Domain level <*no.*>: MA identification number <*mepid*>: MEP ID [Action] A partner switch is not recognized as the same MA. Check that the domain level, MA ID, domain name, and MA name match the partner switches.				
2	E4	VLAN	20900004	0700	MD Level <*level*> MA <*no.*>: detected on fault of ErrorCCM in MEP <*mepid*>.
	The relevant MEP detected a fault (ErrorCCM). [Explanation of message variables] <*level*>: Domain level <*no.*>: MA identification number <*mepid*>: MEP ID [Action] A partner switch and the configuration do not match. Check whether the MEP ID is different from the partner switch, and make sure the send interval (`interval`) matches that of the partner switch.				
3	E4	VLAN	20900005	0700	MD Level <*level*> MA <*no.*>: detected on fault of Timeout in MEP <*mepid*>.
	The relevant MEP detected a fault (Timeout). [Explanation of message variables] <*level*>: Domain level <*no.*>: MA identification number <*mepid*>: MEP ID [Action] The switch is not receiving CCM from partner switches. Check the network status.				
4	E4	VLAN	20900006	0700	MD Level <*level*> MA <*no.*>: detected on fault of PortState in MEP <*mepid*>.
	The relevant MEP detected a fault (PortState). [Explanation of message variables] <*level*>: Domain level <*no.*>: MA identification number <*mepid*>: MEP ID [Action] A partner switch line fault or a port blocking status was detected. Check the status of the partner switch.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
5	E4	VLAN	20900007	0700	MD Level <*level*> MA <*no.*>: detected on fault of RDI in MEP <*mepid*>.
	The relevant MEP detected a fault (RDI). [Explanation of message variables] <*level*>: Domain level <*no.*>: MA identification number <*mepid*>: MEP ID [Action] A fault was detected in a partner switch. Check the status of the partner switch.				
6	E4	VLAN	20900008	0700	Exceeded the number of the maximum port.
	The number of ports exceeds the number for which MEP and MIP can be set. [Explanation of message variables] None. [Action] Check the number of settings.				

3.3.7 Event location = MAC

The following table describes device failure and event information when the event location is MAC.

Table 3-9: Device failure and event information when the event location is MAC

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
1	E3	MAC	20120005	0800	Channel Group(<*channel group number*>) disabled administratively.
	A channel group was designated as disabled by the configuration. [Explanation of message variables] <*channel group number*>: Channel group number [Action] None.				
2	E3	MAC	20120006	0800	Channel Group(<*channel group number*>) enabled administratively.
	A channel group was released from the disabled state by the configuration. [Explanation of message variables] <*channel group number*>: Channel group number [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
3	E3	MAC	20120007	0800	Port(<*nif no.*>/<*port no.*>) detached from Channel Group(<*channel group number*>) - Different Partner System ID is detected.
	The system ID of a partner switch does not match between the ports for LACP mode link aggregation, and the port was detached from the channel group. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] Check the following: 1. Is the connection with the partner switch correct? 2. Is the system ID setting of the partner switch correct?				
4	E3	MAC	20120008	0800	Port(<*nif no.*>/<*port no.*>) detached from Channel Group(<*channel group number*>) - Different Partner Key is detected.
	The key of a partner switch does not match between the ports for LACP mode link aggregation, and the port was detached from the channel group. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] Check the following: 1. Is the connection with the partner switch correct? 2. Is the key setting of the partner switch correct?				
5	E3	MAC	20120009	0800	Port(<*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. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] None.				
6	E3	MAC	20120010	0800	Port(<*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. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] Check the line status.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
7	E3	MAC	20120011	0800	Port(<*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. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] For detached lines, check the settings of the Switch and partner switches.				
8	E3	MAC	20120012	0800	Port(<*nif no.*>/<*port no.*>) detached from Channel Group(<*channel group number*>) - Half-duplex port.
	Lines operating in half-duplex mode were detached from the channel group. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] For detached lines, check the settings of the Switch and partner switches.				
9	E3	MAC	20120013	0800	Port(<*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 partner switch was denied due to LACP, and the port was detached from the channel group. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] Check the partner switch status.				
10	E3	MAC	20120014	0800	Port(<*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 partner switch, and the port was detached from the channel group because of a timeout. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] Check the partner switch status, which is active.				
11	E3	MAC	20120015	0800	Port(<*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. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
12	E3	MAC	20120016	0800	Port(<*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. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] None.				
13	E3	MAC	20120017	0800	Port(<*nif no.*>/<*port no.*>) detached from Channel Group(<*channel group number*>) - Partner Aggregation bit is FALSE.
	The application bit of the partner switch in the LACP mode was false, and the port was detached from the channel group. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] None.				
14	E3	MAC	20120018	0800	Port(<*nif no.*>/<*port no.*>) detached from Channel Group(<*channel group number*>) - Partner Port number is changed.
	The port number of the partner switch was changed, and the port was detached from the channel group. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] None.				
15	E3	MAC	20120019	0800	Port(<*nif no.*>/<*port no.*>) detached from Channel Group(<*channel group number*>) - Partner Port priority is changed.
	The port priority value of the partner switch was changed, and the port was detached from the channel group. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] None.				
16	E3	MAC	20120020	0800	Port(<*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. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
17	E3	MAC	20120021	0800	Port(<*nif no.*>/<*port no.*>) added to Channel Group(<*channel group number*>).
	A port was added to the channel group. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] None.				
18	E3	MAC	20120022	0800	Port(<*nif no.*>/<*port no.*>) attached to Channel Group(<*channel group number*>).
	A port was aggregated to the channel group. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] None.				
19	E3	MAC	20120023	0800	Port(<*nif no.*>/<*port no.*>) attached to Channel Group(<*channel group number*>) - A standby port became active.
	Operation by a standby link has started. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] None.				
20	E3	MAC	20120024	0800	Port(<*nif no.*>/<*port no.*>) detached from Channel Group(<*channel group number*>) - This port became a standby port.
	Operation by a standby link has started. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] None.				
21	E4	MAC	20120002	0800	Channel Group(<*channel group number*>) is Up.
	The channel group status is Up. [Explanation of message variables] <*channel group number*>: Channel group number [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
22	E4	MAC	20120003	0800	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. [Explanation of message variables] <*channel group number*>: Channel group number [Action] For line connection status with partner switches: 1. Check whether the line is down. 2. Check whether the line is half-duplex. 3. Check that the partner switch LACP setting and line statuses are normal.				
23	E4	MAC	20120004	0800	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. [Explanation of message variables] <*channel group number*>: Channel group number [Action] For line connection status with partner switches: 1. Check whether the line is down. 2. Check whether the line is half-duplex. 3. Check that the partner switch LACP setting and line statuses are normal.				

3.4 Switch parts

3.4.1 Event location = SOFTWARE

The following table describes device failure and event information when the event location is `SOFTWARE`.

Table 3-10: Device failure and event information when the event location is SOFTWARE

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
1	E3	SOFTWARE	00003001	1000	System restarted due to abort reset operation.
	The device was restarted because the RESET button was pressed. [Explanation of message variables] None. [Action] None.				
2	E3	SOFTWARE	00003002	1000	System restarted due to default reset operation.
	The device was restarted because the default switch was pressed. [Explanation of message variables] None. [Action] None.				
3	E3	SOFTWARE	00003003	1000	System restarted due to fatal error detected by software.
	The software detected a fatal error and restarted the system. [Explanation of message variables] None. [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.				
4	E3	SOFTWARE	00003004	1000	System restarted due to user operation.
	The device was restarted because of the reload command. [Explanation of message variables] None. [Action] None.				
5	E3	SOFTWARE	00003005	1000	System restarted due to fatal error detected by kernel.
	The kernel detected a fatal error and restarted the system. [Explanation of message variables] None. [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.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
6	E3	SOFTWARE	00003006	1000	System restarted due to WDT timeout.
	The device was restarted because of a WDT (watchdog timer) timeout. [Explanation of message variables] None. [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.				
7	E3	SOFTWARE	00003007	1000	System restarted due to hardware error detected by kernel.
	The device was restarted because of a hardware failure. [Explanation of message variables] None. [Action] Replace the Switch.				
8	E3	SOFTWARE	00003008	1000	System restarted due to hardware error detected.
	The device was restarted because of a hardware failure. [Explanation of message variables] None. [Action] Replace the Switch.				
9	E3	SOFTWARE	00003301	1000	CPU congestion detected.
	Packet congestion in CPU processing was detected. [Explanation of message variables] None. [Action] 1. If any messages that indicate another error or event (for example, indicating an error or event related to the Layer 2 protocol or IPv4/IPv6 routing protocols) are issued along with this message, carry out the action appropriate for those messages. 2. This message is occasionally output if the switch receives a large quantity of packets for the local device (such as for ping or telnet), in a broadcast, or in a multicast. The CPU can process broadcast and multicast packets while the hardware is relaying them. 3. If there is too much access from the network management device, limit the amount of access to the minimum necessary. 4. If (3) above does not start the recovery, see the *Troubleshooting Guide* description of the case in which congestion of packets being processed by the CPU does not recover, and carry out the indicated action.				
10	E3	SOFTWARE	00003302	1000	CPU has recovered from congestion.
	The CPU has recovered from congestion. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
11	E3	SOFTWARE	00003303	1000	Received many packets and loaded into the queue to CPU.
	Numerous received packets have accumulated in CPU queues. [Explanation of message variables] None. [Action] None. If this message is output frequently, check the following. 1. Check if the switch 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. Review the network configuration.				
12	E3	SOFTWARE	00003304	1000	Processed the packets in the queue to CPU.
	Packets that had been accumulating in CPU queues have been processed. [Explanation of message variables] None. [Action] None.				
13	E3	SOFTWARE	00008601	1001	NTP lost synchronization with <*ip address*>.
	Synchronization was lost with the NTP server at <*ip address*>. [Explanation of message variables] <*ip address*>: IPv4 address of NTP server [Action] Use the `show ntp associations` command to check the NTP status. If the non-synchronized state continues, check the NTP configuration, NTP server operation status, and availability of communication.				
14	E3	SOFTWARE	00008602	1001	NTP detected an invalid packet from <*ip address*>.
	An invalid packet from the NTP server at <*ip address*> was detected. [Explanation of message variables] <*ip address*>: IPv4 address of NTP server [Action] Check the NTP server.				
15	E3	SOFTWARE	00008603	1001	NTP could not find the server which synchronize with.
	There is no NTP server for which synchronization is possible. [Explanation of message variables] None. [Action] Check the NTP configuration, NTP server operation status, and availability of communication.				
16	E3	SOFTWARE	01200187	1001	The temperature logging file can't be written.
	Writing of temperature logging information failed. [Explanation of message variables] None. [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).				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
17	E3	SOFTWARE	01700501	1001	Statistics table initialized.
	The switch time has been changed, and the statistics table that holds the CPU usage statistics has been initialized. [Explanation of message variables] None. [Action] None.				
18	E3	SOFTWARE	01700502	1001	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. [Explanation of message variables] None. [Action] If necessary, reenter command or retrieve MIB.				
19	E3	SOFTWARE	01700503	1001	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. [Explanation of message variables] None. [Action] If necessary, reenter command or retrieve MIB.				
20	E3	SOFTWARE	01900250	1001	Software started up.
	The software has started. This log data is collected in UTC time. [Explanation of message variables] None. [Action] None.				
21	E3	SOFTWARE	01910201	1001	System started collecting new "error.log".
	The system has started collecting data into a new reference log. [Explanation of message variables] None. [Action] None.				
22	E3	SOFTWARE	01910202	1001	System restarted by user operation.
	The system was restarted by a user operation. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
23	E3	SOFTWARE	01910203	1001	System restarted after hardware reset.
	The system was restarted by the RESET button. [Explanation of message variables] None. [Action] None.				
24	E3	SOFTWARE	02002010	1001	System failed switching to admin mode.
	The change to the `admin` mode during MIB setup has failed. [Explanation of message variables] None. [Action] Another administrator has become `admin`. Using the `show sessions` command, check the login users and `admin` users.				
25	E3	SOFTWARE	02002012	1001	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. [Explanation of message variables] None. [Action] See the manual *MIB Reference For Version 11.10*, and make sure that the set MIB has read and write attributes.				
26	E3	SOFTWARE	02002013	1001	Incorrect instance value specified.
	The instance value set during MIB setup is not correct. [Explanation of message variables] None. [Action] Check and set the instance value.				
27	E3	SOFTWARE	02002014	1001	MIB value specified was out of range.
	You are attempting to set a MIB value that is outside the setting range during MIB setup. [Explanation of message variables] None. [Action] For details on the MIB value range, see *34. SNMP* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.				
28	E3	SOFTWARE	02002015	1001	Data length of the MIB value was too long.
	The entry for the MIB value set during MIB setup is too long. [Explanation of message variables] None. [Action] For details on the number of characters that can be set for a MIB value, see *34. SNMP* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
29	E3	SOFTWARE	02002016	1001	MIB Set failed due to the lack of necessary MIBs.
	MIB setup was not possible because the MIBs required for setting are insufficient. [Explanation of message variables] None. [Action] See the manual *MIB Reference For Version 11.10*, and check that items required for setting are sufficient.				
30	E3	SOFTWARE	02002017	1001	Illegal character used in MIB setting.
	You are attempting to set up the MIB using invalid characters. [Explanation of message variables] None. [Action] Check the character code list in *1. Reading the Manual* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*, and set up the MIB.				
31	E3	SOFTWARE	02002018	1001	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. [Explanation of message variables] None. [Action] Stop editing of the backup configuration file.				
32	E3	SOFTWARE	02002019	1001	Failed in contact the configuration file while setting up MIB.
	Access to the startup configuration file for MIB settings failed. [Explanation of message variables] None. [Action] Eliminate the cause of the access failure, and try again.				
33	E3	SOFTWARE	02002020	1001	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. [Explanation of message variables] None. [Action] For details on configuration errors, see *Error Messages Displayed When Editing the Configuration messages* in the manual *Configuration Command Reference*.				
34	E3	SOFTWARE	02002021	1001	Not all MIB configured.
	MIB setup failed, and only some of the MIB values were set. [Explanation of message variables] None. [Action] Try setup again. If the retry still does not work, log in (for example, by using telnet) and set the MIB values.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
35	E3	SOFTWARE	02002023	1001	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. [Explanation of message variables] None. [Action] The configuration has not been saved. Save it (for example, by using telnet).				
36	E3	SOFTWARE	02002024	1001	<*object name*> set as <*mib value*> at the request of <*ip address*>.
	<*object name*> was set to <*mib value*> because of a request from <*ip address*>. [Explanation of message variables] <*object name*>: MIB object mnemonic <*mib value*>: MIB value <*ip address*>: IPv4 or IPv6 address of the SNMP manager [Action] None.				
37	E3	SOFTWARE	02002025	1001	SNMP: MAC address table entry cleared at the request of <*ip address*>.
	The MAC address table was cleared due to a MAC address table clear request from the SNMP manager at <*ip address*>. [Explanation of message variables] <*ip address*>: IPv4 or IPv6 address of the SNMP manager [Action] None.				
38	E3	SOFTWARE	05001010	1001	The number of maximum multipath set by the configuration is different from the maximum value when this system starts.
	The maximum multi-path count that was set at configuration differs from the maximum value during startup of this Switch. [Explanation of message variables] None. [Action] 1. Using the show system command, check the maximum multi-path count (2, 4, 8, or 16) 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 switch. After restarting the switch, 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.				
39	E3	SOFTWARE	0d10b002	1001	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*>. [Explanation of message variables] <*subnet address*>: Allocation range subnet address. [Action] Examine the maximum number of clients for the subnet that dhcp_server can allocate.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
40	E3	SOFTWARE	0d10b003	1001	The dhcp_server reused the abandoned IP address <*ip address*>.
	dhcp_server reused the discarded IP address. [Explanation of message variables] <*ip address*>: Allocation IP address. [Action] None.				
41	E3	SOFTWARE	0d10b004	1001	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. [Explanation of message variables] <*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.				
42	E3	SOFTWARE	0d10b005	1001	Failed in NS UPDATE by dhcp_server. : <*map*>
	NS UPDATE processing by dhcp_server has failed. [Explanation of message variables] <*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.				
43	E3	SOFTWARE	0d10b0e4	1001	dhcp_server: Invalid network address.
	The DHCP server detected an invalid configuration. An invalid network address was specified. [Explanation of message variables] None. [Action] Delete the previously-entered setting, and re-specify the setting using a correct network address.				
44	E3	SOFTWARE	0d10b0ec	1001	dhcp_server: Invalid key.(ip dhcp key ... secret-hmac-md5 ...)
	The DHCP server detected an invalid configuration. There is an invalid key. [Explanation of message variables] None. [Action] Delete the previously-entered setting, and re-specify the setting using a correct key.				
45	E3	SOFTWARE	0d10b0ee	1001	dhcp_server: Invalid IP address. (ip dhcp excluded-address ...)
	The DHCP server detected an invalid configuration. An invalid exclusion address range was specified. [Explanation of message variables] None. [Action] Delete the previously-entered setting, and re-specify the setting using a correct exclusion address range.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
46	E3	SOFTWARE	0e008001	1000	Virtual router <*vrid*> of <*interface name*> state has transitioned to <*state*>.
	The virtual router active state transitioned to <*state*>. [Explanation of message variables] <*vrid*>: Virtual router ID <*interface name*>: Name of interface on which VRRP is configured <*state*>: Virtual router state [Action] None.				
47	E3	SOFTWARE	0e008002	1000	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. [Explanation of message variables] <*vrid*>: Virtual router ID <*interface name*>: Name of interface on which VRRP is configured [Action] Check the remote devices that make up the same virtual router.				
48	E3	SOFTWARE	0e008003	1000	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. [Explanation of message variables] <*vrid*>: Virtual router ID <*interface name*>: Name of interface on which VRRP is configured [Action] Check the remote devices that make up the same virtual router.				
49	E3	SOFTWARE	0e008004	1000	Virtual router <*vrid*> of <*interface name*> received VRRP packet that does not pass the authentication check.
	Authentication of a received VRRP ADVERTISEMENT packet failed. [Explanation of message variables] <*vrid*>: Virtual router ID <*interface name*>: Name of interface on which VRRP is configured [Action] Check the password settings for the Switch and the partner switch that make up the same virtual router.				
50	E3	SOFTWARE	0e008005	1000	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. [Explanation of message variables] <*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 partner switch that make up the same virtual router.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
51	E3	SOFTWARE	0e008006	1000	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 transmission interval specified in a received VRRP ADVERTISEMENT packet does not match the settings of the Switch. [Explanation of message variables] <*vrid*>: Virtual router ID <*interface name*>: Name of interface on which VRRP is configured [Action] Check the transmission intervals for the Switch and the partner switch that make up the same virtual router.				
52	E3	SOFTWARE	0e008007	1000	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. [Explanation of message variables] None. [Action] When constructing the Switch with a virtual router, set the VRRP version of the partner switch to 2 for IPv4, and 3 for IPv6, respectively.				
53	E3	SOFTWARE	0e008008	1000	Virtual router <*vrid*> of <*interface name*> priority was changed to <*priority*>.
	The VRRP priority was changed to <*priority*>. [Explanation of message variables] <*vrid*>: Virtual router ID <*interface name*>: Name of interface on which VRRP is configured <*priority*>: Virtual router priority [Action] None.				
54	E3	SOFTWARE	0e008012	1000	Virtual router <*vrid*> of <*interface name*> was finished.
	The virtual router ended. [Explanation of message variables] <*vrid*>: Virtual router ID <*interface name*>: Name of interface on which VRRP is configured [Action] None.				
55	E3	SOFTWARE	0e008015	1000	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. [Explanation of message variables] <*vrid*>: Virtual router ID <*interface name*>: Name of interface on which VRRP is configured [Action] Check the remote devices that make up the same virtual router.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
56	E3	SOFTWARE	0e008016	1000	Virtual router <*vrid*> of <*interface name*> priority changed to <*priority*>, because error detected on line by vrrp-polling.
	VRRP polling detected a line fault, and the VRRP priority was changed to <*priority*>. [Explanation of message variables] <*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.				
57	E3	SOFTWARE	0e008017	1000	<*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 functionality detected a fault. [Explanation of message variables] <*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.				
58	E3	SOFTWARE	0e008018	1000	<*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 functionality detected recovery from a fault. [Explanation of message variables] <*interface name*>: Name of interface on which VRRP is configured <*vrid*>: Virtual router ID [Action] None.				
59	E3	SOFTWARE	0e008019	1000	Critical interface of <*interface name*> is down.
	A fault-monitoring interface is down. [Explanation of message variables] <*interface name*>: Interface name of a fault-monitoring target. [Action] None.				
60	E3	SOFTWARE	0e008020	1000	Critical interface of <*interface name*> is up.
	A fault-monitoring interface is up. [Explanation of message variables] <*interface name*>: Interface name of a fault-monitoring target. [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
61	E3	SOFTWARE	0e008025	1000	Critical interface of <*interface type*> <*interface number*> is down.
	A fault-monitoring interface is down. [Explanation of message variables] <*interface type*>: Interface that is specified as the fault-monitoring interface. • `gigabitethernet`: 10BASE-T/100BASE-TX/1000BASE-T, 100BASE-FX, 1000BASE-X • `tengigabitethernet`: 10GBASE-R • `port-channel`: channel-group <*interface number*>: Interface number specified for the failure monitoring interface • <*nif no.*>/<*port no.*>: NIF number/port number (For gigabitethernet or tengigabitethernet) • <*channel group number*>: Channel group number (For port-channel) [Action] None.				
62	E3	SOFTWARE	0e008026	1000	Critical interface of <*interface type*> <*interface number*> is up.
	A fault-monitoring interface is up. [Explanation of message variables] <*interface type*>: Interface that is specified as the fault-monitoring interface. • `gigabitethernet`: 10BASE-T/100BASE-TX/1000BASE-T, 100BASE-FX, 1000BASE-X • `tengigabitethernet`: 10GBASE-R • `port-channel`: channel-group <*interface number*>: Interface number specified for the failure monitoring interface • <*nif no.*>/<*port no.*>: NIF number/port number (For gigabitethernet or tengigabitethernet) • <*channel group number*>: Channel group number (For port-channel) [Action] None.				
63	E3	SOFTWARE	0e008027	1000	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. [Explanation of message variables] <*interface number*>: Interface number specified for the failure monitoring interface • <*nif no.*>/<*port no.*>: NIF number/port number [Action] None.				
64	E3	SOFTWARE	0f306003 0f406003	1001	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 configuration command `ip pim max-interface`. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
65	E3	SOFTWARE	0f406004	1001	IPv4 multicast routing entry had exceeded maximum value <*number*> for limit, entry has discarded.
	An entry was discarded because the items of IPv4 multicast routing information exceed the limit maximum value of <*number*> [Explanation of message variables] <*number*>: Maximum number of items of IPv4 multicast routing information [Action] Unauthorized access might have been occurred. • Check if more than the expected number of additional requests for multicast routing information were generated. The number of items of multicast routing 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.				
66	E3	SOFTWARE	0f406005	1001	IPv4 multicast routing entry has recovered from the state of discard.
	IPv4 multicast routing information has recovered from the state in which entries were discarded. [Explanation of message variables] None. [Action] None.				
67	E3	SOFTWARE	0f406006	1001	IGMP source-limit <*number*> has been exceeded on interface <*interface name*> due to over-request. Request have been discarded.
	A request was discarded because the interface <*interface name*> received a request that exceeded the IGMP source limit value of <*number*>. [Explanation of message variables] <*number*>: IGMP group limit value <*interface name*>: Interface name [Action] Unauthorized access might have been 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.				
68	E3	SOFTWARE	0f406007	1001	IGMP source-limit on requests on interface <*interface name*> has recovered from state of discard.
	The interface <*interface name*> has recovered from state in which sources belonging to IGMP group were discarded. [Explanation of message variables] <*interface name*>: Interface name [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
69	E3	SOFTWARE	0f406008	1001	IGMP group-limit <*number*> has been exceeded on interface <*interface name*> 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. [Explanation of message variables] <*number*>: IGMP group limit value <*interface name*>: Interface name [Action] Unauthorized access might have been 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.				
70	E3	SOFTWARE	0f406009	1001	IGMP group-limit on requests on interface <*interface name*> has recovered from state of discard.
	The interface <*interface name*> has recovered from the state in which IGMP groups were discarded. [Explanation of message variables] <*interface name*>: Interface name [Action] None.				
71	E3	SOFTWARE	11010001	1001	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. [Explanation of message variables] <*policy list no.*> : the list number of the policy-based routing <*sequence*>: Priority of routing information in the list [Action] None.				
72	E3	SOFTWARE	11010002	1001	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. [Explanation of message variables] <*policy list no.*>: the list number of the policy-based routing [Action] None.				
73	E3	SOFTWARE	1920a003	1001	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 configuration command `ipv6 pim max-interface`. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
74	E3	SOFTWARE	1920a005	1001	IPv6 multicast routing entry had exceeded maximum value <*number*> for limit, entry has discarded.
	An entry was discarded because the IPv6 multicast routing information exceeds the limit maximum value of <*number*> [Explanation of message variables] <*number*>: Maximum number of items of IPv6 multicast routing information [Action] Unauthorized access might have been occurred. • Check if more than the expected number of additional requests for multicast routing information were generated. The number of items of multicast routing 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.				
75	E3	SOFTWARE	1920a006	1001	IPv6 multicast routing entry has recovered from the state of discard.
	IPv6 multicast routing information has recovered from state in which entries were discarded. [Explanation of message variables] None. [Action] None.				
76	E3	SOFTWARE	1f01b024	1001	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. [Explanation of message variables] None. [Action] 1. Use the `show ipv6 dhcp relay binding` command to check the capacity client count. 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`.				
77	E3	SOFTWARE	1f01b025	1001	IPv6 DHCP relay information defined by the configuration file is ignored, since IPv6 DHCP relay function license is not given.
	The IPv6 DHCP relay information set in the startup configuration file is invalid because a license was not granted. [Explanation of message variables] None. [Action] If you are using an IPv6 DHCP relay, set the option license OP-DH6R with the `set license` command, and restart the switch.				
78	E3	SOFTWARE	25090003	1001	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. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
79	E3	SOFTWARE	25090004	1001	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. [Explanation of message variables] None. [Action] None.				
80	E3	SOFTWARE	25090005	1001	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. [Explanation of message variables] None. [Action] None.				
81	E3	SOFTWARE	25090006	1001	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. [Explanation of message variables] None. [Action] None.				
82	E3	SOFTWARE	3000b042	1001	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. [Explanation of message variables] None. [Action] None.				
83	E3	SOFTWARE	3000b043	1001	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. [Explanation of message variables] <*mac address*>/<*vlan id*>/<*ip address*>: DHCP client terminal information • <*mac address*>: MAC address • <*vlan id*>: VLAN ID • <*ip address*>: IP address [Action] The capacity limit of the switch was exceeded. Review the system configuration. If this message is displayed due to addition of a static entry, delete the relevant static entry.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
84	E3	SOFTWARE	3000b044	1001	The binding database can't be restored(<*reason*>).
	The binding database could not be restored. [Explanation of message variables] <*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.				
85	E3	SOFTWARE	3000b045	1001	The binding database can't be stored(<*reason*>).
	The binding database could not be stored. [Explanation of message variables] <*reason*>: Reason for the failure • File is not writing. (Writing to the file is not possible.) [Action] Check the storage destination of the binding database.				
86	E3	SOFTWARE	3000b046	1001	The binding database was restored from <*url*>.
	The binding database could not be restored. [Explanation of message variables] <*url*>: The binding database being read • `previous process`: The process before the restart • `flash`: Internal flash memory • `mc`: MC [Action] None.				
87	E3	SOFTWARE	3000b047	1001	Failed in source guard setting by DHCP snooping (<*mac address*>/<*vlan id*>/<*ip address*>/<*nif no.*>/<*port no.*>).
	The terminal filter setting failed. [Explanation of message variables] <*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 switch was exceeded. Review the system configuration.				
88	E4	SOFTWARE	0e008021	1000	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. [Explanation of message variables] None. [Action] 1. Change the virtual router ID to a different value. 2. Change the VLAN ID of the VLAN for setting the virtual router to a different value.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
89	E4	SOFTWARE	20160002	1001	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. [Explanation of message variables] None. [Action] Review the capacity limit. However, depending on the hardware specification, the setting to the maximum of the capacity limit might not be available.				
90	E4	SOFTWARE	20400003	1001	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. [Explanation of message variables] None. [Action] Review the capacity limit. However, depending on the hardware specification, the setting to the maximum of the capacity limit might not be available.				
91	E4	SOFTWARE	20400004	1001	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. [Explanation of message variables] None. [Action] Review the capacity limit. However, depending on the hardware specification, the setting to the maximum of the capacity limit might not be available.				
92	E4	SOFTWARE	20420002	1001	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. [Explanation of message variables] None. [Action] Review the capacity limit. However, depending on the hardware specification, the setting to the maximum of the capacity limit might not be available.				
93	E4	SOFTWARE	20420003	1001	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. [Explanation of message variables] None. [Action] Restart L2MAC manager program (L2MacManager).				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
94	E4	SOFTWARE	20430002	1001	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. [Explanation of message variables] None. [Action] Review the capacity limit. However, depending on the hardware specification, the setting to the maximum of the capacity limit might not be available.				
95	E4	SOFTWARE	20430003	1001	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. [Explanation of message variables] None. [Action] Restart L2MacManager.				
96	E4	SOFTWARE	27000013	0000	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. [Explanation of message variables] <*number*>: Count of consecutive failures [Action] 1. Check if the configurations for RADIUS server or TACACS+ have been set. 2. Check the configurations to make sure that the IP address for 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.				
97	E7	SOFTWARE	00003101	1000	Memory exhausted. Possibly too many users logged in, or too many sessions(via ftp,http,...) established.
	There is not enough CPU memory. [Explanation of message variables] None. [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. See *3.2 Capacity limit* in the manual *Configuration Guide Vol. 1 For Version 11.10* and review the network configuration.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
98	E7	SOFTWARE	01100001 01200001 01300001 01400001 01600001 01700001 01800001 01900001 01910001 03000001 04000001 05000001 06100001 06200001 06300001 06400001 06500001 07000001 08000001 09100001 09200001 09300001 09400001 09500001 09600001 09700001 09800001	1001	Software failure occurred during operation.
	An error occurred in the software during operation. [Explanation of message variables] None. [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.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
99	E7	SOFTWARE	01100002 01200002 01300002 01400002 01600002 01700002 01800002 01900002 01910002 03000002 04000002 05000002 06100002 06200002 06300002 06400002 06500002 07000002 08000002 09100002 09200002 09300002 09400002 09500002 09600002	1001	Software failure occurred during operation.
	An error occurred in the software during operation. [Explanation of message variables] None. [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.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
100	E7	SOFTWARE	01100004 01200004 01300004 01400004 01600004 01700004 01800004 01900004 01910004 03000004 04000004 05000004 06100004 06200004 06300004 06400004 06500004 07000004 08000004 09100004 09200004 09300004 09400004 09500004 09600004	1001	Software failure occurred during operation.
	An error occurred in the software during operation. [Explanation of message variables] None. [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.				
101	E7	SOFTWARE	02002001	1001	snmpd aborted.
	The SNMP agent program (snmpd) was forced to stop. [Explanation of message variables] None. [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 switch.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
102	E7	SOFTWARE	02002003	1001	rmon aborted.
	The RMON program (rmon) was forced to stop. [Explanation of message variables] None. [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 switch.				
103	E7	SOFTWARE	05001001	1001	Rtm aborted [:<*error string*>].
	The unicast routing program (rtm) was forced to stop. [Explanation of message variables] <*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 he 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 *3.2 Capacity limit* in the manual *Configuration Guide Vol. 1 For Version 11.10*). 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 (Log 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 switch.				
104	E7	SOFTWARE	0d00b001	1001	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 operation, and forced the program to stop. [Explanation of message variables] None. [Action] The DHCP relay program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
105	E7	SOFTWARE	0d10b001	1001	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 operation, and forced the program to stop. [Explanation of message variables] None. [Action] The DHCP server program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
106	E7	SOFTWARE	0e008014	1000	vrrpd aborted.
	The VRRP program (vrrpd) was forced to stop. [Explanation of message variables] None. [Action] The VRRP program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
107	E7	SOFTWARE	0f406001	1001	mrp aborted.
	The IP multicast routing program was forced to stop. [Explanation of message variables] None. [Action] 1. Check whether other log messages related to the IP multicast routing program (log 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 switch.				
108	E7	SOFTWARE	11109901	1001	policyd aborted.
	The policy-based program (policyd) was forced to stop. [Explanation of message variables] None. [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 switch.				
109	E7	SOFTWARE	1920a002	1001	mr6 aborted.
	IPv6 multicast routing program was forced to stop. [Explanation of message variables] None. [Action] 1. Check whether other log messages related to the IPv6 multicast routing program (log 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 switch.				
110	E7	SOFTWARE	1e001000	1001	flowd aborted.
	The flow statistics agent program (flowd) was forced to stop. [Explanation of message variables] None. [Action] The flow statistics agent program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
111	E7	SOFTWARE	1f00b011	1001	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 operation, and forced the program to stop. [Explanation of message variables] None. [Action] The IPv6 DHCP server program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
112	E7	SOFTWARE	1f01b021	1001	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 operation, and forced the program to stop. [Explanation of message variables] None. [Action] The IPv6 DHCP relay program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
113	E7	SOFTWARE	20110000	1001	stpd aborted
	The Spanning Tree program (STPd) was forced to stop. [Explanation of message variables] None. [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 switch.				
114	E7	SOFTWARE	20120001	1001	LAd aborted
	The link aggregation program (LAd) was forced to stop. [Explanation of message variables] None. [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 switch.				
115	E7	SOFTWARE	20130001	1001	gsrpd aborted.
	The GSRP program (gsrpd) was forced to stop. [Explanation of message variables] None. [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 switch.				
116	E7	SOFTWARE	20140001	1001	lldpd aborted.
	The LLDP program (lldpd) was forced to stop. [Explanation of message variables] None. [Action] The LLDP program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
117	E7	SOFTWARE	20150001	1001	oadpd aborted.
	The OADP program (oadpd) was forced to stop. [Explanation of message variables] None. [Action] The OADP program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
118	E7	SOFTWARE	20160001	1001	L2MacManager aborted.
	L2MAC manager program (L2MacManager) was forced to stop. [Explanation of message variables] None. [Action] The L2MAC manager program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
119	E7	SOFTWARE	20170001	1001	axrpd aborted.
	The Ring Protocol program (axrpd) was forced to stop. [Explanation of message variables] None. [Action] Collect the error save information (`axrpd.core` file under `/usr/var/core`), log information, and the configuration of the Ring Protocol program. For details about how to collect the information, see the *Troubleshooting Guide*. The Ring Protocol program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
120	E7	SOFTWARE	20400001	1001	dot1xd aborted
	The IEEE 802.1X program (dot1xd) was forced to stop. [Explanation of message variables] None. [Action] The IEEE 802.1X program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
121	E7	SOFTWARE	20420001	1001	wad aborted.
	The Web authentication program (wad) was forced to stop. [Explanation of message variables] None. [Action] The Web authentication program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
122	E7	SOFTWARE	20430001	1001	macauthd aborted.
	The MAC authentication program was forced to stop. [Explanation of message variables] None. [Action] The MAC authentication program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
123	E7	SOFTWARE	20700001	1001	efmoamd aborted.
	The IEEE 802.3ah/OAM program (efmoamd) was forced to stop. [Explanation of message variables] None. [Action] The IEEE 802.3ah/OAM program should restart automatically. If it does not restart if restarts occur frequently, restart the switch.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
124	E7	SOFTWARE	20800001	1001	l2ldd aborted.
	The L2 loop detection program (l2ldd) was forced to stop. [Explanation of message variables] None. [Action] The L2 loop detection manager program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
125	E7	SOFTWARE	20900001	1001	cfmd aborted.
	The CFM program (cfmd) was forced to stop. [Explanation of message variables] None. [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 switch.				
126	E7	SOFTWARE	21000001	1001	snoopd aborted.
	The IGMP snooping/MLD snooping program (snoopd) was forced to stop. [Explanation of message variables] None. [Action] The IGMP snooping/MLD snooping program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
127	E7	SOFTWARE	25300000	1001	nimd aborted.
	The network interface manager program (nimd) was forced to stop. [Explanation of message variables] None. [Action] The network interface manager program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
128	E7	SOFTWARE	27000001	0000	accountingd aborted.
	The accounting program (accountingd) was forced to stop. [Explanation of message variables] None. [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 switch.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
129	E7	SOFTWARE	27000011	0000	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. [Explanation of message variables] None. [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				
130	E7	SOFTWARE	2a001000	1001	httpd aborted.
	The HTTP program (httpd) was forced to stop. [Explanation of message variables] None. [Action] The HTTP program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
131	E7	SOFTWARE	3000b041	1001	dhcp_snoopingd aborted.
	The DHCP snooping program (dhcp_snoopingd) was forced to stop. DHCP snooping detected an anomaly such as a lack of memory, aborted the operation, and forced the program to stop. [Explanation of message variables] None. [Action] The DHCP snooping program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
132	E7	SOFTWARE	32001001	1001	trackobjd aborted.
	The track object program (trackobjd) was forced to stop. [Explanation of message variables] None. [Action] The track object program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
133	E9	SOFTWARE	01100003 01200003 01300003 01400003 01600003 01700003 01800003 01900003 01910003 03000003 04000003 05000003 06100003 06200003 06300003 06400003 06500003 07000003 08000003 09100003 09200003 09300003 09400003 09500003 09600003	1001	System restarted due to software failure occurred during initialization.
	An error occurred in the software during initialization, and the switch restarted. [Explanation of message variables] None. [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.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
134	E9	SOFTWARE	01100005 01200005 01300005 01400005 01600005 01700005 01800005 01900005 01910005 03000005 04000005 05000005 06100005 06200005 06300005 06400005 06500005 07000005 08000005 09100005 09200005 09300005 09400005 09500005 09600005 09700005 09800005	1001	System restarted due to software failure occurred during operation.
	An error occurred in the software during operation, and the switch restarted. [Explanation of message variables] None. [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.				
135	R7	SOFTWARE	00003101	1000	Recovered from memory exhaustion.
	The CPU has recovered from a lack of memory. [Explanation of message variables] None. [Action] None.				
136	R7	SOFTWARE	02002001	1001	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 restarted automatically. [Explanation of message variables] None. [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 switch.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
137	R7	SOFTWARE	02002003	1001	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. [Explanation of message variables] None. [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 switch.				
138	R7	SOFTWARE	05001001	1001	Rtm restarted.
	The unicast routing program (rtm) has restarted. The switch outputs this message when the unicast routing program restarts automatically, or is restarted by the `restart unicast` command. [Explanation of message variables] None. [Action] None.				
139	R7	SOFTWARE	0d00b001	1001	dhcpd restarted.
	The DHCP relay program (dhcpd) has restarted. The switch outputs this message when the DHCP relay program restarts automatically. [Explanation of message variables] None. [Action] None.				
140	R7	SOFTWARE	0d10b001	1001	dhcp_server restarted.
	The DHCP server program (dhcp_server) has restarted. The switch outputs this message when the DHCP server program restarts automatically. [Explanation of message variables] None. [Action] None.				
141	R7	SOFTWARE	0e008014	1000	vrrpd restarted.
	The VRRP program (vrrpd) has restarted. The switch outputs this message when the VRRP program restarts automatically. [Explanation of message variables] None. [Action] None.				
142	R7	SOFTWARE	0f406001	1001	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. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
143	R7	SOFTWARE	11109901	1001	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. [Explanation of message variables] None. [Action] None.				
144	R7	SOFTWARE	1920a002	1001	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. [Explanation of message variables] None. [Action] None.				
145	R7	SOFTWARE	1e001000	1001	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. [Explanation of message variables] None. [Action] None.				
146	R7	SOFTWARE	1f00b011	1001	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. [Explanation of message variables] None. [Action] None.				
147	R7	SOFTWARE	1f01b021	1001	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. [Explanation of message variables] None. [Action] None.				
148	R7	SOFTWARE	20110001	1001	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. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
149	R7	SOFTWARE	20120001	1001	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. [Explanation of message variables] None. [Action] None.				
150	R7	SOFTWARE	20130002	1001	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. [Explanation of message variables] None. [Action] None.				
151	R7	SOFTWARE	20140001	1001	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. [Explanation of message variables] None. [Action] None.				
152	R7	SOFTWARE	20150001	1001	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. [Explanation of message variables] None. [Action] None.				
153	R7	SOFTWARE	20160001	1001	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. [Explanation of message variables] None. [Action] None.				
154	R7	SOFTWARE	20170001	1001	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. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
155	R7	SOFTWARE	20400001	1001	dot1xd restarted.
	The IEEE 802.1X program (dot1xd) has restarted. The switch outputs this message when the IEEE 802.1X program restarts automatically or a restart is requested by the `restart dot1x` command. [Explanation of message variables] None. [Action] None.				
156	R7	SOFTWARE	20420001	1001	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. [Explanation of message variables] None. [Action] Perform authentication again on the authentication client side.				
157	R7	SOFTWARE	20430001	1001	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. [Explanation of message variables] None. [Action] Perform authentication again on the authentication client side.				
158	R7	SOFTWARE	20700001	1001	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. [Explanation of message variables] None. [Action] None.				
159	R7	SOFTWARE	20800001	1001	l2ldd restarted.
	The L2 loop detection program (l2ldd) has restarted. The switch outputs this message when the L2 loop detection program restarts automatically or a restart is requested by the `restart loop-detection` command. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
160	R7	SOFTWARE	20900001	1001	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. [Explanation of message variables] None. [Action] None.				
161	R7	SOFTWARE	21000001	1001	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. [Explanation of message variables] None. [Action] None.				
162	R7	SOFTWARE	25300000	1001	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. [Explanation of message variables] None. [Action] None.				
163	R7	SOFTWARE	27000001	0000	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. [Explanation of message variables] None. [Action] None.				
164	R7	SOFTWARE	27000011	0000	System accounting recovered from congestion.
	The accounting event transmission has recovered from congestion, and accounting of login and logout commands resumed. [Explanation of message variables] None. [Action] None.				
165	R7	SOFTWARE	2a001000	1001	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. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
166	R7	SOFTWARE	3000b041	1001	dhcp_snoopingd restarted.
	The DHCP snooping program (dhcp_snoopingd) has restarted. The switch outputs this message when the DHCP snooping program restarts automatically. [Explanation of message variables] None. [Action] None.				
167	R7	SOFTWARE	32001001	1001	trackobjd restarted.
	The track object program (trackobjd) has restarted. The switch outputs this message after the track object program is restarted automatically. [Explanation of message variables] None. [Action] None.				

3.4.2 Event location = SOFTWARE (Authentication VLAN) [OP-VAA]

The following table describes device failure and event information when the event location is `SOFTWARE` (Authentication VLAN).

Table 3-11: Device failure and event information when the event location is SOFTWARE (Authentication VLAN)

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
1	E3	SOFTWARE	20410002	1001	vaad connection closed <*ipv4 address*>.
	The connection between VAA and the authentication server <*ipv4 address*> has been disconnected. The switch outputs this message when the TCP connection between VAA and an authentication server is disconnected for any reason, or when VAA stops. [Explanation of message variables] <*ipv4 address*>: IPv4 address of an authentication server [Action] If VAA is already running, the connection is reestablished automatically.				
2	E3	SOFTWARE	20410003	1001	vaad connection was established <*ipv4 address*>.
	VAA connected to the authentication server <*ipv4 address*>. The switch outputs this message when a TCP connection between VAA and an authentication server is established. [Explanation of message variables] <*ipv4 address*>: IPv4 address of an authentication server [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
3	E3	SOFTWARE	20410004	1001	vaad Server protocol version is not supported.
	VAA does not support the version of the authentication server protocol. The switch outputs this message when the authentication server protocol version is other than `1.0`. [Explanation of message variables] None. [Action] Change the version of the authentication server protocol to 1.0.				
4	E3	SOFTWARE	20410005	1001	vaad Since L2MacManager restarted, all MAC was deleted.
	All authentication-registered MAC addresses were deleted because L2MacManager closed a socket with VAA. [Explanation of message variables] None. [Action] Perform authentication again on the authentication client side.				
5	E3	SOFTWARE	20410006	1001	vaad all MAC address were cleared.
	All authentication-registered MAC addresses were deleted because all the TCP connections between VAA and authentication servers were not established within the set number of retries. [Explanation of message variables] None. [Action] Make sure there is no network-related problem between the Switch and authentication server.				
6	E3	SOFTWARE	20410007	1001	vaad The socket with L2MacManager was closed.
	The socket between VAA and L2MacManager was closed. [Explanation of message variables] None. [Action] If this error occurs frequently, restart L2MacManager.				
7	E3	SOFTWARE	20410012	1001	VAA information defined by the configuration file is ignored, since VAA function license is not given.
	VAA information set in the startup configuration file is invalid because a license was not granted. [Explanation of message variables] None. [Action] Set the option license OP-VAA by using the `set license` command, and then restart the switch.				
8	E4	SOFTWARE	20410008	1001	The vaad MAC Address entry can't be registered at hardware tables.
	Using the VAA function, the MAC address of a terminal could not be set in the hardware table. [Explanation of message variables] None. [Action] Review the capacity limit. However, depending on the hardware specification, the setting to the maximum of the capacity limit might not be available.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
9	E4	SOFTWARE	20410009	1001	vaad failed to get configuration data.
	Retrieval of VAA function configuration data inside a switch failed. [Explanation of message variables] None. [Action] Delete the configuration of the VAA functionality, and then reset the VAA configuration.				
10	E4	SOFTWARE	20410010	1001	vaad failed to make temporary file.
	Creation of a VAA-function temporary file inside a switch failed. [Explanation of message variables] None. [Action] Delete the configuration of the VAA functionality, and then reset the VAA configuration.				
11	E4	SOFTWARE	20410011	1001	vaad was not able to get enough memory.
	Sufficient VAA memory failed to be reserved because switch memory capacity is insufficient. [Explanation of message variables] None. [Action] Delete the configuration of the VAA functionality, and then reset the VAA configuration.				
12	E7	SOFTWARE	20410001	1001	vaad aborted.
	The VAA program (vaad) was forced to stop. [Explanation of message variables] None. [Action] The VAA program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
13	R7	SOFTWARE	20410001	1001	vaad restarted.
	The VAA program (vaad) has restarted. The switch outputs this message when the VAA program restarts automatically or a restart is requested by the `restart vaa` command. [Explanation of message variables] None. [Action] Perform authentication again on the authentication client side.				

3.5 Port

3.5.1 Event location = PORT

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

Table 3-12: Device failure and event information when the event location is PORT

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
1	E3	PORT	25011000	1350	Port enabled administratively.
	The port was released from the disabled state by using the configuration commands `no shutdown` or `no schedule-power-control shutdown`. [Explanation of message variables] None. [Action] None.				
2	E3	PORT	25011006	1350	Port activated administratively.
	The port was released from the inactive state by using the `activate` command. [Explanation of message variables] None. [Action] None.				
3	E3	PORT	25011100	1350	Port disabled administratively.
	The port was placed in the disabled state by using the configuration commands `shutdown` or `schedule-power-control shutdown`. [Explanation of message variables] None. [Action] None.				
4	E3	PORT	25011106	1350	Port inactivated administratively.
	The port was placed in the inactive state by using the `inactivate` command. [Explanation of message variables] None. [Action] None.				
5	E3	PORT	25020601	1350	Supplying power was stopped by the overload detection.
	The power supply was stopped because a power overload was detected. [Explanation of message variables] None. [Action] Check the devices receiving the power. Also, if the inter-connected switches are capable of PoE power supply, use a configuration command to disable the PoE function of the relevant ports. For details on PoE function settings, see *14.13 Configuration of PoE [AX3630S]* in the manual *Configuration Guide Vol. 1 For Version 11.10*.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
6	E3	PORT	25230000	1350	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. [Explanation of message variables] None. [Action] Change the bandwidth to inside the setting range. For details about the valid setting range, see the `rate` parameter description in *traffic-shape rate* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.				
7	E3	PORT	25230001	1350	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. [Explanation of message variables] None. [Action] Change the units to specifiable units. For details on specifiable setting units, see the `rate` parameter description in *traffic-shape rate* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.				
8	E3	PORT	25230002	1350	Port half duplex does not support traffic-shape rate feature.
	Port bandwidth control is not available for half-duplex lines. [Explanation of message variables] None. [Action] Do either of the following: 1. If port bandwidth control is to be used, switch to a full-duplex line. 2. If a half-duplex line is to be used, delete port bandwidth control by using the configuration command `no traffic-shape rate`.				
9	E3	PORT	25230003	1350	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. [Explanation of message variables] <*queue no.*>: Queue number [Action] Change the minimum guaranteed bandwidth to a value inside the range of valid settings. For details on the range of valid settings, see the `wfq` parameter description in *qos-queue-list* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.				
10	E3	PORT	25230004	1350	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. [Explanation of message variables] <*queue no.*>: Queue number [Action] Change the units to specifiable units. For details on the specifiable setting range, see the `wfq` parameter description in *qos-queue-list* in the manual *Configuration Command Reference Vol. 1 For Version 11.10*.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
11	E3	PORT	25230005	1350	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. [Explanation of message variables] None. [Action] Using the configuration command `qos-queue-list`, adjust the total value of the minimum guaranteed bandwidths so that the total is within the maximum send bandwidth.				
12	E3	PORT	25230006	1350	Port half duplex does not support WFQ feature.
	The scheduling mode that includes WFQ is not available for half-duplex lines. [Explanation of message variables] None. [Action] Do either of the following: 1. If WFQ is to be used in the scheduling mode, switch to a full-duplex line. 2. If a half-duplex line is to be used, switch to a scheduling mode that does not include WFQ by using the configuration commands `qos-queue-group` and `qos-queue-list`.				
13	E4	PORT	25011001	1350	Port up.
	The port is up. [Explanation of message variables] None. [Action] None.				
14	E4	PORT	25011002	1350	Transceiver connected.
	A transceiver insertion was detected. [Explanation of message variables] None. [Action] None.				
15	E4	PORT	25011101	1350	Error detected on the port.
	Errors were detected at the ports. [Explanation of message variables] None. [Action] For 10BASE-T, 100BASE-TX, or 1000BASE-T: 1. Make sure that the specified cables are properly connected. 2. Make sure that startup of the partner switch has completed. 3. Execute the `test interfaces` command, and make sure that the switches and cables have no problem. For 100BASE-FX, 1000BASE-X, or 10GBASE-R: 1. Make sure that the specified cables are properly connected. Make sure that the end sections of the cables are clean. If they are dirty, clean them. 2. If you are using an optical attenuator, check the attenuation value. 3. Make sure that startup of the partner switch has completed. 4. Execute the `test interfaces` command, and make sure that the switches and cables have no problem.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
16	E4	PORT	25011102	1350	Transceiver notconnected.
	A transceiver removal was detected. [Explanation of message variables] None. [Action] Insert the transceiver properly.				
17	E4	PORT	25011103	1350	Auto negotiation failed.
	Auto negotiation has failed. [Explanation of message variables] None. [Action] • Check the auto negotiation status. • Execute the `test interfaces` command, and make sure that the cables have no problem. • If the devices and the cables are normal, check the destination devices.				
18	E4	PORT	25011104	1350	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. [Explanation of message variables] None. [Action] • Execute the `test interfaces` command, and make sure that the cables have no problem. • If the devices and the cables are normal, check the destination devices.				
19	E4	PORT	25011105	1350	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. [Explanation of message variables] None. [Action] • Execute the `test interfaces` command, and make sure that the switches and cables have no error. • If the devices and the cables are normal, check the destination devices.				
20	E4	PORT	25011500	1350	Transceiver not supported.
	An unsupported transceiver was detected. [Explanation of message variables] None. [Action] See the *SFP List* and *XFP List* in the *Hardware Instruction Manual*. Insert a supported transceiver into the corresponding port number.				
21	E4	PORT	25100009	1350	NIF <*nif no.*> Port <*port no.*>:inactivated because of broadcast storm detection.
	A port was deactivated because a broadcast storm was detected. [Explanation of message variables] <*nif no.*>: NIF number <*port no.*>: Port number [Action] After recovering from the storm, use the `activate` command to change the port status to active.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
22	E4	PORT	2510000a	1350	NIF <*nif no.*> Port <*port no.*>:broadcast storm detected.
	A broadcast storm was detected. [Explanation of message variables] <*nif no.*>: NIF number <*port no.*>: Port number [Action] None.				
23	E4	PORT	2510000b	1350	NIF <*nif no.*> Port <*port no.*>:broadcast storm recovered.
	The system has recovered from a broadcast storm. [Explanation of message variables] <*nif no.*>: NIF number <*port no.*>: Port number [Action] None.				
24	E4	PORT	2510000c	1350	NIF <*nif no.*> Port <*port no.*>:inactivated because of multicast storm detection.
	A port was deactivated because a multicast storm was detected. [Explanation of message variables] <*nif no.*>: NIF number <*port no.*>: Port number [Action] After recovering from the storm, use the `activate` command to change the port status to active.				
25	E4	PORT	2510000d	1350	NIF <*nif no.*> Port <*port no.*>:multicast storm detected.
	A multicast storm was detected. [Explanation of message variables] <*nif no.*>: NIF number <*port no.*>: Port number [Action] None.				
26	E4	PORT	2510000e	1350	NIF <*nif no.*> Port <*port no.*>:multicast storm recovered.
	The system has recovered from a multicast storm. [Explanation of message variables] <*nif no.*>: NIF number <*port no.*>: Port number [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
27	E4	PORT	2510000f	1350	NIF <*nif no.*> Port <*port no.*>:inactivated because of unicast storm detection.
	A port was deactivated because a unicast storm was detected. [Explanation of message variables] <*nif no.*>: NIF number <*port no.*>: Port number [Action] After recovering from the storm, use the `activate` command to change the port status to active.				
28	E4	PORT	25100010	1350	NIF <*nif no.*> Port <*port no.*>:unicast storm detected.
	A unicast storm was detected. [Explanation of message variables] <*nif no.*>: NIF number <*port no.*>: Port number [Action] None.				
29	E4	PORT	25100011	1350	NIF <*nif no.*> Port <*port no.*>:unicast storm recovered.
	The system has recovered from a unicast storm. [Explanation of message variables] <*nif no.*>: NIF number <*port no.*>: Port number [Action] None.				
30	E4	PORT	25100012	1350	NIF <*nif no.*> Port <*port no.*>:inactivated because of uni-directional link detection.
	A port was deactivated because a unidirectional link failure was detected. [Explanation of message variables] <*nif no.*>: NIF number <*port no.*>: Port number [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 switches and cables have no error. • If the devices and the cables are normal, check the destination devices. After the above, activate the port by using the `activate` command.				
31	E4	PORT	25100013	1350	NIF <*nif no.*> Port <*port no.*>:inactivated because of loop detection.
	A port was deactivated because a loop was detected. [Explanation of message variables] <*nif no.*>: NIF number <*port no.*>: Port number [Action] Check the network configuration.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
32	E8	PORT	25020201	1350	Port restarted because of its hardware failure.
	A port was restarted because a hardware failure occurred at the port. [Explanation of message variables] None. [Action] Check subsequent fault recovery log entries or fault recovery failure log entries. If the system has recovered from the fault, 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 implemented, make sure that it is firmly installed.				
33	E8	PORT	25020202	1350	Port stopped because of its hardware failure.
	A port was stopped because a hardware failure occurred at the port. [Explanation of message variables] None. [Action] Switch to an unused port. If you want to reuse the failed port, replace the device.				
34	E8	PORT	25020401	1350	Port restarted, but not recovered from hardware failure.
	A port restarted, but the port has not recovered from a hardware failure. [Explanation of message variables] None. [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. The system may not recover by executing step 1. In that case, change the transceiver after executing the `inactivate` command, and then execute the `activate` command. 3. If the recovery failed after steps 1 or 2, 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.				
35	R8	PORT	25020201	1350	Port recovered from hardware failure.
	A port has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

3.5.2 Event location = ULR

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

Table 3-13: Device failure and event information when the event location is ULR

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
1	E4	ULR	20a00001	2400	ULR:Active port is switched to secondary port(<*nif no.*>/<*port no.*>) from primary port(<*nif no.*>/<*port no.*>).
	The active port was switched to the secondary port because an error occurred in the primary port. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number [Action] Check the failure in the primary port.				
2	E4	ULR	20a00002	2400	ULR:Active port is switched to primary port(<*nif no.*>/<*port no.*>) from secondary port(<*nif no.*>/<*port no.*>).
	The active port was switched to the primary port because an error occurred in the secondary port. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number [Action] Check the failure in the secondary port.				
3	E4	ULR	20a00003	2400	ULR:Active port is switched to secondary port(<*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. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] Check the failure in the primary port.				
4	E4	ULR	20a00004	2400	ULR:Active port is switched to primary port(<*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. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] Check the failure in the secondary port.				
5	E4	ULR	20a00005	2400	ULR:Active port is switched to secondary port(ChGr:<*channel group number*>) from primary port(<*nif no.*>/<*port no.*>).
	The active port was switched to the secondary port because an error occurred in the primary port. [Explanation of message variables] <*channel group number*>: Channel group number <*nif no.*>/<*port no.*>: NIF number/port number [Action] Check the failure in the primary port.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
6	E4	ULR	20a00006	2400	ULR:Active port is switched to primary port(ChGr:<*channel group number*>) from secondary port(<*nif no.*>/<*port no.*>).
	The active port was switched to the primary port because an error occurred in the secondary port. [Explanation of message variables] <*channel group number*>: Channel group number <*nif no.*>/<*port no.*>: NIF number/port number [Action] Check the failure in the secondary port.				
7	E4	ULR	20a00007	2400	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. [Explanation of message variables] <*channel group number*>: Channel group number [Action] Check the failure in the primary port.				
8	E4	ULR	20a00008	2400	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. [Explanation of message variables] <*channel group number*>: Channel group number [Action] Check the failure in the secondary port.				
9	E4	ULR	20a00009	2400	ULR:Active port is switched to secondary port(<*nif no.*>/<*port no.*>) from primary port(<*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. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number [Action] None.				
10	E4	ULR	20a00010	2400	ULR:Active port is switched to primary port(<*nif no.*>/<*port no.*>) from secondary port(<*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. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
11	E4	ULR	20a00011	2400	ULR:Active port is switched to secondary port(<*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. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] None.				
12	E4	ULR	20a00012	2400	ULR:Active port is switched to primary port(<*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. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] None.				
13	E4	ULR	20a00013	2400	ULR:Active port is switched to secondary port(ChGr:<*channel group number*>) from primary port(<*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. [Explanation of message variables] <*channel group number*>: Channel group number <*nif no.*>/<*port no.*>: NIF number/port number [Action] None.				
14	E4	ULR	20a00014	2400	ULR:Active port is switched to primary port(ChGr:<*channel group number*>) from secondary port(<*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. [Explanation of message variables] <*channel group number*>: Channel group number <*nif no.*>/<*port no.*>: NIF number/port number [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
15	E4	ULR	20a00015	2400	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. [Explanation of message variables] <*channel group number*>: Channel group number [Action] None.				
16	E4	ULR	20a00016	2400	ULR:Active port is switched to primary ChGr(<*channel group number*>) from secondary 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. [Explanation of message variables] <*channel group number*>: Channel group number [Action] None.				
17	E4	ULR	20a00017	2400	ULR:Primary port(<*nif no.*>/<*port no.*>) became the active port.
	The primary port has become the active port. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number [Action] None.				
18	E4	ULR	20a00018	2400	ULR:Primary port(ChGr:<*channel group number*>), became the active port.
	The primary port has become the active port. [Explanation of message variables] <*channel group number*>: Channel group number [Action] None.				
19	E4	ULR	20a00019	2400	ULR:Secondary port(<*nif no.*>/<*port no.*>) became the active port.
	The secondary port has become the active port. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number [Action] None.				
20	E4	ULR	20a00020	2400	ULR:Secondary port(ChGr:<*channel group number*>) became the active port.
	The secondary port has become the active port. [Explanation of message variables] <*channel group number*>: Channel group number [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
21	E4	ULR	20a00021	2400	ULR:Both uplink redundant port(<*nif no.*>/<*port no.*>) and port(<*nif no.*>/port no.>) are down.
	Both the primary port and the secondary port have gone down. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number [Action] Make sure that no error occurred between the primary and secondary port.				
22	E4	ULR	20a00022	2400	ULR:Both uplink redundant port(<*nif no.*>/<*port no.*>) and port(ChGr:<*channel group number*>) are down.
	Both the primary port and the secondary port have gone down. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] Make sure that no error occurred between the primary and secondary port.				
23	E4	ULR	20a00023	2400	ULR:Both uplink redundant port(ChGr:<*channel group number*>) and port(<*nif no.*>/<*port no.*>) are down.
	Both the primary port and the secondary port have gone down. [Explanation of message variables] <*channel group number*>: Channel group number <*nif no.*>/<*port no.*>: NIF number/port number [Action] Make sure that no error occurred between the primary and secondary port.				
24	E4	ULR	20a00024	2400	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. [Explanation of message variables] <*channel group number*>: Channel group number [Action] Make sure that no error occurred between the primary and secondary port.				
25	E4	ULR	20a00025	2400	ULR:Active port is switched to primary port(<*nif no.*>/<*port no.*>) from secondary port(<*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. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
26	E4	ULR	20a00026	2400	ULR:Active port is switched to primary port(<*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. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number <*channel group number*>: Channel group number [Action] None.				
27	E4	ULR	20a00027	2400	ULR:Active port is switched to primary port(ChGr:<*channel group number*>) from secondary port(<*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. [Explanation of message variables] <*channel group number*>: Channel group number <*nif no.*>/<*port no.*>: NIF number/port number [Action] None.				
28	E4	ULR	20a00028	2400	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. [Explanation of message variables] <*channel group number*>: Channel group number [Action] None.				
29	E4	ULR	20a00029	2400	ULR:Exceeded the number of MAC Address Table entry update request to uplink-switch from active port(<*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. [Explanation of message variables] <*nif no.*>/<*port no.*>: NIF number/port number [Action] None.				
30	E4	ULR	20a00030	2400	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. [Explanation of message variables] <*channel group number*>: Channel group number [Action] None.				

3.6 Optional module

3.6.1 Event location = PS

The following table describes device failure and event information when the event location is PS.

Table 3-14: Device failure and event information when the event location is PS

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
1	E3	PS	00000003	2200	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. [Explanation of message variables] <*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.				
2	E8	PS	00000001	2200	<*ps*> is power off.
	The displayed power unit is off. <*ps*> displays the power unit (either PS or EPU) that is turned off. [Explanation of message variables] <*ps*>: PS or EPU [Action] 1. Check the power switch, and turn it on. 2. Check the power cable connection and the power source, and then connect them properly. 3. Check the implementation status of the EPU.				
3	E8	PS	00000002	2200	<*ps*> is power off.
	The displayed power supply unit is turned off. <*ps*> displays a power supply unit (either PS1 or PS2) that is turned off. [Explanation of message variables] <*ps*>: PS1 or PS2 [Action] 1. Check the power switch, and turn it on. 2. Check the power cable connection and the power source, and then connect them properly. 3. If the power supply unit has failed, replace it.				
4	E8	PS	00000004	2200	Error detected on EPU.
	The EPU detected a fault. [Explanation of message variables] None. [Action] 1. The power supply module installed on the EPU might be half-inserted. Insert the power supply module correctly. 2. If the power supply module installed on the EPU has failed, replace it.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
5	E8	PS	00000102	2200	Power unit isn't redundantly mounted.
	The power unit is not in a redundant configuration. [Explanation of message variables] None. [Action] Check the implementation status of the power supply unit. If the power unit is not implemented in a redundant configuration, set `no power redundancy-mode` by the configuration command.				
6	R8	PS	00000001	2200	<*ps*> is normal.
	The displayed power unit is operating normally. <*ps*> displays the power unit (either `PS` or `EPU`) that is in a normal state. This message appears when the following conditions are met: 1. When the power unit state changes from an anomalous state to a normal state, or from an unimplemented state to a normal state, the power unit in the normal state is displayed. 2. When an EPU is removed for a power unit that is in a redundant configuration, PS in a normal state is displayed. [Explanation of message variables] <*ps*>: `PS` or `EPU` [Action] None.				
7	R8	PS	00000002	2200	<*ps*> is normal.
	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: 1. When the power supply unit state changes from an anomalous state to a normal state, or from an unimplemented state to a normal state, the power supply unit in the normal state is displayed. 2. When either one of the power supply units in a redundant configuration is removed, the power supply unit in the normal state is displayed. [Explanation of message variables] <*ps*>: `PS1` or `PS2` [Action] None.				
8	R8	PS	00000004	2200	EPU recovered from error.
	The EPU is in a normal state. [Explanation of message variables] None. [Action] None.				
9	R8	PS	00000005	2200	EPU was removed.
	The EPU was removed. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
10	R8	PS	00000102	2200	Power unit is mounted redundantly or mode changed.
	The power unit is in a redundant configuration. The operation mode was changed. [Explanation of message variables] None. [Action] None.				

3.6.2 Event location = EQUIPMENT

The following table describes device failure and event information when the event location is `EQUIPMENT`.

Table 3-15: Device failure and event information when the event location is EQUIPMENT

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
1	E3	EQUIPMENT	00000003	2101	Failed in accumulated running time access to main.
	Access to the total operating time for the switch failed. [Explanation of message variables] None. [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 device.				
2	E3	EQUIPMENT	00020106	2101	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. [Explanation of message variables] <*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.).				
3	E3	EQUIPMENT	00020107	2101	The temperature of hardware came down from the warning level.
	The hardware temperature has been 3 degrees Celsius or more lower than the temperature that is set with the `system temperature-warning-level` configuration command. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
4	E3	EQUIPMENT	25040b01	2101	Layer-2 hardware table entry can't be registered. Change to recommended l2-table mode <*mode*>.
	An entry could not be registered in the Layer 2 hardware table. Change the search method for the Layer 2 hardware table to <*mode*>. [Explanation of message variables] <*mode*>: Search method of the Layer 2 hardware table after the change [Action] None.				
5	E3	EQUIPMENT	25040b02	2101	Layer-2 hardware table entry can't be registered. The recommended l2-table mode is <*mode*>.
	An entry could not be registered in the Layer 2 hardware table. The search method for the most optimal Layer 2 hardware table is <*mode*>. [Explanation of message variables] <*mode*>: Search method of the most optimal Layer 2 hardware table [Action] When using the search method displayed in this message, change the configuration command `system l2-table mode`, and execute the `restart vlan` command.				
6	E3	EQUIPMENT	25040b03	2101	The recommended l2-table mode can't be selected.
	The search method for the most optimal Layer 2 hardware table could not be selected. [Explanation of message variables] None. [Action] Review the system configuration.				
7	E3	EQUIPMENT	25040c01	2101	Corrected memory soft errors.
	The system has recovered from a memory software error. Some frames may be discarded because of the software error. [Explanation of message variables] None. [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.				
8	E7	EQUIPMENT	00020102	2101	Hardware exceeded tolerance level of low temperature(<*temperature*> degree). Check room temperature.
	The hardware temperature went below the permissible temperature range (<*temperature*> degrees Celsius or lower). [Explanation of message variables] <*temperature*>: 0 [Action] 1. Check and, if necessary, improve the environment such as the room temperature around the switches. 2. Check and, if necessary, replace the fan.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
9	E7	EQUIPMENT	00020103	2101	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*> degrees Celsius or higher). [Explanation of message variables] <*temperature*>: 40 [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check and, if necessary, replace the fan.				
10	E8	EQUIPMENT	00000001	2102	FAN stopped.
	A failure was detected at the displayed fan. You can identify the stopped fan by the additional information. Additional information = 2102:ABCD******** "*" represents an indefinite value. It can be ignored. A, B, C, and D correspond to the fan numbers. A=FAN4 0=Normal, 1=Stopped B=FAN3 0=Normal, 1=Stopped C=FAN2 0=Normal, 1=Stopped D=FAN1 0=Normal, 1=Stopped [Explanation of message variables] None. [Action] Replace the Switch.				
11	E8	EQUIPMENT	25040201	2101	Hardware restarted because of its failure.
	The switch was restarted because a hardware failure occurred at the switch. [Explanation of message variables] None. [Action] Check subsequent fault recovery log entries or fault recovery failure log entries. If the recovery was successful, operations can resume. If the recovery failed, replace the device.				
12	E8	EQUIPMENT	25040400	2101	Hardware restarted, but not recovered.
	The device restarted, but it has not recovered from a hardware failure. [Explanation of message variables] None. [Action] Replace the Switch.				
13	E9	EQUIPMENT	00020105	2101	Hardware is becoming high temperature which give damage to this system. (<*temperature*> degree).
	The hardware temperature has reached a temperature (<*temperature*> degrees Celsius or higher) that is likely to critically damage device operation. [Explanation of message variables] <*temperature*> Detected temperature (60 degrees Celsius or higher) [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check and, if necessary, replace the fan.				

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
14	R7	EQUIPMENT	00020102	2101	The temperature of hardware returned to normal level (<*temperature*> degree).
	The hardware temperature returned to normal (<*temperature*> degrees Celsius). [Explanation of message variables] <*temperature*>: 3 [Action] None.				
15	R7	EQUIPMENT	00020103	2101	The temperature of hardware returned to normal level (<*temperature*> degree).
	The hardware temperature returned to normal (<*temperature*> degrees Celsius). [Explanation of message variables] <*temperature*>: 37 [Action] None.				
16	R8	EQUIPMENT	00000001	2102	FAN is normal.
	The displayed fan is in a normal state. You can identify the state of other fans with the additional information. Additional information = 2102:ABCD******** "*" represents an indefinite value. It can be ignored. A, B, C, and D correspond to the fan numbers. A=FAN4 0=Normal, 1=Stopped B=FAN3 0=Normal, 1=Stopped C=FAN2 0=Normal, 1=Stopped D=FAN1 0=Normal, 1=Stopped [Explanation of message variables] None. [Action] None.				
17	R8	EQUIPMENT	25040200	2101	Hardware initialized.
	The hardware has been initialized. [Explanation of message variables] None. [Action] None.				
18	R8	EQUIPMENT	25040201	2101	Hardware recovered.
	The switch recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

3.6.3 Event location = FAN

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

Table 3-16: Device failure and event information when the event location is FAN

#	Event level	Event location	Message ID	Added info Highest 4 digits	Message text
	Description				
1	E3	FAN	00000003	1800	Failed in accumulated running time access to <*fan*>.
	Access to the total operating time for the fan unit failed. <*fan*> displays a fan unit (either FAN1 or FAN2) for which access to the total operating time has failed. [Explanation of message variables] <*fan*>: FAN1 or FAN2 [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.				
2	E3	FAN	00000004	1800	Failed in accumulated running time access to the fan unit.
	Access to the total operating time for the fan unit failed. [Explanation of message variables] None. [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.				
3	E8	FAN	00000002	1800	<*fan*> stopped.
	The displayed fan has stopped or is not implemented. <*fan*> displays a fan that has stopped or is not implemented. [Explanation of message variables] Any of `FAN1(1)`, `FAN1(2)`, `FAN2(1)`, or `FAN2(2)` [Action] 1. Check the implementation status of the power supply unit or fan unit. Check the implementation status either visually or by using the `show system` command. 2. If the power supply unit or fan unit has failed, replace it.				
4	R8	FAN	00000002	1800	<*fan*> is normal.
	The displayed fan is in a normal state. <*fan*> displays a fan in a normal state. [Explanation of message variables] Any of `FAN1(1)`, `FAN1(2)`, `FAN2(1)`, or `FAN2(2)` [Action] None.				

Chapter

4. Tracking Object Log [AX3640S] [OS-L3A]

This chapter describes the log data output by the tracking functionality of the policy-based routing.

4.1 Tracking object log

The following table describes the tracking object log.

Table 4-1: Tracking object log

#	Message text	Description
1	Track object <*track object id*> is up. (type ICMP, address <*destination address*>)	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 [Action] None.
2	Track object <*track object id*> is down. (type ICMP, address <*destination address*>)	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 [Action] None.

Index

V