AX6700S/AX6600S/AX6300S Software Manual

Message and Log Reference

For Version 11.7

AX63S-S008X-C0

AlaxalA

■ Relevant products

This manual applies to the models in the AX6700S, AX6600S, and AX6300S series of switches. It also describes the functionality of version 11.7 of the software for the AX6700S, AX6600S, and AX6300S series switches. The described functionality is that supported by the OS-S/OS-SE basic software and 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.

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 Lucent Technologies.

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.

■ Note

Information in this document is subject to change without notice.

■ Edition history

January 2012 (Edition 13) AX63S-S008X-C0

■ Copyright

All Rights Reserved, Copyright(C), 2006, 2012, ALAXALA Networks, Corp.

History of Amendments

[For Version 11.7]

Summary of amendments

Location and title	Changes
1.2 Checking logs	• A description of the tracking object log was added.
2.4.1 PIM-SM/PIM-DM	• Log messages related to the IPv4 PIM-SM relay-forwarding functionality during a system switchover were added.
3.4.1 Event location = SOFTWARE	• Log messages related to policy-based routing and policy-based switching were added. • Log messages related to the policy-based routing tracking functionality were added.
5 Tracking Object Log	• This chapter was added.

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

[For Version 11.5]

Summary of amendments

Item	Changes
Log type	• Notes were added to Table 1-4 Features of the operation log and reference log.
PIM-SM/PIM-DM	• A description related to PIM-DM was added.
Event location = SOFTWARE	• Log messages related to managing the switch were added. • A description of the tracking functionality was changed. • Log messages related to IPv4 multicast routing were added.
Event location = BCU	• Log messages related to managing the switch were added.
Event location = CSU	• Log messages related to managing the switch were added.
Event location = MSU	• Log messages related to managing the switch were added.

[For Version 11.4]

Summary of amendments

Item	Changes
Event location = ACCESS	• A description of VRF was added.
Event location = SOFTWARE	• A description of VRF was added to log messages related to SNMP. • Log messages related to IPv6 DHCP relays were added. • Log messages related to the traffic-based power saving functionality were added. • Descriptions of traffic-based power saving were added to log messages related to the traffic-based power saving functionality. • Log messages related to DHCP snooping were added.
Event location = NIF	• Log messages related to NIF redundancy were added.

[For Version 11.3]

Summary of amendments

Item	Changes
Checking the log	• A description of the access list log was added.

Item	Changes
IPv6 multicast routing information (MR6)	• Log messages related to VRF were added.
Event location = SOFTWARE	• A description of VRF was added to log messages related to IPv6 multicasts. • Log messages related to IPv6 multicasts were added. • Log messages related to access list logging were added.
Access list log	• This chapter was added.

[For Version 11.2]

Summary of amendments

Item	Changes
BGP4+	• A description of VRF was added.
Common to IPv6 unicast routing protocols	• Log messages related to VRF were added.
Event location = VLAN (Ring Protocol)	• Log messages related to path switch-back suppression functionality were added.
Event location = SOFTWARE	• A description of VRF was added to log messages related to NTP. • Log messages related to VRRP tracking functionality were added.
Event location = BCU	• Log messages related to health checks were added.
Event location = CSU	• Log messages related to health checks were added.
Event location = MSU	• Log messages related to health checks were 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.
Event location = SOFTWARE	• Log messages related to the power saving functionality were added.
Event location = PS	• A description of CSU was added.
Control and switching unit	• This section was added.
Event location = MSU	• Log messages related to unknown MSU boards were added.
Log information for the system operation panel (KEY)	• A description of the AX6600S series switches was added.
Log information for the system operation panel (RSP)	• A description of the AX6600S series switches was added.

[For Version 11.0]

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.

Item	Changes
Common to IPv4 unicast routing protocols	• Log messages related to VRF were added.
PIM-SM	• A description of VRF was added.
Event location = VLAN	• Log messages for clearing the MAC address table by receiving ordinary Flush Request frames were added.
Event location = VLAN (GSRP)	• Log messages for when the automatic master wait time elapsed were added.
Event location = SOFTWARE	• Log messages related to the VRRP group switchover functionality were added. • Log messages related to multicasts were added. • A description of VRF was added to log messages related to multicasts. • Log messages were added in regards to supporting the option license OP-NPAR.
Event location = NIF	• Log messages related to the layering shaper were added.
Event location = PORT	• Log messages indicating that the half duplex mode is unsupported were added. • Log messages related to the layering shaper were added.
Event location = NK1GS-8M	• This subsection was added.
Event location = NH1GS-6M	• This subsection was added.

[For Version 10.7]

Summary of amendments

Item	Changes
BGP4	• Log messages related to BGP4 were added.
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 (detecting L2 loops)	• 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 = CONFIG	• Log messages indicating configurations corresponding to NIF boards were added.
Event location = SOFTWARE	• Log messages related to MAC-based authentication were added.
Event location = BSU	• Log messages were added because the BSU's fixed mode is now available.

[For Version 10.5]

Summary of amendments

Item	Changes
Common to IPv4 unicast routing protocols	• A new log message (item number 2) was 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 the Ring Protocol were added.

[For Version 10.3]

Summary of amendments

Item	Changes
OSPF	• New log messages (item numbers 13 to 16) were added.
BGP4	• New log messages (item numbers 103 to 105) were added.
OSPFv3	• New log messages (item numbers 13 to 16) were added.
BGP4+	• New log messages (item numbers 100 to 102) were added.
IPv6 PIM-SM	• New log messages (item numbers 23 to 24) were added.
Event location = ACCESS	• Log messages related to local command authentication were added. • Log messages related to dial-up connections were added.
Event location = VLAN	• Log messages related to IGMP snooping and MLD snooping were added.
Event location = SOFTWARE	• Log messages related to IEEE802.3ah/UDLD were added. • Log messages related to Web authentication were added. • Log messages related to IGMP snooping and MLD snooping were added. • Log messages related to sFlow were added.
Event location = BSU	• This subsection was added.
Event location = PORT	• Log messages related to IEEE802.3ah/UDLD were added. • Log messages related to storm control were added.
Event location = BCU	• This subsection was added.
Basic switching unit	• This section was added.
AX6700S series network interface board	• This section was added.
AX6300S series network interface board	• The following items were added: • Event location = NH1G-24T • Event location = NH1G-24S • Event location = NH10G-4RX • Event location = NH10G-8RX

Preface

Applicable products and software versions

This manual applies to the models in the AX6700S, AX6600S, and AX6300S series of switches. The manual describes the functionality in software version 11.7 for the AX6700S, AX6600S, and AX6300S series switches that is supported by the OS-S/OS-SE basic software and optional licenses.

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

Unless otherwise noted, this manual describes functionality applicable to AX6700S, AX6600S, and AX6300S series switches. Functionality specific to a model is indicated as follows:

[AX6700S]:

The description applies to the AX6700S series.

[AX6600S]:

The description applies to the AX6600S series.

[AX6300S]:

The description applies to the AX6300S series.

Unless otherwise noted, this manual describes functionality applicable to the basic software OS-S/OS-SE. Functionality specific to an optional license is indicated as follows:

[OP-BGP]:

The description applies to optional license OP-BGP.

[OP-DH6R]:

The description applies to the optional license OP-DH6R.

[OP-MBSE]:

The description applies to the optional license OP-MBSE.

[OP-NPAR]:

The description applies to optional license OP-NPAR.

[OP-VAA]:

The description applies to the optional license OP-VAA.

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**

AX6700S Quick Start Guide (AX67S-Q001X)	AX6600S Quick Start Guide (AX66S-Q001X)	AX6300S Quick Start Guide (AX63S-Q001X)

● **Determining the hardware setup requirements and how to handle the hardware**

AX6700S Hardware Instruction Manual (AX67S-H001X)	AX6600S Hardware Instruction Manual (AX66S-H001X)	AX6300S Hardware Instruction Manual (AX63S-H001X)

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

▽ First, see the following guides to check the functions and device capacities.

- Device capacities **- Basic operations, such as logging in** **- VLANs and Spanning Tree Protocols**	**- Filtering and QoS** **- Layer 2 authentication** **- High-reliability functionality**	**- IPv4 and IPv6 packet forwarding** **- IPv4 and IPv6 routing protocols**
Configuration Guide Vol. 1 (AX63S-S001X)	Configuration Guide Vol. 2 (AX63S-S002X)	Configuration Guide Vol. 3 (AX63S-S003X)

▽ If necessary, see the following references.

- Learning the syntax of commands and the details of command parameters

Configuration Command Reference Vol. 1 (AX63S-S004X)	Configuration Command Reference Vol. 2 (AX63S-S010X)	Configuration Command Reference Vol. 3 (AX63S-S005X)
Operation Command Reference Vol. 1 (AX63S-S006X)	Operation Command Reference Vol. 2 (AX63S-S011X)	Operation Command Reference Vol. 3 (AX63S-S007X)

- Understanding messages and logs

Message and Log Reference (AX63S-S008X)

- Understanding MIBs

MIB Reference (AX63S-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:

AX6700S series switch

AX6600S series switch

AX6300S 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
BCU         Basic Control Unit
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
BSU         Basic Switching Unit
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
CSU         Control and Switching Unit
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
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
LLPQ        Low Latency Priority Queueing
LLQ+3WFQ    Low Latency Queueing + 3 Weighted Fair Queueing
LLRLQ       Low Latency Rate Limited 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
MSU         Management and Switching Unit
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
NIF         Network Interface
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
PRI         Primary Rate Interface
```

```
PS          Power Supply
PSNP        Partial Sequence Numbers PDU
PSP         Packet Switching Processor
QoS         Quality of Service
RA          Router Advertisement
RADIUS      Remote Authentication Dial In User Service
RDI         Remote Defect Indication
REJ         REJect
RFC         Request For Comments
RGQ         Rate Guaranteed Queueing
RIP         Routing Information Protocol
RIPng       Routing Information Protocol next generation
RMON        Remote Network Monitoring MIB
RPF         Reverse Path Forwarding
RQ          ReQuest
RSTP        Rapid Spanning Tree Protocol
SA          Source Address
SD          Secure Digital
SDH         Synchronous Digital Hierarchy
SDU         Service Data Unit
SEL         NSAP SELector
SFD         Start Frame Delimiter
SFP         Small Form factor Pluggable
SMTP        Simple Mail Transfer Protocol
SNAP        Sub-Network Access Protocol
SNMP        Simple Network Management Protocol
SNP         Sequence Numbers PDU
SNPA        Subnetwork Point of Attachment
SOP         System Operational Panel
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
uRPF        unicast Reverse Path Forwarding
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
WGQ         Weighted Guaranteed 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 the operation messages and logs, which are used in the event of a failure to identify where errors have occurred.

1.1 Checking operation messages

The Switch outputs to an operation terminal as operation messages changes in the operating status, failure information, and other kinds of information for the administrator. As well as being output to the terminal, operation messages are stored internally as an operation log. 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. Of these messages, those containing routing protocol event information and the failure and event information output by the Switch are called *operation messages*.

Table 1-1: Message types and references

Message type	Description	Reference
Configuration error message	Messages output by the Switch related to input of a configuration command	*Error Messages on Configuration Editing* in the *Configuration Command Reference*
Command response messages	Messages output by the Switch for command input	*Response Messages* section of each command in the *Operation Command Reference*
Operation message	Event information for routing protocols	*2. Routing Event Information*
	Device failure information and event information	*3. Switch Failure and Event Information*

1.1.2 Contents of operation messages

Event information for routing protocols includes both functional items output by the Switch 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 message
Event information for routing protocols	IPv4 routing information	Yes
	IPv4 multicast routing information	No
	IPv6 routing information	Yes
	IPv6 multicast routing information	No
Switch failure and event information	Error information for a switch event location	Yes
	Event information for a switch event location	Yes

Legend:

Yes: Messages are displayed.

No: Messages are not displayed.

1.1.3 Format of operation messages

(1) Event information for routing protocols

The following figure shows the format of the event information for routing protocols.

Figure 1-1: Format of routing protocol event information

```
mm/dd hh:mm:ss        tttttttttttttt-tttttttttttttt
       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) Switch failure and event information

The following figure shows the format of the switch 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 functionality

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

5. Message identifier

6. Additional information

7. Message text

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

1.1.4 Outputting operation messages

(1) Event information for routing protocols

Routing protocol event information reports the operating status of the 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) Switch failure and event information

All switch failure and event information messages are output to the operation terminal window. Depending on the error severity or the 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 logs

1.2.1 Log type

The Switch acquires two types of logs: an operation log and a reference log. The operation log acquires entered commands, 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 statistical information 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	• Events that occurred are acquired in chronological order.[1], [2]	• Statistical information is recorded for each event, such as the time of the first and last occurrences, and the total number of occurrences.
Maintenance information that is acquired	• Entered commands • Command response messages • Event information for routing protocols • Switch failure and event information • Access list log	• Switch failure and event information
Number of acquired entries	• 10000 entries can be acquired. Within those, the first 5000 log entries are saved chronologically. • The remaining 5000 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. • If the number of log entries exceeds 500, entries that have a lower event level will be deleted, and new entries are acquired.
Overflow processing when the log size is exceeded	• If the number of log entries exceeds 5000, 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 5001 to 10000. If the number of log entries exceeds 10000, old log entries are deleted.	• If the number of log entries exceeds 500 entries, entries that have a lower event level are deleted, and new entries are acquired.

#1: Log messages indicating the reason the switch is rebooted are collected after log messages indicating that the switch started, even though the timestamps of log messages indicating the reason the switch rebooted come before the timestamps of log messages indicating that the switch started.

#2: If a log message related to a switch failure and a log message containing event information are generated at the same time, events with the same time might not be displayed in the chronological order that the events occurred in, or log messages might be displayed in reverse chronological order when log messages related to switch failures and log messages containing event information occur at the same time as other types of log messages.

1.2.2 Log contents

The following table describes the information acquired in the operation log and the 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	Yes	No	--
Command response messages	Messages output by switches to respond to entered commands	Yes	No	*Response Messages* section of each command in the *Operation Command Reference*
Event information for routing protocols	Routing protocol event information	Yes	No	*2. Routing Event Information*
	IPv4 multicast routing information	Yes	No	
	IPv6 routing protocol information	Yes	No	
	IPv6 multicast routing information	Yes	No	
Switch failure and event information	Error information for a switch event location	Yes	Yes	*3. Switch Failure and Event Information*
	Event information for a switch event location	Yes	Yes	
Access list log	Information output by access list logging about the packets discarded by a filter	Yes	No	*4. Access List Logs*
Tracking object log	Information about the policy-based routing tracking functionality	Yes	No	*5. Tracking Object Log*

Legend:

Yes: Messages are displayed or log data is acquired.

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

--: Not applicable.

1.2.3 Format of operation logs

Current messages are saved on the device as operation log data. When log data is stored, it is formatted with a *log type* for output as operation messages to the window.

(1) Event information for routing protocols

The following figure shows the format of the event information for entered commands, command response messages, and routing protocols.

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

```
kkk    mm/dd hh:mm:ss    tttttttttttttt-tttttttttttttt
 1           2                         3
```

1.   Log type: A three-letter identification code assigned to each provided functionality.

   • KEY: Operational information selected by entered commands

- **RSP**: Event information related to command response messages.
- **RTM**, **MRP**, and **MR6**: Event information for a routing protocol

2. Time: Date and time that the event occurred

3. Message text

(2) Switch failure and event information

The following figure shows the format of the switch failure and event information.

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

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

ttt-ttt
   8
```

1. Log type: A three-letter identification code assigned to 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 functionality

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

6. Message identifier

7. Additional information

8. Message text

(3) Access list log

The following figure shows the format of the access list log.

Figure 1-5: Format of the access list log

```
kkk    mm/dd hh:mm:ss      ttttttttttttttt-ttttttttttttttt
 1            2                           3
```

1. Log type: A three-letter identification code assigned to each provided functionality.
   - ACL: Access list log

2. Time: Date and time that the event occurred

3. Message text

(4) Tracking object log

The following figure shows the format of the tracking object log.

Figure 1-6: Format of the tracking object log

```
kkk    mm/dd hh:mm:ss      ttttttttttttttt-ttttttttttttttt
 1            2                           3
```

1. Log type: A three-letter identification code assigned to each provided functionality.
   - TRO: Event information about the policy-based routing tracking functionality

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 log data in the order the error or event occurs, and are also saved as reference log data. A reference log categorizes information by message ID, and then records the time of the first and last occurrences of an event and the total number of occurrences.

The following figure shows the format of a reference log entry.

Figure 1-7: Format of a reference log entry

```
ee    kkkkkkkk    [iii...iii]    xxxxxxxx    yyyy:yyyyyyyyyyyy
1        2             3             4              5


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

1. Event level (E9 to E3)

2. Event location or functionality

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

4. Message identifier

5. Additional information

6. Date and time of the last occurrence of the applicable error

7. Date and time of the first occurrence of the 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 assigned to the operation log entries:

- Command operation by the user and its result

- Operation information output by the switch

- Error information

The table below describes the correspondence between the information acquired as log entries and log entry type. An event level is assigned to switch failure and event information in an operation log and to a reference log.

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	--

Information to be acquired	Log type	Description	Event level
Switch failure and event information	ERR	Error information for a switch event location	E9 to E5
	EVT	Event information for a switch event location	E4, E3, R8 to R5
Access list log	ACL	Information output by access list logging about the packets discarded by a filter	--
Layer 2 authentication information	AUT	Information collected by a Layer 2 authentication function program. This information is displayed by the corresponding operation command. • show dot1x logging • show web-authentication logging • show mac-authentication logging	--
DHCP snooping information	DSN	Information collected by DHCP snooping. This information is displayed by the corresponding operation command. • show ip dhcp snooping logging	--
Tracking object log	TRO	Information about the policy-based routing tracking functionality	--

Legend: --: Not applicable.

(2) Event levels

Events in the reference log are classified into seven levels depending on their severity. The following table describes the event levels and the displayed information.

Table 1-7: Event levels and their contents

Event level	Display contents (type)	Description
9	E9 (fatal error)	This failure stops the entire Switch. (The system might be restarted or operation might stop.)
8	E8 (critical error) R8 (recover from critical error)	This error stops a fan, the power supply, or a part of the switch. • If this error is due to a hardware error, the applicable hardware is restarted.
7	E7 (software error) R7 (recover from software error)	This error stops part of the software.
6	E6 (partial failure) R6 (recover from partial failure)	This failure stops some of the switch components (including an NIF).
5	E5 (error in the other system) R5 (recovery from an error in the other system)	This error is a redundancy error (switching is disabled).
4	E4 (network error)	This error is information related to lines (LAN).
3	E3 (warning)	This error is a warning.

Note that on recovery from an error whose event level is from E5 to E9, a relevant operation message whose event level is from R5 to R8 is output. Also, when an error from E5 to E9 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 locations

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

Table 1-8: Event locations

#	ID	Event location or functionality
1	CONFIG	Configuration
2	ACCESS	Switch access permissions control
3	IP	IP control functionality
4	VLAN	VLAN control functionality
5	MAC	MAC control functionality
6	SOFTWARE	Software control functionality
7	BSU	BSU control functionality
8	NIF	NIF control functionality
9	PORT	Port control functionality
10	FAN	Fan unit control functionality
11	PS	Power supply control functionality
12	BCU	Basic control unit
13	BSU-LA	Basic switching unit BSU-LA
14	BSU-LB	Basic switching unit BSU-LB
15	CSU	Control switching unit
16	MSU	Management and switching unit
17	NK1G-24T	24 10BASE-T, 100BASE-TX, or 1000BASE-T lines
18	NK1G-24S	24 1000BASE-X (SFP) lines
19	NK1GS-8M	Four 10BASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X SFP lines (user selectable) with the hierarchical shaper and four 1000BASE-X SFP lines with the hierarchical shaper
20	NK10G-4RX	Four 10GBASE-R (XFP) lines
21	NK10G-8RX	Eight 10GBASE-R (XFP) lines
22	NH1G-16S	16 1000BASE-X (SFP) lines
23	NH1G-24T	24 10BASE-T, 100BASE-TX, or 1000BASE-T lines
24	NH1G-24S	24 1000BASE-X (SFP) lines
25	NH1G-48T	48 10BASE-T, 100BASE-TX, or 1000BASE-T lines
26	NH1GS-6M	Four 10BASE-T, 100BASE-TX, or 1000BASE-T lines with the hierarchical shaper and two 1000BASE-X SFP lines with the hierarchical shaper
27	NH10G-1RX	One 10GBASE-R (XFP) line
28	NH10G-4RX	Four 10GBASE-R (XFP) lines
29	NH10G-8RX	Eight 10GBASE-R (XFP) lines

(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
BSU:<*bsu no.*>	BSU part
NIF:<*nif no.*>	NIF part
GigabitEthernet <*nif no.*>/<*port no.*>	An Ethernet interface with a maximum line speed of 1000 Mbit/s
TenGigabitEthernet <*nif no.*>/<*port no.*>	An Ethernet interface with a maximum line speed of 10 Gbit/s
MGMT 0	Management port

Legend:

<*bsu no.*>: BSU number

<*nif no.*>: NIF number

<*port no.*>: Port number

(5) Message identifier and additional information

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

(6) First and last time of 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 times the applicable event occurs if there are multiple occurrences. 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

The following describes the occasions when the operation logs and reference logs are automatically saved to internal flash memory. The table below describes where the logs are saved. Note that if the configuration command `no logging syslog-dump` 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 `E5` to `E9` occurs

3. When the Switch is restarted by using the `reload` 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 switch

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 viewed by using the `show logging` command. These logs can also be acquired 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 where the created files are stored 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>*`/`	Files are stored in internal memory.
Temporary directory	`/tmp/`	When the switch stops due to a loss of power or execution of the `reload` command, stored files are 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 the *logging facility* in the manual *Configuration Command Reference Vol. 2 For Version 11.7*.

(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 the email functionality, a transmission error occurs.

For details about the email functionality, see *logging email-from* in the manual *Configuration Command Reference Vol. 2 For Version 11.7* or *logging email-server* in the manual *Configuration Command Reference Vol. 2 For Version 11.7*.

Chapter

2. Routing Event Information

This chapter explains the contents of routing event information. Routing protocol event information reports the operating status of the 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 the event information for the IPv4 routing protocol.

2.1.1 RIP

The following table describes the event information of the 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\>* [(VRF *\<vrf id\>*)]	Error (remote device)
		Route information that has an invalid metric value (0, or 17 or larger) was received. [Explanation of message variables] *\<metric\>*: Metric value of the route information *\<destination address\>*: Destination address for the route information *\<source address\>*: Source gateway *\<vrf id\>*: VRF ID [Action] Check the unicast routing program (RIP) of the source gateway.
2	rip_recv_response: Bad mask (*\<mask\>*) for net *\<destination address\>* from *\<source address\>* [(VRF *\<vrf id\>*)]	Error (remote device)
		Route information that has an invalid network mask was received. [Explanation of message variables] *\<mask\>*: Route information network mask *\<destination address\>*: Destination address for the route information *\<source address\>*: Source gateway *\<vrf id\>*: VRF ID [Action] Check the unicast routing program (RIP) of the source gateway.
3	rip_recv: Ignoring RIP *\<rip command\>* packet from *\<source address\>* [(VRF *\<vrf id\>*)] - ignoring version 0 packets	Error (remote device)
		A received RIP packet is ignored because the version field is 0. [Explanation of message variables] *\<rip command\>*: Received message type • `Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry` *\<source address\>*: Source gateway *\<vrf id\>*: VRF ID [Action] Check the unicast routing program (RIP) of the source gateway.
4	rip_recv: Ignoring RIP *\<rip command\>* packet from *\<source address\>* [(VRF *\<vrf id\>*)] - reserved field not zero	Error (remote device)
		A received RIP packet is ignored because the reserved field is not 0. [Explanation of message variables] *\<rip command\>*: Received message type • `Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry` *\<source address\>*: Source gateway *\<vrf id\>*: VRF ID [Action] Check the unicast routing program (RIP) of the source gateway.

#	Message text	Description
5	rip_recv: Ignoring RIP *\<rip command\>* packet from *\<source address\>* [(VRF *\<vrf id\>*)] - authentication failure [(Key-ID *\<key id\>*)]	Error (local device or remote device)

		A received RIP packet is ignored because of an authentication error.
		Output of this operation message is as follows:
		1. For the first 16 events, the message is output for each event.
		2. For the 17th and subsequent events, the message is output once every 256 events.
		3. If events occur three or more minutes after the last event has occurred, the message is output as described in 1 and 2 above.
		Note that the counting described above includes the number of times the following messages are output:
		    rip_recv: Ignoring RIP *\<rip command\>* packet from *\<source address\>* [(VRF *\<vrf id\>*)] - illegal authentication type
		    rip_recv: Ignoring RIP *\<rip command\>* packet from *\<source address\>* [(VRF *\<vrf id\>*)] - illegal authentication key identifier (Key-ID *\<key id\>*)
		    rip_recv: Ignoring RIP *\<rip command\>* packet from *\<source address\>* [(VRF *\<vrf id\>*)] - illegal authentication sequence number (Key-ID *\<key id\>*)
		
		[Explanation of message variables]
		\<rip command\>: Received message type
		• `Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry`
		\<source address\>: Source gateway
		\<vrf id\>: VRF ID
		\<key id\>: Key ID
		[Action]
		Check whether the authentication key for the local device RIP matches the authentication key for the remote device RIP.
		If they do not match, specify the authentication keys so that they do match.

6	rip_recv: Ignoring RIP *\<rip command\>* packet from *\<source address\>* [(VRF *\<vrf id\>*)] - TRACE packets not supported	Warning (remote device)
		A received RIP packet is ignored because `TRACE` packets are not supported. [Explanation of message variables] *\<rip command\>*: Received message type • `TraceOn, TraceOff` *\<source address\>*: Source gateway *\<vrf id\>*: VRF ID [Action] Check the specifications of the unicast routing program (RIP) for the source gateway.
7	rip_init: Old copy of rtm is running	Error (local device)
		The unicast routing program might already be running. The unicast routing program will be restarted automatically. [Explanation of message variables] None. [Action] Take action in response to the `rtm aborted` log entry.

#	Message text	Description
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 revise the RIP settings so that the maximum number of neighboring routers does not exceed the capacity limits.
9	rip_recv: Ignoring RIP *<rip command>* packet from *<source address>* [(VRF *<vrf id>*)] - illegal authentication type	Error (remote device)

		A received RIP packet is ignored because the authentication type of authentication information is invalid.
		Output of this operation message is as follows:
		1. For the first 16 events, the message is output for each event.
		2. For the 17th and subsequent events, the message is output once every 256 events.
		3. If events occur three or more minutes after the last event has occurred, the message is output as described in 1 and 2 above.
		Note that the counting described above includes the number of times the following messages are output:
		    rip_recv: Ignoring RIP *<rip command>* packet from *<source address>* [(VRF *<vrf id>*)] - authentication failure [(Key-ID *<key id>*)]
		    rip_recv: Ignoring RIP *<rip command>* packet from *<source address>* [(VRF *<vrf id>*)] - illegal authentication key identifier (Key-ID *<key id>*)
		    rip_recv: Ignoring RIP *<rip command>* packet from *<source address>* [(VRF *<vrf id>*)] - illegal authentication sequence number (Key-ID *<key id>*)
		
		[Explanation of message variables]
		<rip command>: Received message type
		• `Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry`
		<source address>: Source gateway
		<vrf id>: VRF ID
		[Action]
		Check the unicast routing program (RIP) of the source gateway.

#	Message text	Description
10	rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> [(VRF <*vrf id*>)] - illegal authentication key identifier (Key-ID <*key id*>)	Error (local device or remote device)
		A received RIP packet is ignored because the key identifier of authentication information is invalid. Output of this operation message is as follows: 1. For the first 16 events, the message is output for each event. 2. For the 17th and subsequent events, the message is output once every 256 events. 3. If events occur three or more minutes after the last event has occurred, the message is output as described in 1 and 2 above. Note that the counting described above includes the number of times the following messages are output: <blockquote>rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> [(VRF <*vrf id*>)] - authentication failure [(Key-ID <*key id*>)] rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> [(VRF <*vrf id*>)] - illegal authentication type rip_recv: Ignoring RIP <*rip command*> packet from <*source address*> [(VRF <*vrf id*>)] - illegal authentication sequence number (Key-ID <*key id*>)</blockquote> [Explanation of message variables] <*rip command*>: Received message type • `Invalid`, `Request`, `Response`, `TraceOn`, `TraceOff`, `Poll`, `PollEntry` <*source address*>: Source gateway <*vrf id*>: VRF ID <*key id*>: Key ID [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>* [(VRF *<vrf id>*)] - illegal authentication sequence number (Key-ID *<key id>*)	Error (remote device)
		A received RIP packet is ignored because the sequence number of authentication information is invalid. Output of this operation message is as follows: 1. For the first 16 events, the message is output for each event. 2. For the 17th and subsequent events, the message is output once every 256 events. 3. If events occur three or more minutes after the last event has occurred, the message is output as described in 1 and 2 above. Note that the counting described above includes the number of times the following messages are output: rip_recv: Ignoring RIP *<rip command>* packet from *<source address>* [(VRF *<vrf id>*)] - authentication failure [(Key-ID *<key id>*)] rip_recv: Ignoring RIP *<rip command>* packet from *<source address>* [(VRF *<vrf id>*)] - illegal authentication type rip_recv: Ignoring RIP *<rip command>* packet from *<source address>* [(VRF *<vrf id>*)] - illegal authentication key identifier (Key-ID *<key id>*) [Explanation of message variables] *<rip command>*: Received message type • `Invalid, Request, Response, TraceOn, TraceOff, Poll, PollEntry` *<source address>*: Source gateway *<vrf id>*: VRF ID *<key id>*: Key ID [Action] Check the unicast routing program (RIP) of the source gateway.

2.1.2 OSPF

The following table describes the event information of the IPv4 routing protocol information (RTM).

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

#	Message text	Description
1	OSPF SENT *<source address>* -> *<destination address>* [(VRF *<vrf id>*)] : *<error string>*	Warning (local device)
		An attempt to send an OSPF packet failed. [Explanation of message variables] *<source address>*: Source IPv4 address *<destination address>*: Destination IPv4 address *<vrf id>*: VRF ID *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.

#	Message text	Description
2	OSPF: Helper to adjacency *<router id>* address *<address>* [(VRF *<vrf 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>*: Router ID of the neighboring router *<address>*: IPv4 address of the neighboring router *<vrf id>*: VRF ID [Action] Check if the neighboring router has stopped the restart operation. If the operation has not stopped, adjust the restart time of the neighboring router.
3	OSPF: Helper to adjacency *<router id>* address *<address>* [(VRF *<vrf id>*)] failed because network topology is changed.	Warning (local device or network)
		The helper router operations stopped because the topology was changed. [Explanation of message variables] *<router id>*: Router ID of the neighboring router *<address>*: IPv4 address of the neighboring router *<vrf id>*: VRF ID [Action] None.
4	OSPF RECV [Area *<area id>*] *<source address>* -> *<destination address>* [(VRF *<vrf id>*)] : *<log type>*.	Warning (local device or remote device)
		A received OSPF packet is invalid. However, multicast packets received from broadcast-type interfaces that have not been set as OSPF interfaces are discarded without being logged. [Explanation of message variables] *<area id>*: Area ID *<source address>*: Source IPv4 address *<destination address>*: Destination IPv4 address *<vrf id>*: VRF ID *<log type>*: One of the following log types: • IP: bad destination • IP: bad protocol • IP: received my own packet • OSPF: bad packet type • OSPF: bad version • OSPF: bad checksum • OSPF: packet too small • OSPF: packet size > ip length • OSPF: bad area id • OSPF: unknown neighbor • OSPF: area mismatch • OSPF: bad virtual link • OSPF: bad authentication type • OSPF: bad authentication key • OSPF: interface down • HELLO: netmask mismatch • HELLO: hello timer mismatch • HELLO: dead timer mismatch • HELLO: NBMA neighbor unknown

#	Message text	Description

20		• 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.
		
		• IP: bad protocol
		• IP: received my own packet
		• OSPF: bad packet type
		• OSPF: bad version
		• OSPF: bad checksum
		• OSPF: packet too small
		• OSPF: packet size > ip length
		• OSPF: bad area id
		  A neighboring router has sent invalid packets. Check the unicast routing program (OSPF) of the new neighboring router.
		• OSPF: unknown neighbor
		  Non-Hello packets were received from a 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.

#	Message text	Description
		• LS ACK: Unknown LSA type • LS REQ: empty request • LS REQ: bad request • LS UPD: LSA checksum bad A neighboring router has sent invalid packets. Check the unicast routing program (OSPF) of the new 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 will be restarted automatically. [Explanation of message variables] *<address>*: Destination address for the route information *<mask1>*: Route information network mask *<lsid>*: LSA LSID *<mask2>*: LSA network mask *<age>*: Time elapsed from generation of LSA [Action] Take action in response to the `rtm aborted` log entry.
6	OSPF: Lost adjacency *<router id>* address *<address>*(*<interface name>*) due to sequence mismatch (*<sequence1>* versus *<sequence2>*)	Warning (local device or remote device)
		A neighboring router was lost due to a sequence mismatch. [Explanation of message variables] *<router id>*: Router ID of the neighboring router *<address>*: IPv4 address of the neighboring router *<interface name>*: Interface name *<sequence1>*: Sequence number in the 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 this device and neighboring router. [Explanation of message variables] *<router id>*: Router ID of the neighboring router *<address>*: IPv4 address of the neighboring router *<interface name>*: Interface name [Action] If this warning occurs frequently, reduce the interval for sending Hello packets (`hellointerval`) and extend the maximum interval for receiving Hello packets (`routerdeadinterval`).

#	Message text	Description
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 this device. This occurs when the neighboring router is restarted or Hello packets sent by this device are not properly received by the neighboring router. [Explanation of message variables] *\<router id>*: Router ID of the neighboring router *\<address>*: IPv4 address of the neighboring router *\<interface name>*: Interface name [Action] If this warning occurs frequently, reduce the interval for sending Hello packets (`hellointerval`) and 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)
		A neighboring router was lost due to an invalid LS request. [Explanation of message variables] *\<router id1>*: Router ID of the neighboring router *\<address>*: IPv4 address of the neighboring router *\<interface name>*: Interface name *\<lsid>*: LSA LSID *\<router id2>*: LSA advertising router ID *\<ls type>*: LSA LS type code [Action] Check the unicast routing program (OSPF) of the new neighboring router.
10	OSPF: Adjacency *\<router id>* address *\<address>*(*\<interface name>*) is established.	Information (local device or remote device)
		A connection with the OSPF neighboring router was successfully established. [Explanation of message variables] *\<router id>*: Router ID of the neighboring router *\<address>*: IPv4 address of the neighboring router *\<interface name>*: Interface name [Action] None.
11	OSPF: Checksum failed at LSA type *\<ls type>* ID *\<lsid>* adv-router *\<router id>* in this system's LSDB that belongs to Area *\<area id>*, Domain *\<domain id>* [on VRF *\<vrf id>*].	Error (local device)
		LSDB checksum is invalid. The unicast routing program will be restarted automatically. [Explanation of message variables] *\<ls type>*: LSA LS type code *\<lsid>*: LSA LSID *\<router id>*: LSA advertising router ID *\<area id>*: LSA area ID *\<domain id>*: LSA domain ID *\<vrf id>*: VRF ID [Action] Take action in response to the `rtm aborted` log entry.
12	OSPF: Recovered from stub router (in [(VRF *\<vrf id>*)] domain *\<domain id>*).	Information (local device)
		The stub router operation will now end. [Explanation of message variables] *\<vrf id>*: VRF ID *\<domain id>*: OSPF domain ID [Action] None.

#	Message text	Description
13	OSPF: Graceful restart failed (in [(VRF *\<vrf id\>*)] domain *\<domain id\>*) because adjacency *\<router id\>* address *\<address\>* doesn't help me.	Warning (remote device or network)
		Graceful restart has failed because the neighboring router was not operating as the helper router. [Explanation of message variables] *\<vrf id\>*: VRF ID *\<domain id\>*: OSPF domain ID *\<router id\>*: Router ID of the neighboring router *\<address\>*: IPv4 address of the neighboring router [Action] Check the configuration of graceful restart for the neighboring router.
14	OSPF: Graceful restart failed (in [(VRF *\<vrf id\>*)] domain *\<domain id\>*) because adjacency *\<router id\>* address *\<address\>* gives up me	Warning (remote device or network)
		Graceful restart has failed because the neighboring router stopped helper router operations. [Explanation of message variables] *\<vrf id\>*: VRF ID *\<domain id\>*: OSPF domain ID *\<router id\>*: Router ID of the neighboring router *\<address\>*: IPv4 address of the neighboring router [Action] If this warning occurs frequently, check the OSPF status of the neighboring router and the cause of helper functionality termination.
15	OSPF: Graceful restart failed (in [(VRF *\<vrf id\>*)] domain *\<domain id\>*) because restart time is up.	Warning (local device)
		Graceful restart failed because all neighboring routers that were connected before the restart cannot be reconnected and LSA synchronization cannot be completed within the restart time. [Explanation of message variables] *\<vrf id\>*: VRF ID *\<domain id\>*: OSPF domain ID [Action] Check the configuration of the restart time.
16	OSPF: Graceful restart finished successfully (in [(VRF *\<vrf id\>*)] domain *\<domain id\>*).	Information (local device)
		Graceful restart was completed successfully. [Explanation of message variables] *\<vrf id\>*: VRF ID *\<domain id\>*: OSPF domain ID [Action] None.

2.1.3 BGP4 [OP-BGP]

The following table describes the event information of the 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) on the peer.

#	Message text	Description
2	bgp_trace: Unsupported BGP version *<version>*!!!	Error (local device)
		The BGP version number in the control data is invalid. The unicast routing program will be restarted automatically. [Explanation of message variables] *<version>*: BGP version number in the control data [Action] Take action in response to the rtm aborted log entry.
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 is invalid. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length>*: Received message length [Action] Check the unicast routing program (BGP4) on 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 was full. [Explanation of message variables] *<bgp name>*: Destination peer name *<description>*: Destination peer description name *<length>*: Length of the message requested to be sent *<error string>*: Error cause [Action] If this error occurs frequently, check 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 failed. [Explanation of message variables] *<bgp name>*: Destination peer name *<description>*: Destination peer description name *<length>*: Length of the message requested to be sent *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.
6	bgp_send: Sending *<length>* bytes to *<bgp name>* [(*<description>*)]: connection closed	Warning (local device, remote device, or network)
		An attempt to send a message to the relevant peer failed due to a disconnection. [Explanation of message variables] *<bgp name>*: Destination peer name *<description>*: Destination peer description name *<length>*: Length of the message requested to be sent [Action] If this error occurs frequently, check the cause of the disconnection.

2. Routing Event Information

#	Message text	Description
7	bgp_send: Sending to *\<bgp name\>* [(*\<description\>*)] looping: *\<error string\>*	Warning (local device)
		The retry count was exceeded during sending of a message to the relevant peer. [Explanation of message variables] *\<bgp name\>*: Destination peer name *\<description\>*: Destination peer description name *\<error string\>*: Error cause [Action] If this error occurs frequently, check the cause of the error.
8	bgp_send_open: Internal error! peer *\<bgp name\>* [(*\<description\>*)], version *\<version\>*	Error (local device)
		The BGP version number of the OPEN message to be sent to the relevant peer is invalid. The unicast routing program will be restarted automatically. [Explanation of message variables] *\<bgp name\>*: Destination peer name *\<description\>*: Destination peer description name *\<version\>*: BGP version number in the send message [Action] Take action in response to the rtm aborted log entry.
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\>*: Source peer description name *\<length\>*: Error data length *\<error data\>*: First five bytes of error data [Action] Check the unicast routing program (BGP4) on 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\>*: Source peer description name *\<error string\>*: Error cause [Action] If this error occurs frequently, check 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 a disconnection. [Explanation of message variables] *\<bgp name\>*: Source peer name *\<description\>*: Source peer description name [Action] If this error occurs frequently, check the cause of the disconnection.

#	Message text	Description
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>*: Source peer description name *<message type>*: Received message type • invalid, Open, Update, Notification, KeepAlive *<length>*: Received message length [Action] Check the unicast routing program (BGP4) on the peer.
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>*: Source peer description name *<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) on 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>*: Source peer description name *<version>*: BGP version number in the received message *<length>*: Received message length [Action] Check the unicast routing program (BGP4) on the peer.
15	bgp_get_open: Received unsupported version *<version>* message from peer *<bgp name>* [(*<description>*)]	Warning (remote device)
		An OPEN message whose BGP version is unsupported was received from the relevant peer. [Explanation of message variables] *<version>*: BGP version number in the received message *<bgp name>*: Source peer name *<description>*: Source peer description name [Action] Make sure that the peer supports the 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>*: Source peer description name *<holdtime>*: Hold time in the received message [Action] Check the configuration of the peer.

#	Message text	Description
17	bgp_get_open: Peer *<bgp name>* [(*<description>*)]: invalid BGP identifier *<router id>*	Error (remote device)
		An OPEN message that has an invalid BGP identifier was received from the relevant peer. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<router id>*: BGP identifier in the received message [Action] Check the unicast routing program (BGP4) on the peer.
18	bgp_get_open: Peer *<bgp name>* [(*<description>*)]: Unsupported optional parameter *<option>*	Error (remote device)
		An OPEN message that contains an invalid option code was received from the relevant peer. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<option>*: Option code in the received message [Action] Check the unicast routing program (BGP4) on 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>*: Source peer description name *<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>*: Source peer description name *<version1>*: Remote BGP version number *<version2>*: Local BGP version number [Action] Make sure that the peer supports the 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.

#	Message text	Description
22	bgp_pp_recv: Rejecting connection from *<bgp name>* [(*<description>*)], peer in state *<state>*	Warning (remote device or network)
		An OPEN message was received from the relevant peer during the Idle, OpenConfirm, or Established state. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<state>*: Peer state • Idle, OpenConfirm, Established [Action] The connection is unstable. If this error occurs frequently, check the cause of the instability.
23	bgp_pp_recv: Dropping *<bgpp name>* version *<version>*, *<bgp name>* [(*<description>*)] wants version 4	Warning (remote device)
		An OPEN message whose BGP version is unsupported was received from the relevant peer. [Explanation of message variables] *<bgpp name>* and *<bgp name>*: Source peer name *<version>*: BGP version number in the received message *<description>*: Source peer description name [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>*: Source peer description name [Action] Check the unicast routing program (BGP4) on the peer.
25	bgp_check_capability_match: Capability of peer *<bgp name>* [(*<description>*)] is unmatched	Warning (remote device)
		The capability settings specified for this device are not specified for the relevant peer. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name [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 failed. [Explanation of message variables] *<length1>*: Length of the data requested to be sent *<length2>*: Length of the sent data *<bgp name>*: Destination peer name *<description>*: Destination peer description name *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.

#	Message text	Description
27	bgp_write_flush: Sending *<length1>* (sent *<length2>*) bytes to *<bgp name>* [(*<description>*)]: Connection closed	Warning (local device, remote device, or network)
		An attempt to send a message to the relevant peer failed due to a disconnection. [Explanation of message variables] *<length1>*: Length of the data requested to be sent *<length2>*: Length of the sent data *<bgp name>*: Destination peer name *<description>*: Destination peer description name [Action] If this error occurs frequently, check the cause of the disconnection.
28	bgp_write_flush: Sending to *<bgp name>* [(*<description>*)] (sent *<length1>*, *<length2>* remain[s]) looping: *<error string>*	Warning (local device)
		The retry count was exceeded during sending of a message to the relevant peer. [Explanation of message variables] *<bgp name>*: Destination peer name *<description>*: Destination peer description name *<length1>*: Length of the sent data *<length2>*: Length of the data that remains unsent *<error string>*: Error cause [Action] If this error occurs frequently, check 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 destination peer name *<description>*: Connection destination peer description name *<error string>*: Error cause [Action] If this error occurs frequently, check 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 destination peer name *<description>*: Connection destination peer description name *<ipv4 address>*: Local address used for peering [Action] If this error occurs frequently, check 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 destination peer name *<description>*: Connection destination peer description name [Action] Check the unicast routing program (BGP4) on the peer.

#	Message text	Description
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>*: Destination peer name *<description>*: Destination peer description name *<error string>*: Error cause [Action] If this error occurs frequently, check 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 occurs frequently, check the cause of the error.
34	bgp_listen_accept: task_get_addr_local() failed, terminating!!	Error (local device)
		Extraction of the local address used for establishing a connection failed. The process that establishes a connection will terminate. [Explanation of message variables] None. [Action] If the error occurs frequently, check the unicast routing program (BGP4) on 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 will be restarted automatically. [Explanation of message variables] None. [Action] Take action in response to the `rtm aborted` log entry.
36	bgp_listen_start: listen: *<error string>*	Error (local device)
		Preparation for accepting a connection failed. The unicast routing program will be restarted automatically. [Explanation of message variables] *<error string>*: Error cause [Action] Take action in response to the `rtm aborted` log entry.
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 destination peer name *<description>*: Connection destination peer description name [Action] Check the configuration.

#	Message text	Description
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 on the same network. [Explanation of message variables] <*bgp name*>: Connection destination peer name <*description*>: Connection destination peer description name <*ipv4 address*>: Local address used for establishing a connection [Action] Check the configuration.
39	bgp_pp_timeout: Peer <*bgpp name*> timed out waiting for OPEN	Warning (remote device or network)
		The timer for waiting for an OPEN message from the relevant peer timed out. [Explanation of message variables] <*bgpp name*>: Connection destination peer name [Action] Check the unicast routing program (BGP4) on the peer.
40	bgp_peer_init: BGP peer <*bgp name*> [(<*description*>)] local address <*ipv4 address*> not found. Leaving peer idled	Warning (local device)
		The interface for the local address used for establishing a connection to the relevant peer is not found. [Explanation of message variables] <*bgp name*>: Connection destination peer name <*description*>: Connection destination peer description name <*ipv4 address*>: Local address used for establishing a connection [Action] Check the configuration.
41	bgp_recv_v4_update: Peer <*bgp name*> [(<*description*>)]: Strange message header length <*length*>	Error (remote device)
		The message length in the message header of a message received from the relevant peer is invalid. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Source peer description name <*length*>: Message length of the received message header [Action] Check the unicast routing program (BGP4) on 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*>: Source peer description name <*type*>: Message type [Action] Check the unicast routing program (BGP4) on the peer.

#	Message text	Description
43	bgp_recv_v4_update: Received OPEN message from *<bgp name>* [(*<description>*)], state is ESTABLISHED	Warning (remote device or network)
		An OPEN message was received from the relevant peer in the ESTABLISHED state. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name [Action] The connection is 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>*: Source peer description name *<length>*: Received message length [Action] Check the unicast routing program (BGP4) on the peer.
45	bgp_recv_v4_update: Peer *<bgp name>* [(*<description>*)] UPDATE unreachable prefix length *<length1>* exceeds packet length *<length2>*	Error (remote device)
		The prefix length of unreachable route information of the UPDATE message from the relevant peer exceeds the packet length. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length1>*: Prefix length of unreachable route information in the received message *<length2>*: Received packet length [Action] Check the unicast routing program (BGP4) on 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>*: Source peer description name *<length>*: Actual data length [Action] Check the unicast routing program (BGP4) on 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 when compared with the actual path attribute length. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length1>*: Path attribute length of the received message *<length2>*: Actual data length [Action] Check the unicast routing program (BGP4) on the peer.

#	Message text	Description
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>*: Source peer description name [Action] Check the unicast routing program (BGP4) on 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>*: Source peer description name [Action] Check the unicast routing program (BGP4) on the peer.
50	bgp_recv_v4_update: Peer *<bgp name>* [(*<description>*)] UPDATE no LOCALPREF attribute found	Error (remote device)
		The LOCALPREF attribute is not found in the UPDATE message from the relevant internal peer. [Explanation of message variables] *<bgp name>*: Source peer number *<description>*: Source peer description name [Action] Check the unicast routing program (BGP4) on 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>*: Source peer description name [Action] Check the unicast routing program (BGP4) on the peer.
52	bgp_recv_v4_unreach: Peer *<bgp name>* [(*<description>*)] UPDATE: Invalid unreachable prefix length *<length>*	Error (remote device)
		The prefix length of the unreachable route information in the UPDATE message received from the relevant peer is invalid. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length>*: Prefix length in the received message [Action] Check the unicast routing program (BGP4) on the peer.

#	Message text	Description
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 the unreachable route information in the UPDATE message received from the relevant peer exceeds the prefix data of the unreachable route information. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length1>*: Prefix length in the received message *<length2>*: Actual data length [Action] Check the unicast routing program (BGP4) on 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)
		The routes of unreachable route information that has multiple labels in the UPDATE message received from the relevant peer will be ignored. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length1>* of *<length2>*: Location of the invalid information in the message [Action] Check the unicast routing program (BGP4) on the peer.
55	bgp_recv_v4_unreach: Peer *<bgp name>* [(*<description>*)] UPDATE: Ignoring unreachable route with RD 0 prefix (*<length1>* of *<length2>*)	Error (remote device)
		The routes of unreachable route information that has RD 0 of the UPDATE message received from the relevant peer will be ignored. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length1>* of *<length2>*: Location of the invalid information in the message [Action] Check the unicast routing program (BGP4) on the peer.
56	bgp_recv_v4_unreach: Peer *<bgp name>* [(*<description>*)] UPDATE: Ignoring invalid unreachable route *<ipv4 address>*/*<mask>* (*<length1>* of *<length2>*)	Error (remote device)
		Invalid routes of unreachable route information of the UPDATE message received from the relevant peer will be ignored. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<ipv4 address>*: Destination address of the unreachable route information *<mask>*: Network mask of the unreachable route information *<length1>* of *<length2>*: Location of the invalid information in the message [Action] Check the unicast routing program (BGP4) on the peer.

2. Routing Event Information

#	Message text	Description
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*>: Source peer description name <*as1*>: AS number of the source peer <*as2*>: Next-hop AS number in the received message [Action] Check the unicast routing program (BGP4) on 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*>: Source peer description name <*length*>: Prefix length in the received message [Action] Check the unicast routing program (BGP4) on 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*>: Source peer description name <*length1*>: Prefix length in the received message <*length2*>: Actual prefix length [Action] Check the unicast routing program (BGP4) on the peer.
60	bgp_recv_v4_reach: Peer <*bgp name*> [(<*description*>)] UPDATE: Ignoring route with two or more labels (<*length1*> of <*length2*>)	Warning (remote device)
		Routes that have multiple labels of the UPDATE message received from the relevant peer are ignored. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Source peer description name <*length1*> of <*length2*>: Location of the invalid information in the received message [Action] Check the unicast routing program (BGP4) on 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*>: Source peer description name <*length1*> of <*length2*>: Location of the invalid information in the received message [Action] Check the unicast routing program (BGP4) on the peer.

#	Message text	Description
62	bgp_recv_v4_reach: Peer <*bgp name*> [(<*description*>)] UPDATE:Included invalid route <*ipv4 address*>/<*mask*> (<*length1*> of <*length2*>)	Error (remote device)
		The UPDATE message received from the relevant peer includes invalid routes. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Source peer description name <*ipv4 address*>: Destination address <*mask*>: Network mask <*length1*> of <*length2*>: Location of the invalid information in the received message [Action] Check the unicast routing program (BGP4) on 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*>: Source peer description name <*length1*> of <*length2*>: Location of the invalid information in the received message [Action] Check the unicast routing program (BGP4) on 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*>: Source peer description name <*length1*> of <*length2*>: Location of the invalid information in the received message [Action] Check the unicast routing program (BGP4) on the peer.
65	bgp_recv_mp_unreach: Peer <*bgp name*> [(<*description*>)] UPDATE: Invalid length of MP_UNREACH_NLRI attribute(<*length*>) : No address family	Error (remote device)
		The length of the MP_UNREACH_NLRI attribute for the UPDATE message received from the relevant peer is invalid. No address family exists. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Source peer description name <*length*>: Received MP_UNREACH_NLRI attribute length [Action] Check the unicast routing program (BGP4) on 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 relevant peer is invalid. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Source peer description name <*address family*>: Address family information of the received MP_UNREACH_NLRI attribute [Action] Check the unicast routing program (BGP4) on the peer.

#	Message text	Description
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 relevant peer is invalid. No address family exists. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length>*: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4) on 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>*: Source peer description name *<address family>*: Address family information of the received MP_REACH_NLRI attribute [Action] Check the unicast routing program (BGP4) on 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 relevant peer is invalid. No next-hop length exists. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length>*: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4) on the peer.
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 relevant peer is invalid. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length>*: Next-hop length of the received MP_REACH_NLRI attribute [Action] Check the unicast routing program (BGP4) on 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 relevant peer is invalid. No next hop exists. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length>*: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4) on the peer.

#	Message text	Description
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 relevant peer is invalid. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Source peer description name <*rd1*>:<*rd2*>: Next-hop RD of the received MP_REACH_NLRI attribute [Action] Check the unicast routing program (BGP4) on 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 relevant peer is invalid. No reserved field exists. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Source peer description name <*length*>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4) on 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 relevant peer is invalid. No SNPA length exists. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Source peer description name <*length*>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4) on the peer.
75	bgp_recv_mp_reach: Peer <*bgp name*> [(<*description*>)] UPDATE: Invalid length of MP_REACH_NLRI attribute(<*length*>) : No snpa	Error (remote device)
		The length of the MP_REACH_NLRI attribute for the UPDATE message received from the relevant peer is invalid. No SNPA exists. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Source peer description name <*length*>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4) on the peer.
76	bgp_peer_established: Peer <*bgp name*> [(<*description*>)] connection established	Information (local device or remote device)
		A BGP4 connection was established with the relevant peer. [Explanation of message variables] <*bgp name*>: Connection destination peer name <*description*>: Connection destination peer description name [Action] None.
77	bgp_ifachange: Peer <*bgp name*> [(<*description*>)]: Closed connection by changing interface state	Information (local device or remote device)
		A BGP4 connection was closed due to a change in the interface state. [Explanation of message variables] <*bgp name*>: Connection destination peer name <*description*>: Connection destination peer description name [Action] Check the cause of the change in the interface state.

#	Message text	Description
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 destination peer name <*description*>: Connection destination peer description name [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 destination peer name <*description*>: Connection destination peer description name [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 destination peer name <*description*>: Connection destination peer description name [Action] None.
81	bgp_peer_clear: Peer <*bgp name*> [(<*description*>)]: Closed connection by clearing peer	Information (local device)
		A BGP4 connection was closed by entering the `clear ip bgp` command. [Explanation of message variables] <*bgp name*>: Connection destination peer name <*description*>: Connection destination peer description name [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)
		The peer that performed graceful restart could not save the forwarding routes. All the routes that had been learned have been deleted from the relevant peer. [Explanation of message variables] <*bgp name*>: Connection destination peer name [Action] Check the unicast routing program (BGP4) on 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)
		The peer that performed graceful restart could not save the forwarding routes. All the routes that had been learned have been deleted from the relevant peer. [Explanation of message variables] <*bgp name*>: Connection destination peer name [Action] Check the unicast routing program (BGP4) on the peer.

#	Message text	Description
84	bgp_restart_timeout: Peer *<bgp name>* [(*<description>*)]: Timed out waiting for reconnect.	Error (local device or remote device)
		Graceful restart failed. A connection with the peer router could not be established within the restart time specified by the peer router. [Explanation of message variables] *<bgp name>*: Connection destination peer name *<description>*: Connection destination peer description name [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)
		Graceful restart failed. End-Of-RIB could not be received from the peer router. [Explanation of message variables] *<bgp name>*: Connection destination peer name *<description>*: Connection destination peer description name [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 device or remote device)
		A BGP connection with the relevant peer was re-established. [Explanation of message variables] *<bgp name>*: Connection destination peer name *<description>*: Connection destination peer description name [Action] None.
87	bgp_receive_End-Of-RIB: End-Of-RIB marker received from *<bgp name>* [(*<description>*)].	Information (local device)
		End-Of-RIB was received. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name [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>*: Destination peer name *<description>*: Destination peer description name [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>*: Destination peer name *<description>*: Destination peer description name *<code>* (*<code string>*) and *<subcode>* (*<subcode string>*): Error code and error subcode

#	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/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, *<code string>* displays `invalid`. If the *<subcode>* value is invalid, *<subcode string>* displays `unknown`.
		   - *<value>* or *<data>* indicates information about the data field of the `NOTIFICATION` message.
		   <value>: Decimal notation
		   <data>: Hexadecimal notation
		
		[Action]
		Check the network configuration and the peer configuration. If there is no problem with the configurations, check the unicast routing program (BGP4) on the peer.

90	BGP:	Warning (local device)
	NOTIFICATION received from *<bgp name>* [(*<description>*)]: code *<code>* (*<code string>*) [subcode *<subcode>* (*<subcode string>*)] [value *<value>*] [data *<data>*]	A `NOTIFICATION` message was received from the relevant peer. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<code>* (*<code string>*) and *<subcode>* (*<subcode string>*): Error code and error subcode

#	Message text	Description

42		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/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, *<code string>* displays `invalid`. If the *<subcode>* value is invalid, *<subcode string>* displays `unknown`.
		   - *<value>* or *<data>* indicates information about the data field of the `NOTIFICATION` message.
		   <value>: Decimal notation
		   <data>: Hexadecimal notation
		
		[Action]
		Check the network configuration and other configurations.

91	BGP:	Warning (remote device)

#	Message text	Description
	No MD5 digest from *<source ipv4>*+*<port no.>* to *<destination ipv4>*+*<port no.>* [VRF *<vrf id>*]	The MD5 authentication option is not set for the TCP segment received by BGP4 connection. Output of this operation message is as follows: 1. For the first 16 events, the message is output for each event. 2. For the 17th and subsequent events, the message is output once every 256 events. 3. If events occur three or more minutes after the last event has occurred, the message is output as described in 1 and 2 above. Note that the counting described above includes the number of times the BGP: Invalid MD5 digest from *<source ipv4>* + *<port no.>* to *<destination ipv4>* + *<port no.>* message is output. [Explanation of message variables] *<source ipv4>*: Source IPv4 address *<port no.>*: TCP port number *<destination ipv4>*: Destination IPv4 address *<vrf id>*: VRF ID [Action] Check whether the MD5 authentication is set in BGP4 of the remote system. If it is not set, set the MD5 authentication so that it matches. If the setting matches, check whether TCP segments are sent from a peer other than the source BGP4 peer.
92	BGP:	Warning (local device or remote device)
	Invalid MD5 digest from *<source ipv4>*+*<port no.>* to *<destination ipv4>*+*<port no.>* [VRF *<vrf id>*]	The MD5 authentication option for TCP segments received by BGP4 connection is invalid. Output of this operation message is as follows: 1. For the first 16 events, the message is output for each event. 2. For the 17th and subsequent events, the message is output once every 256 events. 3. If events occur three or more minutes after the last event has occurred, the message is output as described in 1 and 2 above. Note that the counting described above includes the number of times the BGP: No MD5 digest from *<source ipv4>* + *<port no.>* to *<destination ipv4>* + *<port no.>* message is output. [Explanation of message variables] *<source ipv4>*: Source IPv4 address *<destination ipv4>*: Destination IPv4 address *<port no.>*: TCP port number *<vrf id>*: VRF ID [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)

#	Message text	Description
	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>*: Source peer description name *<routes1>*: Number of paths learned from the peer *<routes2>*: Maximum number of paths that can be learned from the peer [Action] If the number of paths learned from the relevant peer further increases, check the number of the paths advertised by the peer.
94	BGP:	Warning (remote device)
	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>*: Source peer description name *<routes1>*: Number of paths learned from the peer *<routes2>*: Maximum number of paths that can be learned from the peer [Action] Check the number of the paths advertised by the relevant peer.
95	BGP:	Information (remote device)
	Peer *<bgp name>* [(*<description>*)]: Closed connection by maximum-prefix	BGP4 connection was closed due to the limitation of the number of learned paths. [Explanation of message variables] *<bgp name>*: Connection destination peer name *<description>*: Connection destination peer description name [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_pp_recv:	Warning (remote device)
	Peer *<bgp name>* as receiving-speaker failed to retain stale routes, the packets forwarded to the peer may be discarded.	The peer running as the receiving router could not save the forwarding routes. The packets forwarded to the relevant peer might have been discarded. [Explanation of message variables] *<bgp name>*: Connection destination peer name [Action] During negotiation of the graceful restart functionality, it was reported that forwarding was disabled. Make sure that the peer router has not failed.
97	bgp_recv_open:	Warning (remote device)
	Peer *<bgp name>* as receiving-speaker failed to retain stale routes, the packets forwarded to the peer may be discarded.	The peer running as the receiving router could not save the forwarding routes. The packets forwarded to the relevant peer might have been discarded. [Explanation of message variables] *<bgp name>*: Connection destination peer name [Action] During negotiation of the graceful restart functionality, it was reported that forwarding was disabled. Make sure that the peer router has not failed.
98	BGP:	Information (local device)

#	Message text	Description
	Completed the learning from receiving-speakers	Learning of route information from the receiving router has been completed. [Explanation of message variables] None. [Action] None.
99	BGP:	Information (local device)
	Start advertisement, giving up learning from several receiving-speakers	Route advertisement will start, interrupting the learning of route information from some receiving routers. [Explanation of message variables] None. [Action] None.
100	BGP:	Warning (remote device)
	Peer *<bgp name>* [(*<description>*)] UPDATE included attribute type code (0) [- AS Path (*<as number>*): *<aspath>*]	An UPDATE message including a path attribute with 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>*: Source peer description name *<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) on the peer.

2.1.4 Event information common to the IPv4 unicast routing protocol

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

Table 2-4: Event information common to the IPv4 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. Check the capacity limits.

#	Message text	Description
2	Rtm: Graceful Restart terminated because this system failed to retain the routes.	Warning (local device)
		Graceful Restart failed because the routes could not be retained. [Explanation of message variables] None. [Action] Make sure that a system switchover was not performed again or that the unicast routing program was not restarted during graceful restart.
3	The number of IPv4 unicast routes on global network exceeded the limit.	Warning (local device)
		The number of IPv4 unicast routes on the global network exceeded the maximum number of routes. [Explanation of message variables] None. [Action] 1. Delete unnecessary routes. 2. Check the maximum number of routes specified in the configuration.
4	The number of IPv4 unicast routes on VRF *<vrf id>* exceeded the limit.	Warning (local device)
		The number of IPv4 unicast routes on the VRF *<vrf id>* exceeded the maximum number of routes. [Explanation of message variables] *<vrf id>*: VRF ID [Action] 1. Delete unnecessary routes. 2. Check the maximum number of routes specified in the configuration.
5	The number of IPv4 unicast routes on global network exceeded the warning threshold.	Information (local device)
		The number of IPv4 unicast routes on the global network exceeded the warning threshold. [Explanation of message variables] None. [Action] When adding routes, make sure that the maximum number of routes is not exceeded.
6	The number of IPv4 unicast routes on VRF *<vrf id>* exceeded the warning threshold.	Information (local device)
		The number of IPv4 unicast routes on the VRF *<vrf id>* exceeded the warning threshold. [Explanation of message variables] *<vrf id>*: VRF ID [Action] When adding routes, make sure that the maximum number of routes is not exceeded.

2.2 IPv6 routing protocol information (RTM)

This section explains the event information for the IPv6 routing protocol.

2.2.1 RIPng

The following table describes the event information of the IPv6 routing 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)
		Route information that has an invalid metric value (0, or 17 or larger) was received. [Explanation of message variables] *<metric>*: Metric value of the route information *<prefix>*: Route information destination prefix *<source address>*: Source gateway address [Action] Check the unicast routing program (RIPng) of the source gateway.
2	ripng_recv: Bad prefixlen (*<prefixlen>*) for net *<prefix>* from *<source address>*	Error (remote device)
		Route information that has an invalid prefix length was received. [Explanation of message variables] *<prefixlen>*: Prefix length of the route information *<prefix>*: Route information destination *<source address>*: Source gateway address [Action] Check the unicast routing program (RIPng) of 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) of the source gateway.
4	ripng_recv: Packet hoplimit is *<hoplimit>* hop limit must be 255.	Error (remote device)
		A received RIPng packet was ignored because the hop limit was invalid. [Explanation of message variables] *<hoplimit>*: Received hop-limit [Action] Check the unicast routing program (RIPng) of the source gateway.
5	ripng_init: Old copy of rtm is running	Error (local device)
		The unicast routing program might already be running. The unicast routing program will be restarted automatically. [Explanation of message variables] None. [Action] Take action in response to the `rtm aborted` log entry.

#	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) of 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) of 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) of 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) of 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 route information of invalid length was included. [Explanation of message variables] *\<source address\>*: Source gateway [Action] Check the unicast routing program (RIPng) of the source gateway.
11	ripng_recv: Ignoring a routing entry of improper length - packet from *\<source address\>*	Error (remote device)
		Route information with an invalid length was ignored. [Explanation of message variables] *\<source address\>*: Source gateway [Action] Check the unicast routing program (RIPng) of 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 revise the RIPng settings so that the maximum number of neighboring routers does not exceed the capacity limits.

2.2.2 OSPFv3

The following table describes the event information of the IPv6 routing 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 occurs frequently, check the cause of the error.
2	OSPFv3: Helper to adjacency *<router id>* [(VRF *<vrf 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>*: Router ID of the neighboring router *<vrf id>*: VRF ID [Action] None.
3	OSPFv3: Helper to adjacency *<router id>* [(VRF *<vrf id>*)] failed because restart time is up.	Information (remote device)
		The helper router operations stopped because the waiting time for restart elapsed. [Explanation of message variables] *<router id>*: Router ID of the neighboring router *<vrf id>*: VRF ID [Action] Check if the neighboring router has stopped the restart operation. If the operation 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 is invalid. However, multicast packets received from broadcast-type interfaces that have not been set as OSPFv3 interfaces are discarded without being logged. [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

50		• 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
		  A neighboring router has sent invalid packets. Check the unicast routing program (OSPFv3) for the new neighboring router.
		• unknown neighbor
		  Non-Hello packets were received from a 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 route information might have failed because the MTU length did not match the neighboring router. Match the MTU length. • LS ACK: Unknown LSA type • LS REQ: empty request • LS REQ: bad request • LS UPD: LSA checksum bad • LS UPD: Unknown LSA type A neighboring router has sent invalid packets. Check the unicast routing program (OSPFv3) for the new 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 will be restarted automatically. [Explanation of message variables] *<lsid>*: LSA LSID *<prefix>*: Destination address for the route information *<prefixlen>*: Prefix length of the route information [Action] Take action in response to the `rtm aborted` log entry.
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 this device and neighboring router. [Explanation of message variables] *<router id>*: Router ID of the neighboring router *<id>*: Interface ID of the neighboring router *<interface name>*: Interface name [Action] If this warning occurs frequently, reduce the interval for sending Hello packets (`hellointerval`) and 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 this device. This occurs when the neighboring router is restarted or Hello packets sent by this device are not properly received by the neighboring router. [Explanation of message variables] *<router id>*: Router ID of the neighboring router *<id>*: Interface ID 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)
		A neighboring router was lost due to an invalid LS request. [Explanation of message variables] *<router id1>*: Router ID of the neighboring router *<id>*: Interface ID of the neighboring router *<interface name>*: Interface name *<lsid>*: LSA LSID *<router id2>*: LSA advertising router ID *<ls type>*: LSA LS type code [Action] Check the unicast routing program (OSPFv3) for the new neighboring router.
9	OSPFv3: Lost adjacency *<router id>* with interfaceID *<id>* (*<interface name>*) due to sequence mismatch (*<sequence1>* versus *<sequence2>*)	Warning (local device or remote device)
		A neighboring router was lost due to a sequence (or option) mismatch. [Explanation of message variables] *<router id>*: Router ID of the neighboring router *<id>*: Interface ID of the neighboring router *<interface name>*: Interface name *<sequence1>*: Sequence number in the 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 device or remote device)
		A connection with the OSPFv3 neighboring router was successfully established. [Explanation of message variables] *<router id>*: Router ID of the neighboring router *<interface name>*: Interface name [Action] None.
11	OSPFv3: Checksum failed at LSA type *<ls type>* ID *<lsid>* adv-router *<router id>* in this system's LSDB that belongs to Area *<area id>*, Domain *<domain id>* [on VRF *<vrf id>*].	Error (local device)
		LSDB checksum is invalid. The unicast routing program will be restarted automatically. [Explanation of message variables] *<ls type>*: LSA LS type code *<lsid>*: LSA LSID *<router id>*: LSA advertising router ID *<area id>*: LSA area ID *<domain id>*: LSA Domain ID *<vrf id>*: VRF ID [Action] Take action in response to the `rtm aborted` log entry.
12	OSPFv3: Recovered from stub router (in [(VRF *<vrf id>*)] domain *<domain id>*).	Information (local device)
		The stub router operation will now end. [Explanation of message variables] *<vrf id>*: VRF ID *<domain id>*: OSPFv3 Domain ID [Action] None.

#	Message text	Description
13	OSPFv3: Graceful restart failed (in [(VRF *<vrf id>*)] domain *<domain id>*) because adjacency *<router id>* doesn't help me.	Warning (remote device or network)
		Graceful restart has failed because the neighboring router was not operating as the helper router. [Explanation of message variables] *<vrf id>*: VRF ID *<domain id>*: OSPFv3 domain ID *<router id>*: Router ID of the neighboring router [Action] Check the configuration of graceful restart for the neighboring router.
14	OSPFv3: Graceful restart failed (in [(VRF *<vrf id>*)] domain *<domain id>*) because adjacency *<router id>* gives up me.	Warning (remote device or network)
		Graceful restart has failed because the neighboring router stopped helper router operations. [Explanation of message variables] *<vrf id>*: VRF ID *<domain id>*: OSPFv3 domain ID *<router id>*: Router ID of the neighboring router [Action] If this warning occurs frequently, check the OSPF status of the neighboring router and the cause of helper functionality termination.
15	OSPFv3: Graceful restart failed (in [(VRF *<vrf id>*)] domain *<domain id>*) because restart time is up.	Warning (local device)
		Graceful restart failed because all neighboring routers that were connected before the restart cannot be reconnected and LSA synchronization cannot be completed within the restart time. [Explanation of message variables] *<vrf id>*: VRF ID *<domain id>*: OSPFv3 domain ID [Action] Check the configuration of the restart time.
16	OSPFv3: Graceful restart finished successfully (in [(VRF *<vrf id>*)] domain *<domain id>*).	Information (local device)
		Graceful restart was completed successfully. [Explanation of message variables] *<vrf id>*: VRF ID *<domain id>*: OSPFv3 domain ID [Action] None.

2.2.3 BGP4+ [OP-BGP]

The following table describes the event information of the IPv6 routing 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 is invalid. [Explanation of message variables] *<task name>*: BGP4+ task name [Action] Check the unicast routing program (BGP4+) on the peer.

#	Message text	Description
2	bgp4+_trace: Unsupported BGP version *<version>*!!!	Error (local device)
		The BGP version number in the control data is invalid. The unicast routing program will be restarted automatically. [Explanation of message variables] *<version>*: BGP version number in the control data [Action] Take action in response to the `rtm aborted` log entry.
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 is invalid. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length>*: Received message length [Action] Check the unicast routing program (BGP4+) on 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 was full. [Explanation of message variables] *<length>*: Length of the message requested to be sent *<bgp name>*: Destination peer name *<description>*: Destination peer description name *<error string>*: Error cause [Action] If this error occurs frequently, check 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 failed. [Explanation of message variables] *<length>*: Length of the message requested to be sent *<bgp name>*: Destination peer name *<description>*: Destination peer description name *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.
6	bgp4+_send: Sending *<length>* bytes to *<bgp name>* [(*<description>*)]: connection closed	Warning (local device, remote device, or network)
		An attempt to send a message to the relevant peer failed due to a disconnection. [Explanation of message variables] *<length>*: Length of the message requested to be sent *<bgp name>*: Destination peer name *<description>*: Destination peer description name [Action] If this error occurs frequently, check the cause of the disconnection.

#	Message text	Description
7	bgp4+_send: sending to *<bgp name>* [(*<description>*)] looping: *<error string>*	Warning (local device)
		The retry count was exceeded during sending of a message to the relevant peer. [Explanation of message variables] *<bgp name>*: Destination peer name *<description>*: Destination peer description name *<error string>*: Error cause [Action] If this error occurs frequently, check 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 is invalid. The unicast routing program will be restarted automatically. [Explanation of message variables] *<bgp name>*: Destination peer name *<description>*: Destination peer description name *<version>*: BGP version number in the send message [Action] Take action in response to the rtm aborted log entry.
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>*: Source peer description name *<length>*: Error data length *<error data>*: First five bytes of error data [Action] Check the unicast routing program (BGP4+) on 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>*: Source peer description name *<error string>*: Error cause [Action] If this error occurs frequently, check the cause of the error.
11	bgp4+_recv: Peer *<bgp name>* [(*<description>*)]: Received unexpected EOF	Warning (local device, remote device, or network)
		An attempt to receive a message from the relevant peer failed due to a disconnection. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name [Action] If this error occurs frequently, check the cause of the disconnection.

#	Message text	Description
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>*: Source peer description name *<message type>*: Received message type • invalid, Open, Update, Notification, KeepAlive *<length>*: Received message length [Action] Check the unicast routing program (BGP4+) on the peer.
13	bgp4+_read_message: Peer *<bgp name>* [(*<description>*)]: *<message type1>* arrived, expected *<message type2>* [or *<message type 2>*]	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>*: Source peer description name *<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+) on 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>*: Source peer description name *<version>*: BGP version number in the received message *<length>*: Received message length [Action] Check the unicast routing program (BGP4+) on the peer.
15	bgp4+_get_open: Received unsupported version *<version>* message from peer *<bgp name>* [(*<description>*)]	Warning (remote device)
		An OPEN message whose BGP version is unsupported was received from the relevant peer. [Explanation of message variables] *<version>*: BGP version number in the received message *<bgp name>*: Source peer name *<description>*: Source peer description name [Action] Make sure that the peer supports the BGP version 4.
16	bgp4+_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>*: Source peer description name *<holdtime>*: Hold time in the received message [Action] Check the configuration of the peer.

#	Message text	Description
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>*: Source peer description name *<router id>*: BGP4+ identifier in the received message [Action] Check the unicast routing program (BGP4+) on 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>*: Source peer description name *<option>*: Option code in the received message [Action] Check the unicast routing program (BGP4+) on 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>*: Source peer description name *<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>*: Source peer description name *<version1>*: Remote BGP version number *<version2>*: Local BGP version number [Action] Make sure that the peer supports BGP4+.
21	bgp4+_pp_recv: No group for *<bgpp name>* found, dropping peer	Warning (local device or remote device)
		An OPEN message was received from a peer that was not set. [Explanation of message variables] *<bgpp name>*: Source peer name [Action] Check the configuration.

#	Message text	Description
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>*: Source peer description name *<state>*: Peer state • `Idle`, `OpenConfirm`, `Established` [Action] The connection is 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 whose BGP version is unsupported was received from the relevant peer. [Explanation of message variables] *<bgpp name>* and *<bgp name>*: Source peer name *<version>*: BGP version number in the received message *<description>*: Source peer description name [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>*: Source peer description name [Action] Check the unicast routing program (BGP4+) on the peer.
25	bgp4+_check_capability_match: Capability of peer *<bgp name>* [(*<description>*)] is unmatched	Warning (remote device)
		The capability settings specified for this device are not specified for the relevant peer. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name [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 failed. [Explanation of message variables] *<length1>*: Length of the data requested to be sent *<length2>*: Length of the sent data *<bgp name>*: Destination peer name *<description>*: Destination peer description name *<error string>*: Error cause [Action] If this error occurs frequently, check 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)
		An attempt to send a message to the relevant peer failed due to a disconnection. [Explanation of message variables] *\<length1\>*: Length of the data requested to be sent *\<length2\>*: Length of the sent data *\<bgp name\>*: Destination peer name *\<description\>*: Destination peer description name [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)
		The retry count was exceeded during sending of a message to the relevant peer. [Explanation of message variables] *\<bgp name\>*: Destination peer name *\<description\>*: Destination peer description name *\<length1\>*: Length of the sent data *\<length2\>*: Length of the data that remains unsent *\<error string\>*: Error cause [Action] If this error occurs frequently, check 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 destination peer name *\<description\>*: Connection destination peer description name *\<error string\>*: Error cause [Action] If this error occurs frequently, check 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 destination peer name *\<description\>*: Connection destination peer description name *\<ipv6 address\>*: Local address used for peering [Action] If this error occurs frequently, check 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 destination peer name *\<description\>*: Connection destination peer description name [Action] Check the unicast routing program (BGP4+) on 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*>: Destination peer name <*description*>: Destination peer description name <*error string*>: Error cause [Action] If this error occurs frequently, check 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 occurs frequently, check 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 process that establishes a connection will terminate. [Explanation of message variables] None. [Action] If the error occurs frequently, check the unicast routing program (BGP4+) on 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 process that establishes a connection will terminate. [Explanation of message variables] None. [Action] If the error occurs frequently, check the unicast routing program (BGP4+) on 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 will be restarted automatically. [Explanation of message variables] None. [Action] Take action in response to the rtm aborted log entry.
37	bgp4+_listen_start: listen: <*error string*>	Error (local device)
		Preparation for accepting a connection failed. The unicast routing program will be restarted automatically. [Explanation of message variables] <*error string*>: Error cause [Action] Take action in response to the rtm aborted log entry.

#	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 destination peer name *<description>*: Connection destination peer description name [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 on the same network. [Explanation of message variables] *<bgp name>*: Connection destination peer name *<description>*: Connection destination peer description name *<ipv6 address>*: Local address used for establishing a connection [Action] Check the configuration.
40	bgp4+_pp_timeout: Peer *<bgpp name>* timed out waiting for OPEN	Warning (remote device or network)
		The timer for waiting for an OPEN message from the relevant peer timed out. [Explanation of message variables] *<bgpp name>*: Connection destination peer name [Action] Check the unicast routing program (BGP4+) on 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 destination peer name *<description>*: Connection destination peer description name *<ipv6 address>*: Local address used for establishing a connection [Action] Check the configuration.
42	bgp4+_recv_update: Peer *<bgp name>* [(*<description>*)]: Strange message header length *<length>*	Error (remote device)
		The message length in the message header of a message received from the relevant peer is invalid. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length>*: Message length of the received message header [Action] Check the unicast routing program (BGP4+) on the peer.
43	bgp4+_recv_update: Peer *<bgp name>* [(*<description>*)] unrecognized message type *<type>*	Error (remote device)
		The message type of the UPDATE message from the relevant peer is invalid. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<type>*: Message type [Action] Check the unicast routing program (BGP4+) on 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 received from the relevant peer in the ESTABLISHED state. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name [Action] The connection is 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>*: Source peer description name *<length>*: Received message length [Action] Check the unicast routing program (BGP4+) on the peer.
46	bgp4+_recv_update: Peer *<bgp name>* [(*<description>*)] UPDATE unreachable prefix length *<length1>* exceeds packet length *<length2>*	Error (remote device)
		The prefix length of unreachable route information of the UPDATE message from the relevant peer exceeds the packet length. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length1>*: Prefix length of unreachable route information in the received message *<length2>*: Received packet length [Action] Check the unicast routing program (BGP4+) on the peer.
47	bgp4+_recv_update: Peer *<bgp name>* [(*<description>*)] UPDATE unreachable prefix length *<length>* too long	Error (remote device)
		The prefix length of the unreachable route information of the UPDATE message from the relevant peer exceeds 128 bits. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length>*: Prefix length in the received message [Action] Check the unicast routing program (BGP4+) on the peer.
48	bgp4+_recv_update: Peer *<bgp name>* [(*<description>*)] UPDATE prefix length *<length1>* exceeds unreachable prefix data remaining (*<length2>* bytes)	Error (remote device)
		The prefix length of unreachable route information of the UPDATE message from the relevant peer exceeds the prefix data of unreachable route information. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length1>*: Prefix length in the received message *<length2>*: Actual data length [Action] Check the unicast routing program (BGP4+) on 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>*: Source peer description name *<length>*: Actual data length [Action] Check the unicast routing program (BGP4+) on 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 when compared with the actual path attribute length. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length1>*: Path attribute length of the received message *<length2>*: Actual data length [Action] Check the unicast routing program (BGP4+) on 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>*: Source peer description name [Action] Check the unicast routing program (BGP4+) on 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>*: Source peer description name [Action] Check the unicast routing program (BGP4+) on 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>*: Source peer description name [Action] Check the unicast routing program (BGP4+) on the peer.
54	bgp4+_recv_update: Peer *<bgp name>* [(*<description>*)] UPDATE has path attributes but no reachable prefixes!	Error (remote device)
		The UPDATE message from the relevant peer has path attributes but does not have the corresponding route information. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name [Action] Check the unicast routing program (BGP4+) on 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>*: Source peer description name *<as1>*: AS number of the source peer *<as2>*: Next-hop AS number in the received message [Action] Check the unicast routing program (BGP4+) on the peer.
56	bgp4+_recv_update: Ignores prefix from peer *<bgp name>* [(*<description>*)] in RFC-1771's NLRI field	Warning (remote device)
		Route information in a format that complies with RFC1771 instead of RFC2858 is ignored. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name [Action] Check the unicast routing program (BGP4+) on 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 relevant peer is invalid. No address family exists. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length>*: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4+) on 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 relevant peer is invalid. No next-hop length exists. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length>*: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4+) on 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 relevant peer is invalid. No next hop exists. [Explanation of message variables] *<bgp name>*: Source peer name *<description>*: Source peer description name *<length>*: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4+) on 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 relevant peer is invalid. No reserved field exists. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Source peer description name <*length*>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4+) on 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 relevant peer is invalid. No SNPA length exists. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Source peer description name <*length*>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4+) on 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 relevant peer is invalid. No SNPA exists. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Source peer description name <*length*>: Received MP_REACH_NLRI attribute length [Action] Check the unicast routing program (BGP4+) on 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 when compared with the remaining data. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Source peer description name <*length1*>: Prefix length in the received message <*length2*>: Actual data length [Action] Check the unicast routing program (BGP4+) on 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*>: Source peer description name <*length*>: Received message length [Action] Check the unicast routing program (BGP4+) on 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>*: Source peer description name *\<length>*: Next-hop address length [Action] Check the unicast routing program (BGP4+) on 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 on the same network. [Explanation of message variables] *\<bgp name>*: Source peer name *\<description>*: Source peer description name *\<ipv6 address>*: Next hop address [Action] Check the unicast routing program (BGP4+) on the peer.
67	bgp4+_recv_reach: Peer *\<bgp name>* [(*\<description>*)] unknown family/subfamily *\<family>*/ *\<subfamily>*	Error (remote device)
		Route information other than IPv6 unicast was received from the relevant peer. [Explanation of message variables] *\<bgp name>*: Source peer name *\<description>*: Source peer description name *\<family>*: Address family *\<subfamily>*: Sub-address family [Action] Check the unicast routing program (BGP4+) on 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 relevant peer is invalid. No address family exists. [Explanation of message variables] *\<bgp name>*: Source peer name *\<description>*: Source peer description name *\<length>*: Received MP_UNREACH_NLRI attribute length [Action] Check the unicast routing program (BGP4+) on 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 the unreachable route information of the UPDATE message from the relevant peer exceeds the data length of remaining unreachable route information. [Explanation of message variables] *\<bgp name>*: Source peer name *\<description>*: Source peer description name *\<length>*: Next-hop address length [Action] Check the unicast routing program (BGP4+) on 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 the unreachable route information of the UPDATE message from the relevant peer exceeds 128 bits. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Source peer description name <*length*>: Prefix length in the received message [Action] Check the unicast routing program (BGP4+) on the peer.
71	bgp4+_recv_unreach: Peer <*bgp name*> [(<*description*>)] unknown family/subfamily <*family*>/<*subfamily*>	Error (remote device)
		Unreachable route information other than IPv6 unicast was received from the relevant peer. [Explanation of message variables] <*bgp name*>: Source peer name <*description*>: Source peer description name <*family*>: Address family <*subfamily*>: Sub-address family [Action] Check the unicast routing program (BGP4+) on the peer.
72	bgp4+_peer_established: Peer <*bgp name*> [(<*description*>)] connection established	Information (local device or remote device)
		A BGP4+ connection was established with the relevant peer. [Explanation of message variables] <*bgp name*>: Connection destination peer name <*description*>: Connection destination peer description name [Action] None.
73	bgp4+_ifachange: Peer <*bgp name*> [(<*description*>)]: Closed connection by changing interface state	Information (local device or remote device)
		A BGP4+ connection was closed due to a change in the interface state. [Explanation of message variables] <*bgp name*>: Connection destination peer name <*description*>: Connection destination peer description name [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 destination peer name <*description*>: Connection destination peer description name [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 destination peer name <*description*>: Connection destination peer description name [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 destination peer name *<description>*: Connection destination peer description name [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 destination peer name *<description>*: Connection destination peer description name [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)
		The peer that performed graceful restart could not save the forwarding routes. All the routes that had been learned have been deleted from the relevant peer. [Explanation of message variables] *<bgp name>*: Connection destination peer name [Action] Check the unicast routing program (BGP4+) on 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)
		The peer that performed graceful restart could not save the forwarding routes. All the routes that had been learned have been deleted from the relevant peer. [Explanation of message variables] *<bgp name>*: Connection destination peer name [Action] Check the unicast routing program (BGP4+) on the peer.
80	bgp4+_restart_timeout: Peer *<bgp name>* [(*<description>*)]: Timed out waiting for reconnect.	Error (local device or remote device)
		Graceful restart failed. A connection with the peer router could not be established within the restart time specified by the peer router. [Explanation of message variables] *<bgp name>*: Connection destination peer name *<description>*: Connection destination peer description name [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)
		Graceful restart failed. `End-Of-RIB` could not be received from the peer router. [Explanation of message variables] *<bgp name>*: Connection destination peer name *<description>*: Connection destination peer description name [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 device or remote device)
		A BGP connection with the relevant peer was re-established. [Explanation of message variables] <*bgp name*>: Connection destination peer name <*description*>: Connection destination peer description name [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*>: Source peer description name [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*>: Destination peer name <*description*>: Destination peer description name [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*>: Destination peer name <*description*>: Destination peer description name <*code*> (<*code string*>) and <*subcode*> (<*subcode string*>): Error code and error subcode

#	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/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, *<code string>* displays `invalid`. If the *<subcode>* value is invalid, *<subcode string>* displays `unknown`.
		  - *<value>* or *<data>* indicates information about the data field of the `NOTIFICATION` message.
		  <value>: Decimal notation
		  <data>: Hexadecimal notation
		
		[Action]
		Check the network configuration and the peer configuration. If there is no problem with the configurations, check the unicast routing program (BGP4+) on 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>*: Source peer description name *<code>* (*<code string>*) and *<subcode>* (*<subcode string>*): Error code and error subcode

#	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/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, *<code string>* displays `invalid`. If the *<subcode>* value is invalid, *<subcode string>* displays `unknown`. - *<value>* or *<data>* indicates information about the data field of the `NOTIFICATION` message. *<value>*: Decimal notation *<data>*: Hexadecimal notation [Action] Check the network configuration and other configurations.
87	BGP4+: No MD5 digest from *<source ipv6>*+*<port no.>* to *<destination ipv6>*+*<port no.>* [VRF *<vrf id>*]	Warning (remote device)
		The MD5 authentication option is not set for the TCP segment received by BGP4+ connection. Output of this operation message is as follows: 1. For the first 16 events, the message is output for each event. 2. For the 17th and subsequent events, the message is output once every 256 events. 3. If events occur three or more minutes after the last event has occurred, the message is output as described in 1 and 2 above. Note that the counting described above includes the number of times the `BGP4+: Invalid MD5 digest from` *<source ipv6>* + *<port no.>* `to` *<destination ipv6>* + *<port no.>* message is output.

#	Message text	Description
72		[Explanation of message variables] *<source ipv6>*: Source IPv6 address *<port no.>*: TCP port number *<destination ipv6>*: Destination IPv6 address *<vrf id>*: VRF ID [Action] Check whether the MD5 authentication is set in BGP4+ of the remote system. If it is not set, set the MD5 authentication so that it matches. If the setting matches, check whether TCP segments are sent from a peer other than the source BGP4+ peer.
88	BGP4+:	Warning (local device or remote device)
	Invalid MD5 digest from *<source ipv6>*+*<port no.>* to *<destination ipv6>*+*<port no.>* [VRF *<vrf id>*]	The MD5 authentication option for TCP segments received by BGP4+ connection is invalid. Output of this operation message is as follows: 1. For the first 16 events, the message is output for each event. 2. For the 17th and subsequent events, the message is output once every 256 events. 3. If events occur three or more minutes after the last event has occurred, the message is output as described in 1 and 2 above. Note that the counting described above includes the number of times the `BGP4+: No MD5 digest from`*<source ipv6>* + *<port no.>* `to` *<destination ipv6>* + *<port no.>* message is output. [Explanation of message variables] *<source ipv6>*: Source IPv6 address *<port no.>*: TCP port number *<destination ipv6>*: Destination IPv6 address *<vrf id>*: VRF ID [Action] Check 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 being sent from a peer other than the source BGP4+ peer.
89	BGP4+:	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>*: Source peer description name *<routes1>*: Number of paths learned from the peer *<routes2>*: Maximum number of paths that can be learned from the peer [Action] If the number of paths learned from the relevant peer further increases, check the number of the paths advertised by the peer.
90	BGP4+:	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>*: Source peer description name *<routes1>*: Number of paths learned from the peer *<routes2>*: Maximum number of paths that can be learned from the peer [Action] Check the number of the paths advertised by the relevant peer.
91	BGP4+:	Information (remote device)
	Peer *<bgp name>* [(*<description>*)]: Closed connection by maximum-prefix	BGP4+ connection was closed due to the limitation on the number of learned paths. [Explanation of message variables] *<bgp name>*: Connection destination peer name *<description>*: Connection destination peer description name [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+_pp_recv:	Warning (remote device)
	Peer *<bgp name>* as receiving-speaker failed to retain stale routes, the packets forwarded to the peer may be discarded.	The peer running as the receiving router could not save the forwarding routes. The packets forwarded to the relevant peer might have been discarded. [Explanation of message variables] *<bgp name>*: Connection destination peer name [Action] During negotiation of the graceful restart functionality, it was reported that forwarding was disabled. Make sure that the peer router has not failed.
93	bgp4+_recv_open:	Warning (remote device)
	Peer *<bgp name>* as receiving-speaker failed to retain stale routes, the packets forwarded to the peer may be discarded.	The peer running as the receiving router could not save the forwarding routes. The packets forwarded to the relevant peer might have been discarded. [Explanation of message variables] *<bgp name>*: Connection destination peer name [Action] During negotiation of the graceful restart functionality, it was reported that forwarding was disabled. Make sure that the peer router has not failed.
94	BGP4+:	Information (local device)
	Completed the learning from receiving-speakers	Learning of route information from the receiving router has been completed. [Explanation of message variables] None. [Action] None.
95	BGP4+:	Information (local device)

#	Message text	Description
74	Start advertisement, giving up learning from several receiving-speakers	Route advertisement will start, interrupting the learning of route information from some receiving routers. [Explanation of message variables] None. [Action] None.
96	BGP4+: Peer *<bgp name>* [(*<description>*)] UPDATE included attribute type code (0) [- AS Path (*<as number>*): *<aspath>*]	Warning (remote device)
		An UPDATE message including a path attribute with 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>*: Source peer description name *<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+) on the peer.

2.2.4 Event information common to the IPv6 unicast routing protocols

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

Table 2-8: Event information common to the IPv6 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. Check the capacity limits.
2	Rtm: Graceful Restart terminated because this system failed to retain the routes.	Warning (local device)
		Graceful Restart failed because the routes could not be retained. [Explanation of message variables] None. [Action] Make sure that a system switchover was not performed again or that the unicast routing program was not restarted during graceful restart.

#	Message text	Description
3	The number of IPv6 unicast routes on global network exceeded the limit.	Warning (local device)
		The number of IPv6 unicast routes on the global network exceeded the maximum number of routes. [Explanation of message variables] None. [Action] 1. Delete unnecessary routes. 2. Check the maximum number of routes specified in the configuration.
4	The number of IPv6 unicast routes on VRF *<vrf id>* exceeded the limit.	Warning (local device)
		The number of IPv6 unicast routes on the VRF *<vrf id>* exceeded the maximum number of routes. [Explanation of message variables] *<vrf id>*: VRF ID [Action] 1. Delete unnecessary routes. 2. Check the maximum number of routes specified in the configuration.
5	The number of IPv6 unicast routes on global network exceeded the warning threshold.	Information (local device)
		The number of IPv6 unicast routes on the global network exceeded the warning threshold. [Explanation of message variables] None. [Action] When adding routes, make sure that the maximum number of routes is not exceeded.
6	The number of IPv6 unicast routes on VRF *<vrf id>* exceeded the warning threshold.	Information (local device)
		The number of IPv6 unicast routes on the VRF *<vrf id>* exceeded the warning threshold. [Explanation of message variables] *<vrf id>*: VRF ID [Action] When adding routes, make sure that the maximum number of routes is not exceeded.

2.3 IPv6 routing information (RTM)

2.3.1 RA

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

Table 2-9: 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 is 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 is 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 the interface that receives the router solicitation [Action] Check the router solicitation setting on 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 is ignored because the link layer address option has been set for the router solicitation from an unspecified address (: :). [Explanation of message variables] *<interface name>*: Name of the interface that receives the router solicitation [Action] Check the router solicitation setting on the router solicitation sender terminal.
4	rs_input: RS received on non advertising interface(*<interface name>*)	Warning (local device)
		The router solicitation is ignored because the router solicitation was received by an interface that does not advertise routers. [Explanation of message variables] *<interface name>*: Name of the interface that receives the router solicitation [Action] If it is necessary to respond to the router solicitation, enable router advertisement in the interface.

#	Message text	Description
5	rs_input: RS with invalid hop limit (*\<hoplimit\>*) received from *\<address\>* on *\<interface name\>*	Error
		The router solicitation is ignored because the hop limit of the received router solicitation packet is not the correct value (255). [Explanation of message variables] *\<hoplimit\>*: Hop limit value of the received router solicitation message *\<address\>*: Router solicitation sender address *\<interface name\>*: Name of the interface that receives the router solicitation [Action] Check the settings of the router that sends router solicitations.
6	rs_input: RS with invalid ICMP6 code(*\<code\>*) received from *\<address\>* on *\<interface name\>*	Error
		The router solicitation is 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 the interface that receives the router solicitation [Action] Check the settings of the router that sends router solicitations.
7	rs_input: RS from *\<address\>* on *\<interface name\>* does not have enough length (len = *\<length\>*)	Error
		The router solicitation is ignored because the received router solicitation packet is too short. [Explanation of message variables] *\<address\>*: Router solicitation sender address *\<interface name\>*: Name of the interface that receives the router solicitation *\<length\>*: Length of the received router solicitation packet [Action] Check the settings of the router that sends router solicitations.
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 for 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 the router advertisement sending interface [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 the router advertisement sending interface [Action] If this error frequently occurs, check the status of the interface.

#	Message text	Description
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 the router advertisement sending interface *<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/PIM-DM

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

Table 2-10: IPv4 multicast routing (PIM-SM/PIM-DM) event information

#	Message text	Description
1	IGMP: received packet too short (*<length>* bytes) for IP header [on VRF *<vrf id>*]	Error (remote device)
		A packet smaller than the IP header was received. [Explanation of message variables] *<length>*: Received packet size *<vrf id>*: VRF ID [Action] The remote device has sent invalid packets. Check the IPv4 multicast communication program of the remote device.
2	IGMP: received packet (*<length1>* bytes) from *<source address>* shorter than header + data length (*<length2>* + *<length3>* bytes) [on VRF *<vrf id>*]	Error (remote device)
		A packet smaller than the data length specified in the IP header was received. [Explanation of message variables] *<length1>*: Size of the received packet *<source address>*: Source IPv4 address *<length2>*: Received IP header size *<length3>*: Size of the received IP packet data *<vrf id>*: VRF ID [Action] The remote device has sent invalid packets. Check the IPv4 multicast communication program of the remote device.
3	IGMP: received IP data field too short (*<length>* bytes) for IGMP header, from *<source address>* to *<destination address>* [on VRF *<vrf id>*]	Error (remote device)
		A packet smaller than an IGMP header length (8) was received. [Explanation of message variables] *<length>*: Size of the received IP packet data *<source address>*: Source IPv4 address *<destination address>*: Destination IPv4 address *<vrf id>*: VRF ID [Action] The remote device has sent invalid packets. Check the IPv4 multicast communication program of the remote device.
4	IGMP: ignoring packet from *<source address>* to *<destination address>* [on VRF *<vrf id>*] - invalid igmp header checksum (data '*<data>*', length '*<length>*')	Error (remote device)
		A received IGMP packet was ignored because of an IGMP header checksum error. [Explanation of message variables] *<source address>*: Source IPv4 address *<destination address>*: Destination IPv4 address *<vrf id>*: VRF ID *<data>*: Contents of the first byte (packet type) of IGMP received data *<length>*: IGMP received data length [Action] The remote device has sent invalid packets. Check the IPv4 multicast communication program of the remote device.

#	Message text	Description
5	IGMP: ignoring *\<packet\>* from *\<source address\>* to *\<destination address\>* [on VRF *\<vrf id\>*] - invalid group address '*\<group address\>*'	Error (remote device)
		A received IGMP packet was ignored because the group address in the packet was invalid. [Explanation of message variables] *\<packet\>*: Packet type • `Group Membership Report`, `Group Leave Report` *\<source address\>*: Source IPv4 address *\<destination address\>*: Destination IPv4 address *\<vrf id\>*: VRF ID *\<group address\>*: Received group address [Action] The remote device has sent invalid packets. Check the IPv4 multicast communication program of the remote device.
6	IGMP: Querier was changed on interface *\<interface name\>* [of VRF *\<vrf id\>*] - new querier *\<querier ip address\>* (was *\<old querier ip address\>*)	Event (local device)
		The querier router changed on the interface. [Explanation of message variables] *\<interface name\>*: Interface name *\<vrf id\>*: VRF ID *\<querier ip address\>*: Querier IPv4 address *\<old querier ip address\>*: Previous querier IPv4 address [Action] None.
7	PIM: received packet too short (*\<length\>* bytes) for IP header [on VRF *\<vrf id\>*]	Error (remote device)
		A packet smaller than the IP header was received. [Explanation of message variables] *\<length\>*: Received packet size *\<vrf id\>*: VRF ID [Action] The remote device has sent invalid packets. Check the IPv4 multicast routing program (PIM-SM or PIM-DM) of the remote device.
8	PIM: received packet (*\<length1\>* bytes) from *\<source address\>* shorter than header + data length (*\<length2\>* + *\<length3\>* bytes) [on VRF *\<vrf id\>*]	Error (remote device)
		A packet smaller than the data length specified in the IP header was received. [Explanation of message variables] *\<length1\>*: Size of the received packet *\<source address\>*: Source IPv4 address *\<length2\>*: Received IP header size *\<length3\>*: Size of the received IP packet data *\<vrf id\>*: VRF ID [Action] The remote device has sent invalid packets. Check the IPv4 multicast routing program (PIM-SM or PIM-DM) of the remote device.

#	Message text	Description
9	PIM: received IP data field too short (*<length>* bytes) for PIM header, from *<source address>* to *<destination address>* [on VRF *<vrf id>*]	Error (remote device)
		A packet smaller than the PIM header length (4) was received. [Explanation of message variables] *<length>*: Size of the received IP packet data *<source address>*: Source IPv4 address *<destination address>*: Destination IPv4 address *<vrf id>*: VRF ID [Action] The remote device has sent invalid packets. Check the IPv4 multicast routing program (PIM-SM or PIM-DM) of the remote device.
10	PIM: ignoring packet from *<source address>* to *<destination address>* [on VRF *<vrf id>*] - invalid pim header checksum (data '*<data>*', length '*<length>*')	Error (remote device)
		A received PIM packet was ignored because of a PIM header checksum error. [Explanation of message variables] *<source address>*: Source IPv4 address *<destination address>*: Destination IPv4 address *<vrf id>*: VRF ID *<data>*: Contents of the first byte (packet type) of received PIM data *<length>*: Length of the received PIM data [Action] The remote device has sent invalid packets. Check the IPv4 multicast routing program (PIM-SM or PIM-DM) of the remote device.
11	PIM: ignoring *<packet>* message from *<source address>* to *<destination address>* [on VRF *<vrf id>*] - packet too short (*<length>* bytes)	Error (remote device)
		A received PIM packet was ignored because the packet size was smaller than the minimum packet length. [Explanation of message variables] *<packet>*: Packet type • `Register`, `Register-Stop`, `Join/Prune`, `Assert`, `Bootstrap`, `Candidate-RP-Advertisement` *<source address>*: Source IPv4 address *<destination address>*: Destination IPv4 address *<vrf id>*: VRF ID *<length>*: Length of the received PIM data [Action] The remote device has sent invalid packets. Check the IPv4 multicast routing program (PIM-SM) of the remote device.

#	Message text	Description
12	PIM: ignoring *\<packet\>* message from *\<source address\>* to *\<destination address\>* [on VRF *\<vrf id\>*] - invalid encoded unicast address (*\<cause\>*)	Error (remote device)
		A received PIM packet was ignored because the encoding unicast address in the packet was invalid. [Explanation of message variables] *\<packet\>*: Packet type • `Register-Stop, Join/Prune, Assert, Bootstrap, Candidate-RP-Advertisement` *\<source address\>*: Source IPv4 address *\<destination address\>*: Destination IPv4 address *\<vrf id\>*: VRF ID *\<cause\>*: Detailed cause • `address family '`*\<value\>*`'`: The address family *\<value\>* is invalid (other than 1). • `encoding type '`*\<value\>*`'`: The encoding type *\<value\>* is invalid (other than 0). • `source address '`*\<address\>*`'`: The source IPv4 address *\<address\>* is invalid. • `upstream neighbor address '`*\<address\>*`'`: The upstream neighbor IPv4 address *\<address\>* is invalid. • `BSR address '`*\<address\>*`'`: The BSR address *\<address\>* is invalid. • `RP address '`*\<address\>*`'`: The rendezvous point address *\<address\>* is invalid. [Action] The remote device has sent invalid packets. Check the IPv4 multicast routing program (PIM-SM) of the remote device.
13	PIM: ignoring *\<packet\>* message from *\<source address\>* to *\<destination address\>* [on VRF *\<vrf id\>*] - invalid encoded source address (*\<cause\>*)	Error (remote device)
		A received PIM packet was ignored because the encoding sender IPv4 address in the packet was invalid. [Explanation of message variables] *\<packet\>*: Packet type • `Join/Prune` *\<source address\>*: Source IPv4 address *\<destination address\>*: Destination IPv4 address *\<vrf id\>*: VRF ID *\<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] The remote device has sent invalid packets. Check the IPv4 multicast routing program (PIM-SM) of the remote device.

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

#	Message text	Description
17	PIM: ignoring Register message from *<source address>* to *<destination address>* [on VRF *<vrf id>*] - invalid inner source address '*<inner source address>*'	Error (remote device)
		A received PIM packet was ignored because the source IPv4 address of IP packets encapsulated by the Register packet was invalid. [Explanation of message variables] *<source address>*: Source IPv4 address *<destination address>*: Destination IPv4 address *<vrf id>*: VRF ID *<inner source address>*: Encapsulated source IPv4 address [Action] The multicast data sender has sent invalid packets. Check the IPv4 multicast communication program of the multicast data sender.
18	PIM: ignoring Register message from *<source address>* to *<destination address>* [on VRF *<vrf id>*] - invalid inner group address '*<inner group address>*'	Error (remote device)
		A received PIM packet was ignored because the group address of IP packets encapsulated by the Register packet was invalid. [Explanation of message variables] *<source address>*: Source IPv4 address *<destination address>*: Destination IPv4 address *<vrf id>*: VRF ID *<inner group address>*: Encapsulated group address [Action] The multicast data sender has sent invalid packets. Check the IPv4 multicast communication program of the multicast data sender. If the encapsulated group address is in the range from PIM to SSM, check the PIM-SSM setting of the remote device.
19	PIM: ignoring Bootstrap message from *<source address>* to *<destination address>* [on VRF *<vrf id>*] - invalid hash mask length '*<value>*'	Error (remote device)
		A received PIM packet was ignored because the hash mask length in the Bootstrap packet was invalid (33 or more). [Explanation of message variables] *<source address>*: Source IPv4 address *<destination address>*: Destination IPv4 address *<vrf id>*: VRF ID *<value>*: Hash mask length specified for the received packet [Action] The remote device has sent invalid packets. Check the IPv4 multicast routing program (PIM-SM) of the remote device.
20	PIM: BSR information was changed [on VRF *<vrf id>*] - lost BSR information	Warning (remote device)
		BSR information was cleared because advertisements from the bootstrap router were lost. [Explanation of message variables] *<vrf id>*: VRF ID [Action] Investigate why advertisements from the bootstrap router were lost.

#	Message text	Description
21	PIM: BSR information was changed [on VRF *<vrf id>*] - new BSR address *<ip address>*	Event (local device)
		BSR address was changed. [Explanation of message variables] *<vrf id>*: VRF ID *<ip address>*: BSR address If the BSR address is this device, (this system) is displayed after the IPv4 address. [Action] None.
22	PIM: started learning IPv4 multicast routing entries due to a system change (learning time is about *<time>* seconds)	Event (local device)
		A switchover from the standby system to the active system caused the learning of IPv4 multicast route information to be started. (The learning time is about *<time>* seconds.) [Explanation of message variables] *<time>* Re-learning time [Action] None.
23	PIM: completed learning IPv4 multicast routing entries after the system change	Event (local device)
		A switchover from the standby system to the active system caused the learning of IPv4 multicast route information to be finished. [Explanation of message variables] None. [Action] None.

2.5 IPv6 multicast routing information (MR6)

2.5.1 IPv6 PIM-SM

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

Table 2-11: IPv6 multicast routing (PIM-SM) event information

#	Message text	Description
1	MLD: ignoring *<packet>* from *<source address>* [on VRF *<vrf id>*] - invalid scope *<group address>*	Error (remote device)
		MLD packets were ignored because the scope of group addresses included in the packets was invalid (node local or link local). [Explanation of message variables] *<packet>*: Packet type • `Multicast Listener Query, Multicast Listener Report, Multicast Listener Done, MLDv2 Multicast Listener Report` *<source address>*: Source IPv6 address *<vrf id>*: VRF ID *<group address>*: MLD group address [Action] The remote device has sent invalid packets. Check the IPv6 multicast communication program of the partner device.
2	MLD: ignoring *<packet>* from *<source address>* [on VRF *<vrf id>*] - message received from a non linklocal address	Error (remote device)
		MLD packets that have non-link local addresses in the source were ignored. [Explanation of message variables] *<packet>*: Packet type • `Multicast Listener Query` *<source address>*: Source IPv6 address *<vrf id>*: VRF ID [Action] The remote device has sent invalid packets. Check the IPv6 multicast communication program of the partner device.
3	MLD: Querier was changed on interface *<interface name>* [of VRF *<vrf id>*] - new querier *<querier ipv6 address>* (was *<old querier ipv6 address>*)	Event (local device)
		The querier router changed on the interface. [Explanation of message variables] *<interface name>*: Interface name *<vrf id>*: VRF ID *<querier ipv6 address>*: Querier IPv6 address • If the querier IPv6 address is this device, `(this system)` is displayed. *<old querier ipv6 address>*: Previous querier IPv6 address • If the previous querier IPv6 address is this device, `(this system)` is displayed. [Action] None.

#	Message text	Description
4	PIM: ignoring *<packet>* message from *<source address>* [on VRF *<vrf id>*] - packet too short (*<length>* bytes)	Error (remote device)
		A received PIM packet was ignored because the packet size was smaller than the minimum packet length. [Explanation of message variables] *<packet>*: Packet type • `Hello, Register, Register-Stop, Join/Prune, Assert, Bootstrap, Candidate-RP-Advertisement` *<source address>*: Source IPv6 address *<vrf id>*: VRF ID *<length>*: Length of the received PIM data [Action] The remote device has sent invalid packets. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.
5	PIM: ignoring *<packet>* message from *<source address>* [on VRF *<vrf id>*] - invalid encoded unicast address (*<cause>*)	Error (remote device)
		A received PIM packet was ignored because the encoding unicast address in the packet was invalid. [Explanation of message variables] *<packet>*: Packet type • `Hello, Register-Stop, Join/Prune, Assert, Bootstrap, Candidate-RP-Advertisement` *<source address>*: Source IPv6 address *<vrf id>*: VRF ID *<cause>*: Detailed cause • `address family '<value>'`: The address family *<value>* is invalid (other than 2). • `encoding type '<value>'`: The encoding type *<value>* is invalid (other than 0). • `source address '<address>'`: The source address *<address>* is invalid. • `upstream neighbor address '<address>'`: The upstream address *<address>* is invalid. • `BSR address '<address>'`: The BSR address *<address>* is invalid. • `RP address '<address>'`: The rendezvous point address *<address>* is invalid. [Action] The remote device has sent invalid packets. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.
6	PIM: ignoring *<packet>* message from *<source address>* [on VRF *<vrf id>*] - invalid encoded source address (*<cause>*)	Error (remote device)
		A received PIM packet was ignored because the encoding source address was invalid. [Explanation of message variables] *<packet>*: Packet type • `Join/Prune` *<source address>*: Source IPv6 address *<vrf id>*: VRF ID *<cause>*: Detailed cause • `address family '<value>'`: The address family *<value>* is invalid (other than 2). • `encoding type '<value>'`: The encoding type *<value>* is invalid (other than 0). [Action] The remote device has sent invalid packets. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.

#	Message text	Description
7	PIM: ignoring *\<packet\>* message from *\<source address\>* [on VRF *\<vrf id\>*] - invalid encoded group address (*\<cause\>*)	Error (remote device)
		A received PIM packet was ignored because the encoding group address in the packet was invalid. [Explanation of message variables] *\<packet\>*: Packet type • `Register-Stop`, `Join/Prune`, `Assert`, `Bootstrap`, `Candidate-RP-Advertisement` *\<source address\>*: Source IPv6 address *\<vrf id\>*: VRF ID *\<cause\>*: Detailed cause • `address family '`*\<value\>*`'`: The address family *\<value\>* is invalid (other than 2). • `encoding type '`*\<value\>*`'`: The encoding type *\<value\>* is invalid (other than 0). • `mask length '`*\<value\>*`'`: The group mask length *\<value\>* is invalid (not in the range from 8 to 128). • `group address '`*\<address\>*`'`: The group address *\<address\>* is invalid. [Action] The remote device has sent invalid packets. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.
8	PIM: ignoring Hello message from *\<source address\>* [on VRF *\<vrf id\>*] - invalid holdtime option length (*\<length\>*)	Error (remote device)
		A received PIM packet was ignored because the length of the holdtime option in the Hello packet was invalid (other than 2). [Explanation of message variables] *\<source address\>*: Source IPv6 address *\<vrf id\>*: VRF ID *\<length\>*: Received holdtime option length [Action] The remote device has sent invalid packets. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.
9	PIM: ignoring Hello message from *\<source address\>* [on VRF *\<vrf id\>*] - no 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 *\<vrf id\>*: VRF ID [Action] The remote device has sent invalid packets. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.
10	PIM: ignoring Register message from *\<source address\>* [on VRF *\<vrf id\>*] - invalid inner source address '*\<inner source address\>*'	Error (remote device)
		A received PIM packet was ignored because the source address of IPv6 packets encapsulated by the `Register` packet was invalid. [Explanation of message variables] *\<source address\>*: Source IPv6 address *\<vrf id\>*: VRF ID *\<inner source address\>*: Encapsulated source address [Action] The multicast data sender has sent invalid packets. Check the IPv6 multicast communication program of the multicast data sender.

#	Message text	Description
11	PIM: ignoring Register message from *<source address>* [on VRF *<vrf id>*] - invalid inner source address scope '*<inner source address>*'	Error (remote device)
		A received PIM packet was ignored because the scope of the source address of IPv6 packets encapsulated by the Register packet was invalid. [Explanation of message variables] *<source address>*: Source IPv6 address *<vrf id>*: VRF ID *<inner source address>*: Encapsulated source address [Action] The multicast data sender has sent invalid packets. Check the IPv6 multicast communication program of the multicast data sender.
12	PIM: ignoring Register message from *<source address>* [on VRF *<vrf id>*] - invalid inner group address '*<inner group address>*'	Error (remote device)
		A received PIM packet was ignored because the group address of IPv6 packets encapsulated by the Register packet was invalid. [Explanation of message variables] *<source address>*: Source IPv6 address *<vrf id>*: VRF ID *<inner group address>*: Encapsulated group address [Action] The multicast data sender has sent invalid packets. Check the IPv6 multicast communication program of the multicast data sender.
13	PIM: ignoring Register message from *<source address>* [on VRF *<vrf id>*] - invalid inner group address scope '*<inner group address>*'	Error (remote device)
		A received PIM packet was ignored because the scope of the group address of IPv6 packets encapsulated by the Register packet was invalid. [Explanation of message variables] *<source address>*: Source IPv6 address *<vrf id>*: VRF ID *<inner group address>*: Encapsulated group address [Action] The multicast data sender has sent invalid packets. Check the IPv6 multicast communication program of the multicast data sender.
14	PIM: ignoring Register message from *<source address>* [on VRF *<vrf id>*] - invalid inner IP version '*<version>*'	Error (remote device)
		A received PIM packet was ignored because the version of IPv6 packets encapsulated by the Register packet was not version 6. [Explanation of message variables] *<source address>*: Source IPv6 address *<vrf id>*: VRF ID *<version>*: Encapsulated IP packet version [Action] The multicast data sender has sent invalid packets. Check the IPv6 multicast communication program of the multicast data sender.

#	Message text	Description
15	PIM: ignoring Bootstrap message from *\<source address>* [on VRF *\<vrf id>*] - invalid hash mask length '*\<value>*'	Error (remote device)
		A received PIM packet was ignored because the hash mask length in the Bootstrap packet was invalid (129 or more). [Explanation of message variables] *\<source address>*: Source IPv6 address *\<vrf id>*: VRF ID *\<value>*: Hash mask length specified for the received packet [Action] The remote device has sent invalid packets. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.
16	PIM: ignoring Bootstrap message from *\<source address>* [on VRF *\<vrf id>*] - invalid BSR address '*\<ipv6 address>*'	Error (remote device)
		A received PIM packet was ignored because the BSR address in the Bootstrap packet was invalid. [Explanation of message variables] *\<source address>*: Source IPv6 address *\<vrf id>*: VRF ID *\<ipv6 address>*: BSR address [Action] The remote device has sent invalid packets. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.
17	PIM: ignoring Bootstrap message from *\<source address>* [on VRF *\<vrf id>*] - cannot find a route to the BSR(*\<ipv6 address>*)	Warning (local device)
		A received PIM packet was ignored because the unicast route to the BSR address in the bootstrap was not found. [Explanation of message variables] *\<source address>*: Source IPv6 address *\<vrf id>*: VRF ID *\<ipv6 address>*: BSR address [Action] Make sure that the route to the BSR address in the Bootstrap packet exists.
18	PIM: ignoring Candidate-RP-Advertisement message from *\<source address>* [on VRF *\<vrf id>*] - non global address(*\<ipv6 address>*) as RP	Error (remote device)
		A received PIM packet was ignored because the rendezvous point address included in the Candidate-RP-Advertisement packet was invalid. [Explanation of message variables] *\<source address>*: Source IPv6 address *\<vrf id>*: VRF ID *\<ipv6 address>*: Rendezvous point address [Action] The remote device has sent invalid packets. Check the IPv6 multicast routing program (IPv6 PIM-SM) of the remote device.
19	PIM: BSR information was changed [on VRF *\<vrf id>*] - lost BSR information	Warning (remote device)
		BSR information was cleared because advertisements from the bootstrap router were lost. [Explanation of message variables] *\<vrf id>*: VRF ID [Action] Investigate why advertisements from the bootstrap router were lost.

#	Message text	Description
20	PIM: BSR information was changed [on VRF *\<vrf id\>*] - new BSR address *\<ipv6 address\>*	Event (local device)
		BSR address was changed. [Explanation of message variables] *\<vrf id\>*: VRF ID *\<ipv6 address\>*: BSR address If the BSR address is this device, (this system) is displayed after the IPv6 address. [Action] None.
21	PIM: Add interface *\<interface name\>* [of VRF *\<vrf id\>*] to the output interface list of (S,G)=(*\<source address\>*, *\<group address\>*)	Event (local device)
		The interface *\<interface name\>* was added to the output interface list of the multicast routing cache (S, G) (this message is output to the syslog interface only when the output of event information specific to syslog is enabled). Use the debug protocols ipv6-multicast command to enable the event information specific to syslog). [Explanation of message variables] *\<interface name\>*: Interface name *\<vrf id\>*: VRF ID *\<source address\>*: Source IPv6 address *\<group address\>*: IPv6 group address [Action] None.
22	PIM: Delete interface *\<interface name\>* [of VRF *\<vrf id\>*] from the output interface list of (S,G)=(*\<source address\>*, *\<group address\>*)	Event (local device)
		The interface *\<interface name\>* was deleted from the output interface list of the multicast routing cache (S, G) (this message is output to the syslog interface only when the output of event information specific to syslog is enabled). Use the debug protocols ipv6-multicast command to enable the event information specific to syslog). [Explanation of message variables] *\<interface name\>*: Interface name *\<vrf id\>*: VRF ID *\<source address\>*: Source IPv6 address *\<group address\>*: IPv6 group address [Action] None.
23	PIM: started learning IPv6 multicast routing entries due to a system change (learning time is about *\<time\>* seconds)	Event (local device)
		Learning of IPv6 multicast entries has started due to switching from the standby system to the active system (the learning time is about *\<time\>* seconds). [Explanation of message variables] *\<time\>*: Re-learning time [Action] None.
24	PIM: completed learning IPv6 multicast routing entries after the system change	Event (local device)
		Learning of IPv6 multicast entries due to switching from the standby system to the active system has been completed. [Explanation of message variables] None. [Action] None.

Chapter

3. Switch Failure and Event Information

This chapter describes the contents of switch failure and event information. All messages regarding switch failure and event information are output to the operation terminal window. 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 switch failure and event information when the event location is CONFIG.

Table 3-1: Switch 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	00010005	0100	There is mismatch between active and standby configuration.
	The active system configuration differs from the standby system configuration. [Explanation of message variables] None. [Action] 1. There is no problem if the configuration is being edited. 2. In all other cases, execute the save configuration command to make the active and standby system configurations the same (the standby system configuration becomes identical to the active system configuration). Note, however, that if the software versions are not the same for the active and standby systems, execution of the save configuration command might be disabled. If the command cannot be executed, make the software versions the same, and then execute the save configuration command.					
2	E3	CONFIG	00010006	0100	Active and standby configuration is identical.
	The active system configuration and the standby system configuration are the same. [Explanation of message variables] None. [Action] None.					
3	E3	CONFIG	09200001	0100	Active and standby configuration failed in synchronization.
	The running configuration file between the active and standby systems could not be synchronized at the beginning of redundant operation. [Explanation of message variables] None. [Action] Execute the save configuration command to make the configurations of the active and standby systems the same.					
4	E3	CONFIG	09200002	0100	Active and standby configuration successfully synchronized.
	The running configuration file was successfully synchronized between the active and standby systems at the beginning of redundant operation. [Explanation of message variables] None. [Action] None.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
5	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 the startup configuration file was not found or could not 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.					
6	E3	CONFIG	09300002	0100	Configuration command syntax error. line *<line number>* : "*<error syntax>*"
	Application of 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] If this log message is output when the software is downgraded, the configuration command indicated in the message is not supported by the software version after the downgrade. If the Switch is operating in a redundant configuration, the active system and the standby system have different configurations. If system switching occurs in this state, the new active system will restart after the switch. To prevent the switch from being restarted when the system is switched, restore the software to the version that existed before the update, delete the configuration command indicated in the log message, and then update the software again.					
7	E3	CONFIG	09300003	0100	Cannot change the interface configuration commands of NIF*<nif no.>*.
	The interface configuration of the NIF that is no longer consistent with the inserted board because the board was replaced, could not be changed. [Explanation of message variables] *<nif no.>*: NIF number [Action] Remove the NIF board, and then insert it again.					
8	E3	CONFIG	09300005	0100	The interface configuration commands of NIF *<nif no.>* changed, because NIF *<nif no.>* board connected.
	The interface configuration of the NIF changed because an NIF board was connected. [Explanation of message variables] *<nif no.>*: NIF number [Action] None.					
9	E3	CONFIG	09300006	0100	The interface configuration commands of NIF*<nif no.>* deleted, because NIF*<nif no.>* slot not exist.
	The interface configuration of an NIF slot that is non-existent on the Switch was deleted. [Explanation of message variables] *<nif no.>*: NIF number [Action] None.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
10	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.					
11	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.					
12	E3	CONFIG	09600006	1001	Configuration access management error. process*<process name>*:pid*<process id>*:time *<time>*
	The lock was released and the device 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.					
13	E5	CONFIG	00010007	0100	There is mismatch between active and standby configuration.
	The active system configuration differs from the standby system configuration. In this state, system switching cannot be performed by using the `redundancy force-switchover` command. If system switching occurs in this state due to a fatal error, or by clicking the Reset button, by pressing the ACH switch, or by executing the `reload active` command, the new active system will restart after the switch. [Explanation of message variables] None. [Action] 1. This message might be output when you are editing a configuration. In such a case, execute the `show logging` command after you have finished editing and make sure that the `Active and standby configuration is identical.` message has been output. If this message has been output, no action is required because the error has been recovered from automatically. 2. In all other cases, execute the `save` configuration command to make the active and standby system configurations the same (the standby system configuration becomes identical to the active system configuration). 3. Note, however, that if the software versions are not the same for the active and standby systems, execution of the `save` configuration command might be disabled. If the command cannot be executed, make the software versions the same, and then execute the `save` configuration command.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
14	R5	CONFIG	00010007	0100	Active and standby configuration is identical.
	The active system configuration and the standby system configuration are the same. [Explanation of message variables] None. [Action] None.				

3.2 Access

3.2.1 Event location = ACCESS

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

Table 3-2: Switch 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>* [on VRF *<vrf id>*].
	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 *<vrf id>*: VRF ID [Action] 1. There might have been an unauthorized access (an access from a remote host other than one permitted by the configuration) to the Switch. Check the remote host whose IPv4 address or IPv6 address is *<ip address>*. 2. If remote access from *<ip address>* is permitted, the configuration might be incorrect. Check the configuration. 3. If you want to permit remote access from *<ip address>*, specify access permissions for the configuration. 4. If remote access from VRF *<vrf id>* is permitted, the configuration might be incorrect. Check the configuration. 5. If you want to permit remote access from VRF *<vrf id>*, specify access permissions for the configuration.				
2	E3	ACCESS	00000002	0201 0205	Login incorrect *<user name>*.
	An attempt to log in by using the *<user name>* account was made, but 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 in the configuration. Check the operating status of the permitted remote host from the console or in the configuration. 2. This log data is collected even when a legitimate user executes an incorrect operation during login. Therefore, although this log data has been collected, the operating status of the remote host might be correct. 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, in the configuration increase the limit for the number of users who can log in.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
4	E3	ACCESS	00005002	0200	Login *<user name>* from *<host>* [on VRF *<vrf id>*] (*<term>*).
	A user logged in. [Explanation of message variables] *<user name>*: User name *<host>*: Host ID • For a remote operation terminal: IPv4 or IPv6 address • For a console terminal: `console` • For AUX terminal: `aux` *<vrf id>*: VRF ID *<term>*: Terminal name • For a remote operation terminal: `ttyp0` or higher • For a console terminal: `tty00` • For AUX terminal: `tty01` [Action] None.					
5	E3	ACCESS	00005003	0200	Logout *<user name>* from *<host>* [on VRF *<vrf id>*] (*<term>*).
	A user logged out. [Explanation of message variables] *<user name>*: User name *<host>*: Host ID • For a remote operation terminal: IPv4 or IPv6 address • For a console terminal: `console` • For AUX terminal: `aux` *<vrf id>*: VRF ID *<term>*: Terminal name • For a remote operation terminal: `ttyp0` or higher • For a console terminal: `tty00` • For AUX terminal: `tty01` [Action] None.					
6	E3	ACCESS	00010001	0204	SNMP agent program received packet from *<ip address>*[on VRF *<vrf id>*] with unexpected community name *<community name>*.
	The SNMP agent received a packet that had the unexpected community name *<community name>* from *<ip address>*. [Explanation of message variables] *<ip address>*: IPv4 address or IPv6 address of the SNMP manager *<vrf id>*: VRF ID *<community name>*: Community name [Action] Access to the Switch was attempted from a location other than the SNMP manager permitted in the configuration. This message is output if the IP address and the community name of the SNMP manager do not match the IP address and the community name of an SNMP manager permitted for the configuration. Check the configuration to make sure that the IP address and the community name of the SNMP manager that accesses the Switch are identical to *<ip address>* and *<community name>*. If they do not match, invalid access might be occurring. Contact the administrator of the SNMP manager to tell the responsible party not to access the SNMP manager at *<ip address>*. The Switch suppresses repeated output to the operation log of accesses from an invalid IP address or community. A maximum of 16 invalid IP address are saved and, for each saved IP address, one out of every 128 invalid access attempts is output to the log.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
7	E3	ACCESS	00020001	0206	Login incorrect *<user name>* for AUX port.
	An attempt to establish a PPP link via the AUX port by using the *< user name>* account was not permitted. [Explanation of message variables] *<user name>*: User name [Action] 1. There might have been an unauthorized access (failed account or password authentication) during PPP access to the AUX port. 2. This log data is collected even when a legitimate user executes an incorrect operation during login. Therefore, although this log data has been collected, the operating status might be correct.				
8	E3	ACCESS	00020002	0206	AUX port no Configuration.
	A link via the AUX port could not be established because the interface async configuration was not set. [Explanation of message variables] None. [Action] Check the interface async configuration.				
9	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 to the administrator mode (`enable` command). [Explanation of message variables] None. [Action] None.				
10	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 to the administrator mode (`enable` command). [Explanation of message variables] None. [Action] 1. There might have been an unauthorized access to the Switch from a remote host permitted by the configuration. Check the operating 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, although this log data has been collected, the operating status of the remote host might be correct.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
11	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 to the administrator mode (`enable` command). [Explanation of message variables] *<host>*: IP address or host name of the RADIUS server [Action] None.					
12	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 to 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. There might have been an unauthorized access to the Switch from a remote host permitted by the configuration. Check the operating 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, although this log data has been collected, the operating status of the remote host might be correct. 3. Check the RADIUS server setting.					
13	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 to 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. Check that the RADIUS server has started. 4. Check that the IP address of this Switch has been registered as a client IP address on the RADIUS server.					
14	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 to 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. Check if `acct-only` is specified for the RADIUS configuration to suppress authentication.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
15	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 to 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 the 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.					
16	E3	ACCESS	00030008	0201 0205 0208 0209	RADIUS authentication failed.
	RADIUS authentication failed for a user login request or request to change to 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.					
17	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.					
18	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).					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
19	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 to the administrator mode (`enable` command). [Explanation of message variables] *<host>*: IP address or host name of the TACACS+ server [Action] None.				
20	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 to 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. There might have been an unauthorized access to the Switch from a remote host permitted by the configuration. Check the operating 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, although this log data has been collected, the operating status of the remote host might be correct. 3. Check the TACACS+ server setting.				
21	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 to 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. Check that the TACACS+ server has started.				
22	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 to 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. Check if `acct-only` is specified for the TACACS+ configuration to suppress the authentication.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
23	E3	ACCESS	00030018	0201 0205 0208 0209	TACACS+ authentication failed.
	TACACS+ authentication failed for a user login request or request to change to 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.				
24	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. Check that the TACACS+ server has started. 5. Make sure that the IP address of the Switch is registered for the client IP address on the TACACS+ server side.				
25	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).				
26	E3	ACCESS	0003001c	0201 0208	TACACS+ authorization rejected from *<host>*.
	TACACS+ authentication was attempted, 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 the TACACS+ server side.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
27	E3	ACCESS	0003001d	0201 0208	Local authorization response with no contents.
	Local command authorization was performed, but neither a user name nor a command class or command list corresponding to the user name was set. [Explanation of message variables] None. [Action] Make sure that 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 switch failure and event information when the event location is IP.

Table 3-3: Switch 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	2b080b50	0600	Multicast routing entries was beyond 80 percent at total interface capacity.
	The total number of interfaces in the multicast routing information exceeded 80% of the capacity limit of the Switch. [Explanation of message variables] None. [Action] If you want to increase the number of interfaces in the routing information in the future, make sure that the total number of interfaces does not exceed the capacity limit.				
2	E4	IP	2b080b51	0600	Multicast routing entries exceeded capacity at total interface capacity.
	The total number of interfaces in the multicast routing information has exceeded the capacity limit of the Switch. [Explanation of message variables] None. [Action] Use the show ip mroute and show ipv6 mroute commands to make sure that the total number of interfaces in the current multicast routing information does not exceed the capacity limit of the Switch. If the capacity limit is exceeded, take one of the following actions: 1. Delete unnecessary information from the multicast routing information. 2. Review the network system configuration, and change it to one in which the multicast routing information can be reduced.				
3	E4	IP	2b090b00	0600	IPv4 unicast routing entries was beyond 80 percent of capacity.
	The number of IPv4 unicast routing entries exceeded 80% of the capacity limit. [Explanation of message variables] None. [Action] Note that the usage of IPv4 unicast routing entries (including APR entries) exceeded 80% of the capacity limit. Use the entries in a way that does not exceed the capacity limit.				
4	E4	IP	2b090b01	0600	IPv4 unicast routing entries exceeded capacity.
	The number of IPv4 unicast routing entries has exceeded the capacity limit. [Explanation of message variables] None. [Action] The resources for the IPv4 unicast routing entries are used by the IPv4 unicast routing entries and ARP entries. Use the show system command to make sure that the usage of IPv4 unicast routing entries has not reached the capacity limit of the switch. If the capacity limit has been reached, review the system configuration. If the number of entries is not reduced by taking the above actions, use the clear ip route command to update all the routing information.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
5	E4	IP	2b090b10	0600	IPv6 unicast routing entries was beyond 80 percent of capacity.
	The number of IPv6 unicast routing entries exceeded 80% of the capacity limit. [Explanation of message variables] None. [Action] Note that the usage of IPv6 unicast routing entries (including NDP entries) exceeded 80% of the capacity limit. Use the entries in a way that does not exceed the capacity limit.				
6	E4	IP	2b090b11	0600	IPv6 unicast routing entries exceeded capacity.
	The number of IPv6 unicast routing entries has exceeded the capacity limit. [Explanation of message variables] None. [Action] The resources for the IPv6 unicast routing entries are used by the IPv6 unicast routing entries and NDP entries. Use the `show system` command to make sure that the usage of IPv6 unicast routing entries has not reached the capacity limit of the switch. If the capacity limit has been reached, review the system configuration. If the number of entries is not reduced by taking the above actions, use the `clear ipv6 route` command to update all the routing information.				
7	E4	IP	2b090b20	0600	IPv4 multicast routing entries was beyond 80 percent of capacity.
	The number of IPv4 multicast routing information entries exceeded 80% of the capacity limit of the Switch. [Explanation of message variables] None. [Action] If you want to increase the number of entries in the routing information in the future, make sure that the number of entries does not exceed the capacity limit.				
8	E4	IP	2b090b21	0600	IPv4 multicast routing entries exceeded capacity.
	The number of IPv4 multicast routing information entries exceeds the capacity limit of the Switch. [Explanation of message variables] None. [Action] Using the `show system` command, make sure that the current number of IPv4 multicast routing information entries does not exceed the capacity limit. If the capacity limit is exceeded, take one of the following actions: 1. Delete unnecessary information from the IPv4 multicast routing information. 2. Review the network system configuration, and change it to one in which the IPv4 multicast routing information can be reduced.				
9	E4	IP	2b090b30	0600	IPv6 multicast routing entries was beyond 80 percent of capacity.
	The number of IPv6 multicast routing information entries exceeded 80% of the capacity limit of the Switch. [Explanation of message variables] None. [Action] If you want to increase the number of entries in the routing information in the future, make sure that the number of entries does not exceed the capacity limit.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
10	E4	IP	2b090b31	0600	IPv6 multicast routing entries exceeded capacity.
	The number of IPv6 multicast routing information entries exceeds the capacity limit of the Switch. [Explanation of message variables] None. [Action] Using the `show system` command, make sure that the current number of IPv6 multicast routing information entries does not exceed the capacity limit. If the capacity limit is exceeded, take one of the following actions: 1. Delete unnecessary information from the IPv6 multicast routing information. 2. Review the network system configuration, and change it to one in which the IPv6 multicast routing information can be reduced.				
11	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 of 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.				
12	E4	IP	50000006	0600	Because the number of pieces of the ARP entry exceeds the capacity of this system, the old entry was deleted and the new entry was added.
	An old entry was deleted and a new entry was added because the number of ARP table entries exceeded the capacity limit of the Switch. [Explanation of message variables] None. [Action] If this message is output frequently, take one of the following actions: 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 one in which the number of ARP table entries can be reduced.				
13	E4	IP	50000007	0600	Because the number of pieces of the ARP entry exceeds the capacity of *<vrf>*, the old entry was deleted and the new entry was added.
	An old entry was deleted and a new entry was added because the number of ARP table entries in the *<vrf>* exceeded the upper limit for each VRF. [Explanation of message variables] *<vrf>*: VRF that exceeded the upper limit for ARP • VRF *<vrf id>*: VRF whose VRF ID is *<vrf id>* • `global network`: Global network [Action] If this message is output frequently, take one of the following actions: 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 one in which the number of ARP table entries can be reduced.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
14	E4	IP	60000002	0600	Because the number of pieces of the NDP entry exceeds the capacity of this system, the old entry was deleted and the new entry was added.
	An old entry was deleted and a new entry was added because the number of NDP table entries exceeded the capacity limit of the Switch. [Explanation of message variables] None. [Action] If this message is output frequently, take one of the following actions: 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 one in which the number of NDP table entries can be reduced.				
15	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 the Switch is unavailable. You cannot use an unavailable IPv6 address until you change or delete the setting, and then specify it again. 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 a duplicated address was detected *<mac address>*: MAC address of a device for which a duplicated address was detected [Action] 1. If *<ipv6 address>* set in the Switch is incorrect, change *<ipv6 address>* of the Switch. 2. If *<ipv6 address>* of the other device in which a duplicated address was detected is incorrect, correct *<ipv6 address>* of that device. Next, delete *<ipv6 address>* in the Switch and then set it again. 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.				
16	E4	IP	60000004	0600	Because the number of pieces of the NDP entry exceeds the capacity of *<vrf>*, the old entry was deleted and the new entry was added.
	An old entry was deleted and a new entry was added because the number of NDP table entries in the *<vrf>* exceeded the upper limit for each VRF. [Explanation of message variables] *<vrf>*: VRF that exceeded the upper limit for NDP • VRF *<vrf id>*: VRF whose VRF ID is *<vrf id>* • global network: Global network [Action] 1. If this message is output frequently, take one of the following actions: 2. Delete unnecessary information from the ndp configuration. 3. If unnecessary entries have been generated dynamically, delete them by executing the clear ipv6 neighbors command. 4. Review the network system configuration, and change it to one in which the number of NDP table entries can be reduced.				

3.3.2 Event location = VLAN

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

Table 3-4: Switch 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 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 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 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 BPDU for topology change was received. [Explanation of message variables] *<mode>*: Spanning Tree type • `single`: Single Spanning Tree • `PVST+:VLAN` *<vlan id>*: PVST+ Spanning Tree 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 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 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 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 BPDU for topology change was received. [Explanation of message variables] *<mode>*: Spanning Tree type • `single`: Single Spanning Tree • `PVST+:VLAN` *<vlan id>*: PVST+ Spanning Tree 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 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 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 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 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 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 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	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 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.				
20	E3	VLAN	20110043	0700	STP (*<mode>*) : Topology change detected - Topology Change Notification BPDU received on the port(VLID:*<link id>*).
	A BPDU for topology change was received. [Explanation of message variables] *<mode>*: Spanning Tree type • `single`: Single Spanning Tree • `PVST+:VLAN` *<vlan id>*: PVST+ Spanning Tree 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.				
21	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 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
22	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 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.					
23	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.					
24	E3	VLAN	21100001	0700	IGMP snooping: IGMP querier changed on VLAN *<vlan id>* - lost IGMP querier address *<ipv4 address>*.
	The IGMP querier information was deleted because an advertisement (`IGMP Query`) from the IGMP querier at *<ipv4 address>* on VLAN (*<vlan id>*) disappeared. IPv4 multicast data forwarding will not be properly executed because the availability of the IPv4 multicast group member (recipient host) cannot be checked. [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 IGMP 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.					
25	E3	VLAN	21100002	0700	IGMP snooping: IGMP querier changed on VLAN *<vlan id>* - new IGMP querier address *<ipv4 address>*.
	The IGMP querier was changed to *<ipv4 address>* because a new IGMP querier was identified on the VLAN (*<vlan id>*). [Explanation of message variables] *<vlan id>*: VLAN ID *<ipv4 address>*: IPv4 address [Action] None.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
26	E3	VLAN	21100003	0700	IGMP snooping: IPv4 address not defined on VLAN *<vlan id>*,IGMP querier function stopped.
	The IGMP querier on the VLAN (*<vlan id>*) stopped because the IPv4 address is not set. [Explanation of message variables] *<vlan id>*: VLAN ID [Action] 1. Set an IPv4 address for the appropriate VLAN. 2. Execute the `show igmp-snooping` command to check that the IPv4 address set for the appropriate VLAN is displayed.				
27	E3	VLAN	21100004	0700	IGMP snooping:The number of the IGMP snooping entry exceeded the capacity of this system.
	The number of learned entries used in `IGMP snooping` exceeds the capacity limit of the switch. [Explanation of message variables] None. [Action] Check whether the number of learned entries used in `IGMP snooping` has reached the capacity limit of the switch. For details about capacity limit, see *IGMP snooping/MLD snooping* for each model in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*. If the capacity limit has been reached, review the system configuration for ways to reduce the number of entries.				
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 at *<ipv6 address >*on 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 confirmed. [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.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
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 learned entries used in `MLD snooping` exceeds the capacity limit of the switch. [Explanation of message variables] None. [Action] Check whether the number of learned entries used in `MLD snooping` has reached the capacity limit of the switch. For details about capacity limit, see *IGMP snooping/MLD snooping* for each model in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*. If the capacity limit has been reached, review the system configuration for ways to reduce the number of entries.					
32	E3	VLAN	25100016	0700	The memory of the nimd is a tendency of lack.
	There is a tendency for memory in the network interface manager program to be insufficient. [Explanation of message variables] None. [Action] Do not change the configuration or network configuration until a message indicating recovery from the indicated condition has been output.					
33	E3	VLAN	25100017	0700	The memory of the nimd recovered from a tendency of lack.
	The network interface manager program has recovered from insufficient memory. [Explanation of message variables] None. [Action] None.					
34	E3	VLAN	25100018	0700	Because of the memory of the nimd is a lack, the nimd may not operate normally.
	The network interface manager program might not be operating normally because of insufficient memory. [Explanation of message variables] None. [Action] Execute the `restart vlan` command to restart the network interface manager program.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
35	E3	VLAN	2510001b	0700	Sum of number of VLAN on ports exceeded capacity..
	The total number of VLANs for each port exceeded the capacity limit of the switch. [Explanation of message variables] None. [Action] Execute any of the following measures: • Use the `copy` command to apply a configuration file with the total number of VLANs for each port within the capacity limit, to the running configuration file. • Change the total number of VLANs to a number within the capacity limit, and execute the `restart vlan` command. • Change the total number of VLANs to a number within the capacity limit, and restart the switch.				
36	E4	VLAN	20110008	0700	STP(*<mode>*): Port status becomes Forwarding on the port(*<nif no.>*/*<port no.>*).
	A port changed to the forwarding status. [Explanation of message variables] *<mode>*: Spanning Tree type • `single`: Single Spanning Tree • `PVST+:VLAN` *<vlan id>*: PVST+ Spanning Tree 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.				
37	E4	VLAN	20110009	0700	STP(*<mode>*): Port status becomes Blocking on the port(*<nif no.>*/*<port no.>*).
	A port changed to the blocking status. [Explanation of message variables] *<mode>*: Spanning Tree type • `single`: Single Spanning Tree • `PVST+:VLAN` *<vlan id>*: PVST+ Spanning Tree 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.				
38	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 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
39	E4	VLAN	20110015	0700	STP (*<mode>*) : Port status becomes Forwarding on the port(ChGr:*<channel group number>*).
	A port changed to the forwarding status. [Explanation of message variables] *<mode>*: Spanning Tree type • `single`: Single Spanning Tree • `PVST+:VLAN` *<vlan id>*: PVST+ Spanning Tree 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.					
40	E4	VLAN	20110016	0700	STP (*<mode>*) : Port status becomes Blocking on the port(ChGr:*<channel group number>*).
	A port changed to the blocking status. [Explanation of message variables] *<mode>*: Spanning Tree type • `single`: Single Spanning Tree • `PVST+:VLAN` *<vlan id>*: PVST+ Spanning Tree 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.					
41	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 and VLAN ID • `MST`: Multiple Spanning Tree *<channel group number>*: Channel group number [Action] Check the line status.					
42	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. No more trees can be added. [Explanation of message variables] None. [Action] Either review the network configuration, or use a Single Spanning Tree or a Multiple Spanning Tree.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
43	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 route-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 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 partner switch.				
44	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 route-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 and VLAN ID • `CIST`: Multiple Spanning Tree (CIST) • `MST Instance` *<mst instance id>*: Multiple Spanning Tree (MSTI) and MST instance ID *<channel group number>*: Channel group number [Action] Check the settings of the partner switch.				
45	E4	VLAN	20110047	0700	STP (*<mode>*) : Port status becomes Forwarding on the port(VLID:*<link id>*).
	A port changed to the forwarding status. [Explanation of message variables] *<mode>*: Spanning Tree type • `single`: Single Spanning Tree • `PVST+:VLAN` *<vlan id>*: PVST+ Spanning Tree 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.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
46	E4	VLAN	20110048	0700	STP (*<mode>*) : Port status becomes Blocking on the port(VLID:*<link id>*).
	A port changed to the blocking status. [Explanation of message variables] *<mode>*: Spanning Tree type • `single`: Single Spanning Tree • `PVST+:VLAN` *<vlan id>*: PVST+ Spanning Tree 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.				
47	E4	VLAN	21100005	0700	The IGMP snooping entry can't be registered at hardware tables.
	An `IGMP snooping` entry could not be registered in a MAC address table. [Explanation of message variables] None. [Action] Check whether the total usage of the MAC address table has reached the capacity limit of the switch. You can use the `show system` command to check MAC address table usage. If the capacity limit has been reached, see the description in *MAC address table* for each model in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the system configuration.				
48	E4	VLAN	21200005	0700	The MLD snooping entry can't be registered at hardware tables.
	An `MLD snooping` entry could not be registered in a MAC address table. [Explanation of message variables] None. [Action] Check whether the total usage of the MAC address table has reached the capacity limit of the switch. You can use the `show system` command to check MAC address table usage. If the capacity limit has been reached, see the description in *MAC address table* for each model in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the system configuration.				
49	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.				
50	E4	VLAN	25100002	0700	VLAN (*<vlan id>*) Status is Down.
	The VLAN status is DOWN. [Explanation of message variables] *<vlan id>*: VLAN ID [Action] Check the status of lines that belong to the VLAN.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
51	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.				
52	E4	VLAN	25100012	0700	The number of learning MAC addresses exceeded the configured number on the port(*<nif no.>/<port no.>*).
	The MAC address learning count exceeded the limit value in the configuration. [Explanation of message variables] *<nif no.>/<port no.>*: NIF number/port number [Action] None.				
53	E4	VLAN	25100013	0700	The number of learning MAC addresses exceeded the configured number on the Channel Group (ChGr:*<channel group number>*).
	The MAC address learning count exceeded the limit value in the configuration. [Explanation of message variables] *<channel group number>*: Channel group number [Action] None.				
54	E4	VLAN	25100014	0700	The number of learning MAC addresses exceeded the configured number on the VLAN(*<vlan id>*).
	The MAC address learning count exceeded the limit value in the configuration. [Explanation of message variables] *<vlan id>*: VLAN ID [Action] None.				
55	E4	VLAN	25100015	0700	MAC address table entries exceeded capacity.
	The number of MAC address table entries exceeded the capacity limit of the switch. [Explanation of message variables] None. [Action] Check whether the total usage of the MAC address table has reached the capacity limit of the switch. You can use the `show system` command to check MAC address table usage. If the capacity limit has been reached, see the description in *MAC address table* for each model in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the system configuration.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
56	E4	VLAN	25100019	0700	The vlan mapping entry can't be registered at VLAN classification table (VLAN *<vlan id>*, port(*<nif no.>*/ *<port no.>*)).
	The tag translation entry could not be registered in the VLAN identification table. [Explanation of message variables] *<vlan id>*: VLAN ID *<nif no.>*/*<port no.>*: NIF number/port number [Action] Delete the tag translation entry that could not be registered and unnecessary entries in the VLAN identification table, and then register the tag translation entry again. For details about the capacity limit for the VLAN identification table, see *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*.					
57	E4	VLAN	2510001a	0700	The protocol based VLAN can't be registered at VLAN classification table (VLAN *<vlan id>*, port(*<nif no.>*/ *<port no.>*)).
	The protocol VLAN entry could not be registered in the VLAN identification table during configuration of the protocol VLAN on the protocol port. [Explanation of message variables] *<vlan id>*: VLAN ID *<nif no.>*/*<port no.>*: NIF number/port number [Action] Delete the protocol VLAN entry that could not be registered and unnecessary entries in the VLAN identification table, and then register the protocol VLAN entry again. For details about the capacity limit for the VLAN identification table, see *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*.					
58	E4	VLAN	2510001b	0700	Sum of number of VLAN on ports exceeded capacity.
	The total number of VLANs for each port exceeded the capacity limit of the switch. [Explanation of message variables] None. [Action] Execute any of the following measures: 1. Use the `copy` command to apply a configuration file with the total number of VLANs for each port within the capacity limit, to the `running-config` file. 2. Change the total number of VLANs to a number within the capacity limit, and execute the `restart vlan` command. 3. Change the total number of VLANs to a number within the capacity limit, and restart the switch.					
59	E4	VLAN	2510001c	0700	MAC address table entries was beyond 80 percent of capacity.
	The number of MAC address table entries exceeded 80% of the capacity limit of the switch. [Explanation of message variables] None. [Action] Note that the usage of MAC address table entries exceeded 80% of the capacity limit. Use the entries in a way that does not exceed the capacity limit.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
60	E4	VLAN	2510001e	0700	VLAN classification table entries was beyond 80 percent of capacity.
	The number of VLAN identification table entries exceeded 80% of the capacity limit of the switch. [Explanation of message variables] None. [Action] Make sure that the number of VLAN identification table entries is within the capacity limit. For details about the capacity limit for the VLAN identification table, see *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*.				
61	E4	VLAN	2510001f	0700	The static MAC address entry can't be registered at MAC address table. (VLAN *<vlan id>*, mac *<mac>*)
	The static MAC address could not be registered in the MAC address table. [Explanation of message variables] *<vlan id>*: VLAN ID *<mac>*: MAC address [Action] Check whether the total usage of the MAC address table has reached the capacity limit of the switch. You can use the `show system` command to check MAC address table usage. If the capacity limit has been reached, see the description in *MAC address table* for each model in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the system configuration.				
62	E4	VLAN	25100020	0700	The no MAC address table learning entry can't be registered at MAC address table. (VLAN *<vlan id>*)
	The entry required for the MAC address learning suppression function could not be registered in the MAC address table. [Explanation of message variables] *<vlan id>*: VLAN ID [Action] Check whether the total usage of the MAC address table has reached the capacity limit of the switch. You can use the `show system` command to check MAC address table usage. If the capacity limit has been reached, see the description in *MAC address table* for each model in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the system configuration.				
63	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] See *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7* and review the system configuration.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
64	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.					
65	E4	VLAN	25100023	0700	The vlan mapping entry can't be registered at VLAN classification table (VLAN *<vlan id>*, Channel Group *<channel group number>*).
	The tag translation entry could not be registered in the VLAN identification table. [Explanation of message variables] *<vlan id>*: VLAN ID *<channel group number>*: Channel group number [Action] Delete the tag translation entry that could not be registered and unnecessary entries in the VLAN identification table, and then register the tag translation entry again. For details about the capacity limit for the VLAN identification table, see *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*.					
66	E4	VLAN	25100024	0700	The protocol based VLAN entry can't be registered at VLAN classification table (VLAN *<vlan id>*, Channel Group*<channel group number>*).
	The protocol VLAN entry could not be registered in the VLAN identification table during configuration of the protocol VLAN on the protocol port for link aggregation. [Explanation of message variables] *<vlan id>*: VLAN ID *<channel group number>*: Channel group number [Action] Delete the protocol VLAN entry that could not be registered and unnecessary entries in the VLAN identification table, and then register the protocol VLAN entry again. For details about the capacity limit for the VLAN identification table, see *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*.					
67	E4	VLAN	25100025	0700	The protocol based VLAN entry can't be registered at VLAN classification table (protocol *<frame type>*,VLAN *<vlan id>*).
	The protocol VLAN entry could not be registered in the VLAN identification table when the protocol was added to the protocol VLAN. [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 *<vlan id>*: VLAN ID [Action] Delete the protocol VLAN entry that could not be registered and unnecessary entries in the VLAN identification table, and then register the protocol VLAN entry again. For details about the capacity limit for the VLAN identification table, see *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
68	E4	VLAN	25100026	0700	The protocol based VLAN entry can't be registered at VLAN classification table (protocol *\<frame type\>*,Vlan-Protocol *\<protocol name\>*).
	The protocol VLAN entry could not be registered in the VLAN identification table when the protocol value was added to the protocol for the protocol VLAN. [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] Delete the protocol VLAN entry that could not be registered and unnecessary entries in the VLAN identification table, and then register the protocol VLAN entry again. For details about the capacity limit for the VLAN identification table, see *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*.				

3.3.3 Event location = VLAN (Ring Protocol)

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

Table 3-5: Switch 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.				
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.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
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 only the MAC address table for the data transfer VLAN group in a ring whose output destination is a ring port was cleared. [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 was detected on the transit node and the MAC address table was cleared. [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 frame was received with `Ring Protocol`, and MAC address table entries were cleared. The switch outputs this message when the MAC address table entries learned on all ring ports were cleared. [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 switch-back. 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 `preempt-delay` configuration command, or manually remove the path switch-back suppression state with the `clear axrp preempt-delay` command.				
7	E3	VLAN	20170017	0700	AXRP *<ring id>* : canceled the suspension of the fault recovery process.
	Removal of `Ring Protocol` path switch-back suppression was executed. The switch outputs this message when the path switch-back suppression state is removed during such suppression at the master node. [Explanation of message variables] *<ring id>*: Ring ID [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
8	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.				
9	E4	VLAN	20170006	0700	AXRP *<ring id>* : The MAC address entry can't be registered at hardware tables.
	The MAC address used for the Ring Protocol could not be registered in the MAC address table. [Explanation of message variables] *<ring id>*: Ring ID [Action] 1. Make sure that the VLAN used for the control VLAN has been configured. If the VLAN has not been configured, configure it. After the VLAN has been configured, disable the Ring Protocol, and then enable it again by using the `no disable` command. 2. Check whether the total usage of the MAC address table has reached the capacity limit of the switch. You can use the `show system` command to check MAC address table usage. If the capacity limit has been reached, see the description in *MAC address table* for each model in *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*, and review the system configuration.				

3.3.4 Event location = VLAN (GSRP)

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

Table 3-6: Switch 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 has been completed, `backup-lock` in the GSRP configuration is deleted, or the `restart vlan` command is executed while the GSRP is in the Master state and has not identified the partner 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
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.					
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 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	
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 of 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 was 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] Make sure that the direct link port is correctly installed and is operating normally. Also check the current GSRP state in the configuration, and by using the operation command.					
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 is 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.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
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 status 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.				
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] Make sure that the direct link port is correctly installed and is operating normally. Also check the current GSRP state in the configuration, and by using 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 was 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] Make sure that the direct link port is correctly installed and is operating normally. Also check the current GSRP state in the configuration, and by using the operation command.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
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 device transitioned to Backup because the GSRP state of the switch and neighboring device are both Master. [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 state in the configuration, and by using 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 expiration 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 switch failure and event information when the event location is VLAN (L2 loop detection).

Table 3-7: Switch 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.>*).
	A port was 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>*).
	A port was 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.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
3	E4	VLAN	20800003	0700	L2LD : ChGr(*<channel group number>*) inactivated because of loop detection from port(*<nif no.>*/*<port no.>*).
	A port was 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>*).
	A port was 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.					
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.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
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 exceeds 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 switch failure and event information when the event location is VLAN (CFM).

Table 3-8: Switch 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.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
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.					
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.					

3.3.7 Event location = MAC

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

Table 3-9: Switch 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.				
3	E3	MAC	20120007	0800	Port(*<nif no.>*/*<port no.>*) detached from Channel Group(*<channel group number>*) - Different Partner System ID is detected.
	The port was detached from the channel group because the system ID of a partner switch does not match between the ports for LACP mode link aggregation. [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 port was detached from the channel group because the key of a partner switch does not match between the ports for LACP mode link aggregation. [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.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
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.					
7	E3	MAC	20120011	0800	Port(*<nif no.>*/*<port no.>*) detached from Channel Group(*<channel group number>*) - Different Port data rate.
	The channel group contains lines that have different data rates (speeds), and those that have low data rates have been 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 timed out, so 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, which is active.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
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.				
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 port was detached from the channel group because the aggregation bit of the partner switch in the LACP mode was false. [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 was detached from the channel group because the port number of the partner switch was changed. [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 was detached from the channel group because the port priority value of the partner switch was changed. [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
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.				
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 stopped. [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
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.				
22	E4	MAC	20120003	0800	Channel Group(*<channel group number>*) is Down - All port detached.
	All ports in the channel group have been 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 exceeded 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 switch failure and event information when the event location is SOFTWARE.

Table 3-10: Switch 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 switch was restarted because the RESET switch was pressed. [Explanation of message variables] None. [Action] None.				
2	E3	SOFTWARE	00003002	1000	System restarted due to default reset operation.
	The switch 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 switch was restarted because the reload command was executed. [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 a WDT (watchdog timer) timed out. [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 switch 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 switch was restarted because of a hardware failure. [Explanation of message variables] None. [Action] Replace the switch.				
9	E3	SOFTWARE	0000300a	1000	System restarted due to auto restart detected by software.
	The switch was restarted because of an automatic restart by the software. [Explanation of message variables] None. [Action] None.				
10	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. If there are many accesses from network management devices, suppress all but the most essential ones. 3. If (2.) above does not start the recovery, see the *Troubleshooting Guide* description about when congestion of packets being processed by the CPU does not recover, and carry out the indicated action. 4. This message might be output when a lot of ping or other commands that send and receive packets are executed.				
11	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
12	E3	SOFTWARE	00008601	1001	NTP lost synchronization with *<ip address>*[on VRF *<vrf id>*].
	Synchronization was lost with the NTP server at *<ip address>*. [Explanation of message variables] *<ip address>*: IPv4 address of the NTP server *<vrf id>*: VRF ID [Action] Use the `show ntp associations` command to check the NTP status. If the non-synchronized state continues, check the NTP configuration, NTP server operation status, and availability of communication.				
13	E3	SOFTWARE	00008602	1001	NTP detected an invalid packet from *<ip address>*[on VRF *<vrf id>*].
	An invalid packet from the NTP server at *<ip address>* was detected. [Explanation of message variables] *<ip address>*: IPv4 address of the NTP server *<vrf id>*: VRF ID [Action] Check the NTP server.				
14	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.				
15	E3	SOFTWARE	01200123	1001	VRF information defined by the configuration file is ignored, since VRF function license is not given.
	VRF information set in the startup configuration file is invalid because a license was not granted. [Explanation of message variables] None. [Action] If you want to enable the VRF function, set the option license OP-DPAR with the `set license` command, and restart the switch.				
16	E3	SOFTWARE	01200187	1001	The temperature logging file can't be written.
	The writing of temperature logging information failed. [Explanation of message variables] None. [Action] 1. Check the user space of the internal flash memory. 2. If there is not enough free space, delete any unneccessary files to acquire more free space (about 8 KB is required).				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
17	E3	SOFTWARE	01300462	1001	There is mismatch between active and standby software version.
	The software versions of the active system and the standby system are different. [Explanation of message variables] None. [Action] 1. There is no problem if the software is being updated. 2. In all other cases, update the software so that the versions on both the active and the standby systems are the same. For details about how to update the software, see the *Software Installation Guide*.					
18	E3	SOFTWARE	01300463	1001	Active and standby software version is identical.
	The software versions of the active system and the standby system are the same. [Explanation of message variables] None. [Action] None.					
19	E3	SOFTWARE	01300464	1001	There is mismatch between active and standby license key.
	The license key information for the active system and the standby system is not the same. [Explanation of message variables] None. [Action] 1. Execute the synchronize command in the active system to synchronize the license key information of the standby system with that of the active system. 2. After the synchronize command terminates, execute the reload command with the standby parameter specified in the active system to restart the standby system.					
20	E3	SOFTWARE	01300465	1001	Active and standby license key is identical.
	The license key information in the active and the standby systems matches. [Explanation of message variables] None. [Action] None.					
21	E3	SOFTWARE	01700501	1001	Statistics table initialized.
	The statistics table that holds the CPU usage statistics has been initialized because the switch time has been changed. [Explanation of message variables] None. [Action] None.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
22	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 the command or retrieve the MIB.				
23	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 the command or retrieve the MIB.				
24	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.				
25	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.				
26	E3	SOFTWARE	01910202	1001	System restarted by user operation.
	The system was restarted by a user operation. [Explanation of message variables] None. [Action] None.				
27	E3	SOFTWARE	01910203	1001	System restarted after hardware reset.
	The system was restarted by the reset switch. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
28	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 logged-in users and `admin` users.				
29	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 *MIB Reference For Version 11.7*, and make sure that the set MIB has read and write attributes.				
30	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.				
31	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 about the MIB value range, see *24. SNMP* in the manual *Configuration Command Reference Vol. 2 For Version 11.7*.				
32	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 about the number of characters that can be set for a MIB value, see *24. SNMP* in the manual *Configuration Command Reference Vol. 2 For Version 11.7*.				
33	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 *MIB Reference For Version 11.7*, and check that items required for setting are sufficient.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
34	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 11.7*, and set up the MIB.					
35	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.					
36	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.					
37	E3	SOFTWARE	02002020	1001	MIB value has failed to establish. Errors occurred in the "config" command.
	The MIB could not be set because an error occurred while editing the configuration at MIB setup. [Explanation of message variables] None. [Action] For details about configuration errors, see *Error Messages Displayed When Editing the Configuration* in the *Configuration Command Reference*.					
38	E3	SOFTWARE	02002021	1001	Not all MIB configured.
	Only some of the MIB values were set because MIB setup failed. [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.					
39	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).					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
40	E3	SOFTWARE	02002024	1001	*<object name>* set as *<mib value>* at the request of *<ip address>* [on VRF *<vrf id>*].
	<object name> was set to *<mib value>* because of a request from *<ip address>*. [Explanation of message variables] *<object name>*: MIB object mnemonic *<mib value>*: MIB value *<ip address>*: IPv4 address or IPv6 address of the SNMP manager *<vrf id>*: VRF ID [Action] None.					
41	E3	SOFTWARE	02002025	1001	SNMP: MAC address table entry cleared at the request of *<ip address>* [on VRF *<vrf id>*].
	The MAC address table was cleared due to a MAC address table clear request from the SNMP manager at *<ip address>*. [Explanation of message variables] *<ip address>*: IPv4 address or IPv6 address of the SNMP manager *<vrf id>*: VRF ID [Action] None.					
42	E3	SOFTWARE	05001002	1001	BGP information defined by the configuration file is ignored, since BGP function license is not given.
	The BGP4 or BGP4+ information set in the startup configuration is invalid because a license has not been granted. [Explanation of message variables] None. [Action] If you want to use the BGP4 or BGP4+ functionality, install the option license OP-BGP with the `set license` command, and restart the switch.					
43	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.					
44	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.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
			Description		
45	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 already been used 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.				
46	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 and authentication key setting of the Switch and the settings on the DNS server. If you are using an authentication key, make sure that the time information for the Switch matches the time information for the DNS server.				
47	E3	SOFTWARE	0d10b0e4	1001	dhcp_server: Invalid network address.
	The DHCP server detected an invalid configuration. An invalid network address has been specified. [Explanation of message variables] None. [Action] Delete the previously entered setting, and set the correct network address.				
48	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 set the correct key.				
49	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 has been specified. [Explanation of message variables] None. [Action] Delete the previously entered setting, and set the correct exclusion address range.				
50	E3	SOFTWARE	0e008001	1000	Virtual router *<vrid>* of *<interface name>* state has transitioned to *<state>*.
	The active state of the virtual router changed to *<state>*. [Explanation of message variables] *<vrid>*: Virtual router ID *<interface name>*: Name of the interface in which VRRP is set *<state>*: Virtual router state [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
51	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 the interface in which VRRP is set [Action] Check the partner switch that makes up the same virtual router.				
52	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 the interface in which VRRP is set [Action] Check the partner switch that makes up the same virtual router.				
53	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 the interface in which VRRP is set [Action] Check the password settings of the Switch and the partner switch that make up the same virtual router.				
54	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 the interface in which VRRP is set [Action] Check the IP address settings of the virtual router for the Switch and the partner switch that make up the same virtual router.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
55	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 the interface in which VRRP is set [Action] Check the transmission interval settings for the Switch and the partner switch that make up the same virtual router.					
56	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 a virtual router with the Switch, specify the same VRRP version for both the partner switch and the Switch.					
57	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 the interface in which VRRP is set *<priority>*: Virtual router priority [Action] None.					
58	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 the interface in which VRRP is set [Action] None.					
59	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 the interface in which VRRP is set [Action] Check the partner switch that makes up the same virtual router.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
60	E3	SOFTWARE	0e008016	1000	Virtual router *<vrid>* of *<interface name>* priority changed to *<priority>*, because error detected on line by vrrp-polling.
	The VRRP priority was changed to *<priority>* because VRRP polling detected a line fault. [Explanation of message variables] *<vrid>*: Virtual router ID *<interface name>*: Name of the interface in which VRRP is set *<priority>*: Virtual router priority [Action] If switching occurs frequently, adjusting the configuration might solve the problem.					
61	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 an error. [Explanation of message variables] *<interface name>*: Name of the interface in which VRRP is set *<vrid>*: Virtual router ID [Action] If switching occurs frequently, adjusting the configuration might solve the problem.					
62	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 the interface in which VRRP is set *<vrid>*: Virtual router ID [Action] None.					
63	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.					
64	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
65	E3	SOFTWARE	0e008022	1000	Virtual router *<VRID>* of *<Interface Name>* advertisement interval set default advertisement interval (1 second) because not supported Advertisement interval configured.
	An unsupported value is specified for the interval for sending ADVERTISEMENT packets. The default value is used for `Advertisement Interval`. [Explanation of message variables] *<VRID>*: Virtual router ID *<Interface Name>*: Interface name [Action] 1. If the VRRP operation mode is set in the configuration by using the `ietf-ipv6-spec-07-mode` or `ietf-unified-spec-02-mode` command, set the value to 40 seconds or smaller. 2. When you set a millisecond value for the advertisement packet sending interval, set the VRRP operation mode by using the `ietf-ipv6-spec-07-mode` or `ietf-unified-spec-02-mode` command.					
66	E3	SOFTWARE	0e008023	1000	Virtual router *<VRID>* of *<Interface Name>* disabled because Primary virtual router is not running.
	The follow virtual router is disabled because no primary virtual router is configured. [Explanation of message variables] *<VRID>*: Virtual router ID *<Interface Name>*: Interface name [Action] Configure a primary virtual router.					
67	E3	SOFTWARE	0e008024	1000	Virtual router *<VRID>* of *<Interface Name>* enabled because Primary virtual router started.
	The follow virtual router was enabled because a primary virtual router was configured. [Explanation of message variables] *<VRID>*: Virtual router ID *<Interface Name>*: Interface name [Action] None.					
68	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`: 10BBASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X • `tengigabitethernet`: 10GBASE-R • `port-channel`: Channel group *<interface number>*: Interface number specified as the fault-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.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
69	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`: 10BBASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X • `tengigabitethernet`: 10GBASE-R • `port-channel`: Channel group *<interface number>*: Interface number specified as the fault-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.					
70	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 as the fault-monitoring interface • *<nif no.>*/*<port no.>*: NIF number/port number [Action] None.					
71	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.					
72	E3	SOFTWARE	0f406004	1001	IPv4 multicast routing entry had exceeded maximum value *<number>* for limit, entry has discarded[on VRF *<vrf id>*].
	An entry was discarded because the number of IPv4 multicast routing information items exceeded the maximum value of *<number>*. [Explanation of message variables] *<number>*: Maximum number of IPv4 multicast routing information items *<vrf id>*: VRF ID [Action] An unauthorized access might have occurred. • Check if more than the expected number of additional requests for multicast routing information were generated. The number of multicast routing information items exceeds the maximum value that they are limited to. • Check the configuration (`ip pim mroute-limit` command). • After checking the network configuration, reexamine the Switch configuration.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
73	E3	SOFTWARE	0f406005	1001	IPv4 multicast routing entry has recovered from the state of discard[on VRF *<vrf id>*].
	The IPv4 multicast routing information has recovered from a state in which entries were discarded. [Explanation of message variables] *<vrf id>*: VRF ID [Action] None.				
74	E3	SOFTWARE	0f406006	1001	IGMP source-limit *<number>* has been exceeded on interface *<interface name>* [of VRF *<vrf id>*] 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>*: Limit on the number of IGMP groups *<interface name>*: Interface name *<vrf id>*: VRF ID [Action] An unauthorized access might have occurred. • Check if more than the expected number of additional requests were generated for sources belonging to the IGMP group. • Check the configuration (`ip igmp source-limit` command). • After checking the network configuration, reexamine the Switch configuration.				
75	E3	SOFTWARE	0f406007	1001	IGMP source-limit on requests on interface *<interface name>* [of VRF *<vrf id>*] has recovered from state of discard.
	The interface *<interface name>* has recovered from a state in which sources belonging to the IGMP group were discarded. [Explanation of message variables] *<interface name>*: Interface name *<vrf id>*: VRF ID [Action] None.				
76	E3	SOFTWARE	0f406008	1001	IGMP group-limit *<number>* has been exceeded on interface *<interface name>* [of VRF *<vrf id>*] due to over-request. Request have been discarded.
	A request was discarded because the interface *<interface name>* received a request that exceeded the IGMP group limit value of *<number>*. [Explanation of message variables] *<number>*: Limit on the number of IGMP groups *<interface name>*: Interface name *<vrf id>*: VRF ID [Action] An unauthorized access might have occurred. • Check if more than the expected number of additional requests for the IGMP group were generated. • Check the configuration (`ip igmp group-limit` command). • After checking the network configuration, reexamine the Switch configuration.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
77	E3	SOFTWARE	0f406009	1001	IGMP group-limit on requests on interface *<interface name>* [of VRF *<vrf id>*] has recovered from state of discard.
	The interface *<interface name>* has recovered from the state in which IGMP groups were discarded. [Explanation of message variables] *<interface name>*: Interface name *<vrf id>*: VRF ID [Action] None.					
78	E3	SOFTWARE	0f40600a	1001	IPv4 multicast forwarding entry had exceeded maximum value *<number>* for limit, entry has discarded[on VRF *<vrf id>*].
	An entry was discarded because the number of IPv4 multicast forwarding entries exceeded the maximum value of *<number>*. [Explanation of message variables] *<number>*: Maximum number of IPv4 multicast forwarding entries *<vrf id>*: VRF ID [Action] An unauthorized access might have occurred. • Check if more than the expected number of additional requests for a multicast forwarding entry were generated. The number of items of multicast forwarding entries exceeds the maximum value. • Check if a negative cache has been generated due to a reception of multicast packets that are not forwarded. • Check the configuration (`ip pim mcache-limit` command). • After checking the network configuration, reexamine the Switch configuration.					
79	E3	SOFTWARE	0f40600b	1001	IPv4 multicast forwarding entry has recovered from the state of discard[on VRF *<vrf id>*].
	The IPv4 multicast forwarding entries have recovered from a state in which they were discarded. [Explanation of message variables] *<vrf id>*: VRF ID [Action] None.					
80	E3	SOFTWARE	0f40600c	1001	Accept-bootstrap configuration defined by the configuration file is ignored, since accept-bootstrap license is not given.
	The `accept-bootstrap` configuration set in the startup configuration file is invalid because a license was not granted. [Explanation of message variables] None. [Action] If you want to use the functionality that suppresses the receiving of bootstrap messages, set the OP-MBSE optional license with the `set license` command, and then restart the switch.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
81	E3	SOFTWARE	11010001	1001	The list number *<policy list no.>* of the policy base routing changed to the sequence number *<sequence>*.
	A route with the priority *<sequence>* was selected in the policy-based routing information with list number *<policy list no.>*. [Explanation of message variables] *<policy list no.>*: List number of the policy-based routing information *<sequence>*: Priority of the route information in the list [Action] None.				
82	E3	SOFTWARE	11010002	1001	The list number *<policy list no.>* of the policy base routing changed to the default operation.
	The default action was selected in the policy-based routing information with list number *<policy list no.>*. [Explanation of message variables] *<policy list no.>*: List number of the policy-based routing information [Action] None.				
83	E3	SOFTWARE	11020001	1001	The list number *<policy switch list no.>* of the policy base switching changed to the sequence number *<sequence>*.
	A destination interface with the priority *<sequence>* was selected in the policy-based switching information with list number *<policy switch list no.>*. [Explanation of message variables] *<policy switch list no.>*: List number of the policy-based switching information *<sequence>*: Priority of the destination interface in the list [Action] None.				
84	E3	SOFTWARE	11020002	1001	The list number *<policy switch list no.>* of the policy base switching changed to the default operation.
	The default action was selected in the policy-based switching information with list number *<policy switch list no.>*. [Explanation of message variables] *<policy switch list no.>*: List number of the policy-based switching information [Action] None.				
85	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	
86	E3	SOFTWARE	1920a005	1001	IPv6 multicast routing entry had exceeded maximum value *<number>* for limit, entry has discarded[on VRF *<vrf id>*].
	An entry was discarded because the number of IPv6 multicast routing information items exceeded the maximum value of *<number>*. [Explanation of message variables] *<number>*: Maximum number of IPv6 multicast routing information items *<vrf id>*: VRF ID [Action] An unauthorized access might have occurred. • Check if more than the expected number of additional requests for multicast routing information were generated. The number of multicast routing information items exceeds the maximum value that they are limited to. • Check the configuration (`ipv6 pim mroute-limit` command). • After checking the network configuration, reexamine the Switch configuration.					
87	E3	SOFTWARE	1920a006	1001	IPv6 multicast routing entry has recovered from the state of discard[on VRF *<vrf id>*].
	The IPv6 multicast routing information has recovered the state in which entries were discarded. [Explanation of message variables] *<vrf id>*: VRF ID [Action] None.					
88	E3	SOFTWARE	1920a007	1001	IPv6 multicast forwarding entry had exceeded maximum value *<number>* for limit, entry has discarded[on VRF *<vrf id>*].
	An entry was discarded because the number of IPv6 multicast forwarding entries exceeded the maximum value of *<number>*. [Explanation of message variables] *<number>*: Maximum number of IPv6 multicast forwarding entries *<vrf id>*: VRF ID [Action] An unauthorized access might have occurred. • Check if more than the expected number of additional requests for a multicast forwarding entry were generated. The number of items of multicast forwarding entries exceeds the maximum value. • Check if a negative cache has been generated due to a reception of multicast packets that are not forwarded. • Check the configuration (`ipv6 pim mcache-limit` command). • After checking the network configuration, reexamine the Switch configuration.					
89	E3	SOFTWARE	1920a008	1001	IPv6 multicast forwarding entry has recovered from the state of discard[on VRF *<vrf id>*].
	The IPv6 multicast forwarding entries have recovered from a state in which they were discarded. [Explanation of message variables] *<vrf id>*: VRF ID [Action] None.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
90	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`.				
91	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.				
92	E3	SOFTWARE	25090001	1001	The change of power control mode was started.
	The change of power control mode has started. [Explanation of message variables] None. [Action] Do not remove the BSU or CSU until the log message `The change of power control mode was completed.` is displayed.				
93	E3	SOFTWARE	25090002	1001	The change of power control mode was completed.
	Changing of the power control mode has been completed. [Explanation of message variables] None. [Action] None.				
94	E3	SOFTWARE	25090003	1001	System changes to the schedule power control because it became schedule time.
	The scheduled time for power-control has been reached. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
			Description		
95	E3	SOFTWARE	25090004	1001	System changes from the schedule power control because it ended schedule time.
	The scheduled time for power-control has ended. [Explanation of message variables] None. [Action] None.				
96	E3	SOFTWARE	25090011	1001	System changes from the adaptive power control.
	The traffic-based power saving functionality will be turned off because the amount of traffic has increased or the configuration of the functionality has changed. [Explanation of message variables] None. [Action] None.				
97	E3	SOFTWARE	25090012	1001	System changes to the adaptive power control.
	The traffic-based power saving functionality will be started due to a reduction in the amount of traffic. [Explanation of message variables] None. [Action] None.				
98	E3	SOFTWARE	25090101	1001	The change of power control mode could not be started.
	Changing of the power control mode could not be started. [Explanation of message variables] None. [Action] 1. Execute the show system command to review the device configuration. If the system is not configured with a redundant BSU or CSU, the power control mode cannot be changed from normal to mode2 or vice versa even if a scheduled time has been reached. Create a redundant BSU or CSU configuration. 2. Execute the show system command to review the device configuration. If the system is not configured with a redundant BSU or CSU, even with the traffic-based power saving functionality set, the power control mode cannot be changed from normal to mode2 or vice versa for an increase or decrease in traffic. Create a redundant BSU or CSU configuration.				
99	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.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
100	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 the number of entries has exceeded the capacity of the database. [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 because a static entry has been added, delete the relevant static entry.					
101	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.					
102	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.					
103	E3	SOFTWARE	3000b046	1001	The binding database was restored from *<url>*.
	The binding database was 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.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
104	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.					
105	E4	SOFTWARE	20160002	1001	The MAC-VLAN MAC Address entry can't be registered at hardware tables.
	The MAC address that was set for the MAC VLAN by using a configuration command could not be set for the hardware. [Explanation of message variables] None. [Action] Review the capacity limit. However, setting the maximum capacity limit might not be possible due to hardware limitations.					
106	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 IEEE802.1X, could not be set in the hardware table. [Explanation of message variables] None. [Action] Review the capacity limit. However, setting the maximum capacity limit might not be possible due to hardware limitations.					
107	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 IEEE802.1X, could not be set in the hardware table. [Explanation of message variables] None. [Action] Review the capacity limit. However, setting the maximum capacity limit might not be possible due to hardware limitations.					
108	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, setting the maximum capacity limit might not be possible due to hardware limitations.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
109	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).					
110	E4	SOFTWARE	20430002	1001	The macauthd MAC address entry can't be registered at hardware tables.
	Using MAC-based 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. If the total number of MAC addresses registered in the MAC address table is too large, delete unnecessary MAC addresses.					
111	E4	SOFTWARE	20430003	1001	The macauthd MAC address entry failed in the deletion.
	Using MAC-based authentication, the MAC address of a registered terminal could not be deleted from the hardware table. [Explanation of message variables] None. [Action] Restart L2MacManager.					
112	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 the RADIUS server or TACACS+ server have been set. 2. Check the configurations to make sure that the IP address for the RADIUS server or TACACS+ server is correct. 3. Check the configurations to make sure that the port number for the RADIUS server or TACACS+ server is correct.					
113	E5	SOFTWARE	01300479	1001	There is mismatch between active and standby license key.
	The license key information for the active system and the standby system is not the same. In this state, system switching cannot be performed by using the `redundancy force-switchover` command. If system switching occurs in this state due to a fatal error, or by clicking the Reset button, by pressing the ACH switch, or by executing the `reload` command with the `active` parameter specified, the new active system will restart after the switch. [Explanation of message variables] None. [Action] 1. Execute the `synchronize` command in the active system to synchronize the license key information of the standby system with that of the active system. 2. After the `synchronize` command has terminated, execute the `reload` command with the `standby` parameter specified in the active system to restart the standby system.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
114	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 are many accesses from network management devices, suppress all but the most essential ones. 4. If the system does not recover after using any one of the three methods above, the capacity limits of the Switch might not be satisfied. See *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7* and review the network configuration.				
115	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.
	A software failure occurred during operation. [Explanation of message variables] None. [Action] Normal operation might be impossible. Execute the following measures: 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 switch. 3. If the same failure occurs again after the switch is restarted by using the `reload` command, replace the switch.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
116	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.
	A software failure occurred during operation. [Explanation of message variables] None. [Action] Normal operation might be impossible. Execute the following measures: 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 switch. 3. If the same failure occurs again after the switch is restarted by using the `reload` command, replace the switch.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
117	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.
	A software failure occurred during operation. [Explanation of message variables] None. [Action] Normal operation might be impossible. Execute the following measures: 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 switch. 3. If the same failure occurs again after the switch is restarted by using the `reload` command, replace the switch.				
118	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
119	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.				
120	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 there is not enough memory. • Blank: The program was forced to stop because of other causes. [Action] • If the cause is that there is not enough memory: The reason is that the memory area is full. Make sure that the usage is within the limit (see *3. Capacity Limit* in the manual *Configuration Guide Vol. 1 For Version 11.7*). If the usage is within the limit, carry out the actions to be taken when the cause of the forced stop is something other than lack of memory. • If the cause is something other than there not being enough 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.				
121	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.				
122	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.				
123	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		
124	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.					
125	E7	SOFTWARE	11109901	1001	policyd aborted.
	The policy-based program (`policyd`) was forced to stop. [Explanation of message variables] None. [Action] Collect the failure information (the `policyd.core` file under `/usr/var/core`), log information, and the configuration of the policy-based program. For details about how to collect this information, see the *Troubleshooting Guide*. The policy-based program will automatically restart. If it does not automatically restart or if it restarts frequently, restart the switch.					
126	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.					
127	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.					
128	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
129	E7	SOFTWARE	1f01b021	1001	dhcp6_relay aborted.
	The IPv6 DHCP relay program (dhcp6_relay) was forced to stop. The IPv6 DHCP relay aborted the operation and forced the program to stop because the IPv6 DHCP relay detected an anomaly such as a lack of memory. [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.					
130	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.					
131	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.					
132	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.					
133	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.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
134	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.				
135	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.				
136	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.				
137	E7	SOFTWARE	20400001	1001	dot1xd aborted
	The IEEE802.1X program (dot1xd) was forced to stop. [Explanation of message variables] None. [Action] The IEEE802.1X program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.				
138	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.				
139	E7	SOFTWARE	20430001	1001	macauthd aborted.
	The MAC-based authentication program was forced to stop. [Explanation of message variables] None. [Action] The MAC-based authentication 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
140	E7	SOFTWARE	20700001	1001	efmoamd aborted.
	The IEEE802.3ah/OAM program (efmoamd) was forced to stop. [Explanation of message variables] None. [Action] The IEEE802.3ah/OAM program should restart automatically. If it does not restart if restarts occur frequently, restart the switch.					
141	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.					
142	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.					
143	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 (snoopd) should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.					
144	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.					
145	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	
146	E7	SOFTWARE	27000011	0000	System accounting temporary stopped because accounting event congestion detected.

	Accounting of the login and logout commands was stopped temporarily because accounting event transmission is congested.
	[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					

147	E7	SOFTWARE	2a001000	1001	httpd aborted.
	The HTTP program (`httpd`) was forced to stop. [Explanation of message variables] None. [Action] The HTTP program will automatically restart. If it does not automatically restart or if restarts frequently, restart the switch.					
148	E7	SOFTWARE	2d000001	1001	acllogd aborted.
	The access list logging program (acllogd) was forced to stop. [Explanation of message variables] None. [Action] Obtain the error save information (`acllogd.core` file under `/usr/var/core`) of the access list logging program. For details about how to collect the information, see the *Troubleshooting Guide*. The access list logging program should restart automatically. If it does not restart or if restarts occur frequently, restart the switch.					
149	E7	SOFTWARE	3000b041	1001	dhcp_snoopingd aborted.
	The DHCP snooping program (dhcp_snoopingd) was forced to stop. DHCP snooping aborted the operation and forced the program to stop because DHCP snooping detected an anomaly such as a lack of memory. [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.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
Description					
150	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 will automatically restart. If it does not automatically restart or if restarts frequently, restart the switch.					
151	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	
152	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.				
153	E9	SOFTWARE	25040d05	1001	System restarted due to software failure occurred during operation.
	An error occurred with the software during operation, and the switch restarted. [Explanation of message variables] None. [Action] Check the log by executing the show logging command. If some other problem is indicated in the log, take appropriate action according to the error message.				
154	R5	SOFTWARE	01300479	1001	Active and standby license key is identical.
	The license key information in the active and the standby systems matches. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
155	R7	SOFTWARE	00003101	1000	Recovered from memory exhaustion.
	The CPU has recovered from a lack of memory. [Explanation of message variables] None. [Action] None.				
156	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.				
157	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.				
158	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.				
159	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.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
160	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.				
161	R7	SOFTWARE	0e008014	1000	vrrpd restarted.
	The VRRP program (vrrp) has restarted. The switch outputs this message when the VRRP program restarts automatically. [Explanation of message variables] None. [Action] None.				
162	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.				
163	R7	SOFTWARE	11109901	1001	policyd restarted.
	The policy-based program (`policyd`) has restarted. The switch outputs this message when the policy-based program automatically restarts or a restart is requested by the `restart policy` command. [Explanation of message variables] None. [Action] None.				
164	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.				
165	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.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
166	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.				
167	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.				
168	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.				
169	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.				
170	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.				
171	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.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
172	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.				
173	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.				
174	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.				
175	R7	SOFTWARE	20400001	1001	dot1xd restarted.
	The IEEE802.1X program (dot1xd) has restarted. The switch outputs this message when the IEEE802.1X program restarts automatically or a restart is requested by the `restart dot1x` command. [Explanation of message variables] None. [Action] None.				
176	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.				
177	R7	SOFTWARE	20430001	1001	macauthd restarted.
	The MAC-based authentication program has restarted. The switch outputs this message when the MAC-based 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.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
178	R7	SOFTWARE	20700001	1001	efmoamd restarted.
	The IEEE802.3ah/OAM program (efmoamd) has restarted. The switch outputs this message when the IEEE802.3ah/OAM program restarts automatically or a restart is requested by the `restart efmoam` command. [Explanation of message variables] None. [Action] None.				
179	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.				
180	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.				
181	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.				
182	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.				
183	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.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
184	R7	SOFTWARE	27000011	0000	System accounting recovered from congestion.
	Accounting of login and logout commands resumed because the accounting event transmission has recovered from congestion. [Explanation of message variables] None. [Action] None.				
185	R7	SOFTWARE	2a001000	1001	httpd restarted.
	The HTTP program (httpd) restarted. The switch outputs this message when the HTTP program automatically restarts or a restart is requested by the restart web-authentication command. [Explanation of message variables] None. [Action] None.				
186	R7	SOFTWARE	2d000001	1001	acllogd restarted.
	The access list logging program (acllogd) has restarted. The switch outputs this message when the access list logging program restarts automatically or a restart is requested by the restart access-log command. [Explanation of message variables] None. [Action] None.				
187	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.				
188	R7	SOFTWARE	32001001	1001	trackobjd restarted.
	The track object program (trackobjd) restarted. The switch outputs this message when the track object program automatically restarts. [Explanation of message variables] None. [Action] None.				

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

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

Table 3-11: Authentication VLAN 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	20410002	1001	vaad connection closed<*ipv4 address*>.
	The VAA and the authentication server <*ipv4 address*> were 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 the 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 the authentication server [Action] None.				
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 any version 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.				
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.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
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	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 function, and then set the VAA configuration again.					
9	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 function, and then set the VAA configuration again.					
10	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 function, and then set the VAA configuration again.					
11	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.					
12	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.					

3.4.3 Event location = BSU [AX6700S]

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

Table 3-12: Switch failure and event information when the event location is BSU

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
1	E3	BSU	01200174	1681	Failed in accumulated running time access to BSU.
	Access to the total operating time for the BSU failed. [Explanation of message variables] None. [Action] There are no effects on communication and normal operation. However, the functionality for managing the total operating time cannot be used. If you want to use this functionality, replace the BSU.				
2	E3	BSU	23000162	1681	BSU inactivated because of SOP operation.
	The BSU was placed in the inactive state in response to an `inactivate` instruction from the system operation panel. [Explanation of message variables] None. [Action] None.				
3	E3	BSU	23000166	1681	BSU activated because of SOP operation.
	The BSU was released from the inactive state in response to an `activate` instruction from the system operation panel. [Explanation of message variables] None. [Action] None.				
4	E3	BSU	25070000	1681	BSU enabled administratively.
	The BSU was released from the disabled state by using the `power enable` configuration command. [Explanation of message variables] None. [Action] None.				
5	E3	BSU	25070001	1681	BSU board connected.
	Insertion of a BSU board was detected. [Explanation of message variables] None. [Action] None.				
6	E3	BSU	25070003	1681	BSU activated administratively.
	The BSU was released from the inactive state by using the `activate` command. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
7	E3	BSU	25070100	1681	BSU disabled administratively.
	The BSU was disabled by configuring `no power enable` with a configuration command. [Explanation of message variables] None. [Action] None.				
8	E3	BSU	25070101	1681	BSU board notconnected.
	Removal of a BSU board was detected. [Explanation of message variables] None. [Action] The BSU board might not be inserted or might not be fully inserted. Insert the BSU.				
9	E3	BSU	25070103	1681	BSU inactivated administratively.
	The BSU was placed in the inactive state by using the `inactivate` command. [Explanation of message variables] None. [Action] None.				
10	E3	BSU	25070700	1681	BSU online dump command executed.
	The memory dump initiated by executing the BSU dump (without BSU restart) command was completed. [Explanation of message variables] None. [Action] None.				
11	E3	BSU	25070701	1681	Can't execute dump command(other dump executing).
	Other dump processing is being performed. [Explanation of message variables] None. [Action] Wait a while and then re-execute the command.				
12	E3	BSU	25070702	1681	BSU dump canceled.
	The BSU dump was canceled. [Explanation of message variables] None. [Action] 1. Use the `show system` command to check the amount of free space in the user area (the recommended amount is 30 MB). If there is not enough free space, delete dump files and then re-execute the command. 2. After other dump processing has been completed, re-execute the command.				
13	E3	BSU	25070800	1681	BSU offline dump command executed.
	The memory dump initiated by executing the BSU dump (with BSU restart) command was completed. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
14	E3	BSU	25070900	1681	This BSU changed to active.
	This BSU was switched to the active state. [Explanation of message variables] None. [Action] 1. Check the BSU log, and take action appropriate for the failure that has occurred. 2. If a command was used to switch the BSU, no action is required.				
15	E3	BSU	25070901	1681	This BSU changed from active.
	This BSU was switched out of the active state. [Explanation of message variables] None. [Action] 1. Check the BSU log, and take action appropriate for the failure that has occurred. 2. If a command was used to switch the BSU, no action is required.				
16	E3	BSU	25070a01	1681	BSU restarted because of its HDC update done.
	The BSU was restarted because the HDC (Hardware Dependent Code) was updated. [Explanation of message variables] None. [Action] None.				
17	E3	BSU	25070a02	1681	HDC on BSU will updated.Do not pull out BSU.
	The HDC (Hardware Dependent Code) will be updated. [Explanation of message variables] None. [Action] Do not remove the BSU until the log message `BSU restarted because of its HDC update done.` is displayed.				
18	E3	BSU	25070b00	1681	BSU is not initialized because the number or location of BSU is different from "max-bsu" configuration.
	The BSU was not restarted because the number of installed BSUs or the location of the slot where the BSU was installed was different from the `max-bsu` value in the configuration. Using the `show system` command, make sure that the value of `Redundancy bsu-mode` and the status of the BSU installed on the switch are consistent with the configuration. [Explanation of message variables] None. [Action] None.				
19	E5	BSU	25070203	1681	Fatal error detected on standby BSU.
	An error occurred in the standby BSU. [Explanation of message variables] None. [Action] Check the BSU log, and take action appropriate for the failure that has occurred.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
20	E5	BSU	25070204	1681	Fatal error detected on active BSU.
	An error occurred in the active BSU. [Explanation of message variables] None. [Action] Check the BSU log, and take action appropriate for the failure that has occurred.				
21	E6	BSU	25070200	1681	BSU restarted because its hardware failure detected during the self diagnosis.
	A failure was detected during BSU self-diagnosis. The BSU will be restarted. [Explanation of message variables] None. [Action] After the restart, check the log information to determine if recovery from the failure was successful. If recovery was successful, operations can resume. If recovery failed, replace the BSU.				
22	E6	BSU	25070201	1681	BSU stopped because its hardware failure detected.
	A hardware failure was detected in a BSU. The BSU will stop. [Explanation of message variables] None. [Action] Replace the BSU.				
23	E6	BSU	25070400	1681	BSU restarted, but not recovered from hardware failure.
	The BSU was restarted, but recovery from one of the following was not successful: • Hardware fault • Failure that was detected during self-diagnosis • Health check error [Explanation of message variables] None. [Action] Replace the BSU.				
24	E6	BSU	25070500	1681	BSU not initialized because it is unavailable configuration.
	Initialization failed because the configuration was unusable. [Explanation of message variables] None. [Action] Change the configuration of the following so that they are correct: • Flow distribution pattern for filtering and the QoS functionality • Distribution pattern for the maximum number of entries per switch				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
25	E6	BSU	25070501	1681	BSU not initialized because it is unknown BSU.
	The BSU board could not be initialized because it was an unknown BSU board. [Explanation of message variables] None. [Action] 1. The BSU board is not fully inserted. Insert the BSU board properly. 2. The BSU board is not supported by the software version. Check the BSU board type and the software version, and then either replace the BSU board or update the software. 3. The BSU board is not supported by the Switch. Replace the BSU board.				
26	E6	BSU	25070502	1681	BSU not initialized because it is mismatch BSU.
	Initialization failed because different types of BSU boards existed. [Explanation of message variables] None. [Action] Replace the BSU board with the same type of BSU board as the other BSU boards.				
27	E6	BSU	25070902	1681	System cannot execute BSU swap. All BSU restarted.
	System switching of the BSU could not be performed. All BSUs will be restarted. [Explanation of message variables] None. [Action] None.				
28	E6	BSU	25070903	1681	Health check error detected on standby BSU. This system (BCU1) is active.
	An error occurred during a health check performed for the standby BSU from the active BCU1. The BCU1 system is the active system. [Explanation of message variables] None. [Action] 1. Make sure that the recovery log message `Health check error recovered.` for this log data has been output. If this message has been output, no action is required. 2. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 3. If the problem cannot be corrected after the above actions, see the *Troubleshooting Guide* and take appropriate action.				
29	E6	BSU	25070904	1681	Health check error detected on standby BSU. This system (BCU2) is active.
	An error occurred during a health check performed for the standby BSU from the active BCU2. The BCU2 system is the active system. [Explanation of message variables] None. [Action] 1. Make sure that the recovery log message `Health check error recovered.` for this log data has been output. If this message has been output, no action is required. 2. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 3. If the problem cannot be corrected after the above actions, see the *Troubleshooting Guide* and take appropriate action.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
30	E6	BSU	25070a00	1681	BSU restarted because of its HDC update failure.
	The BSU was restarted because updating of the HDC (Hardware Dependent Code) failed. [Explanation of message variables] None. [Action] Replace the BSU.				
31	R6	BSU	25070002	1681	BSU initialized.
	The BUS has been initialized. [Explanation of message variables] None. [Action] None.				
32	R6	BSU	25070200	1681	BSU recovered from hardware failure detected during the self diagnosis.
	The BSU has recovered from the hardware failure detected during BSU self-diagnosis. [Explanation of message variables] None. [Action] None.				
33	R6	BSU	25070903	1681	Standby BSU health check error recovered. This system (BCU1) is active.
	Recovery from the error in the health check from the active BCU1 for the standby BSU was successful. The BCU1 system is the active system. [Explanation of message variables] None. [Action] None.				
34	R6	BSU	25070904	1681	Standby BSU health check error recovered. This system (BCU2) is active.
	Recovery from the error in the health check from the active BCU2 for the standby BSU was successful. The BCU2 system is the active system. [Explanation of message variables] None. [Action] None.				
35	R6	BSU	25070905	1681	BSU event initialized as a result of changing this system from active to standby.
	Past BSU event information was initialized because the Switch was switched from the active BCU to the standby BCU. This log data is displayed only for the standby BCU. [Explanation of message variables] None. [Action] None.				

3.4.4 Event location = NIF

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

Table 3-13: Switch failure and event information when the event location is NIF

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
1	E3	NIF	01200174	1240	Failed in accumulated running time access to NIF.
	Access to the total operating time for the NIF failed. [Explanation of message variables] None. [Action] There are no effects on communication and normal operation. However, the functionality for managing the total operating time cannot be used. If you want to use this functionality, replace the NIF.				
2	E3	NIF	23000163	1240	NIF inactivated because of SOP operation.
	The NIF was placed in the inactive state in response to an `inactivate` instruction from the system operation panel. [Explanation of message variables] None. [Action] None.				
3	E3	NIF	23000167	1240	NIF activated because of SOP operation.
	The NIF was released from the inactive state in response to an `activate` instruction from the system operation panel. [Explanation of message variables] None. [Action] None.				
4	E3	NIF	25000000	1240	NIF enabled administratively.
	The NIF was released from the disabled state by using the `power enable` or `no schedule-power-control shutdown` configuration command. [Explanation of message variables] None. [Action] None.				
5	E3	NIF	25000001	1240	NIF board connected.
	Insertion of an NIF board was detected. [Explanation of message variables] None. [Action] None.				
6	E3	NIF	25000003	1240	NIF activated administratively.
	The NIF was released from the inactive state by using the `activate` command. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
7	E3	NIF	25000004	1240	Redundancy NIF Group *<nif group no.>*:This NIF changed to active.
	The indicated NIF has changed to the active system of the redundant group. [Explanation of message variables] *<nif group no.>*: NIF redundant group number [Action] 1. Check the NIF or port log, and take action appropriate for the failure that has occurred. 2. If a command or scheduling was used to change the operating status, no action is required.				
8	E3	NIF	25000100	1240	NIF disabled administratively.
	The NIF was disabled by configuring `no power enable` or `schedule-power-control shutdown` with a configuration command. [Explanation of message variables] None. [Action] None.				
9	E3	NIF	25000101	1240	NIF board notconnected.
	Removal of a NIF board was detected. [Explanation of message variables] None. [Action] The NIF board has been removed or has not been fully inserted. Insert the NIF.				
10	E3	NIF	25000103	1240	NIF inactivated administratively.
	The NIF was placed in the inactive state by using the `inactivate` command. [Explanation of message variables] None. [Action] None.				
11	E3	NIF	25000104	1240	Redundancy NIF Group *<nif group no.>*:This NIF changed from active.
	The indicated NIF is no longer the active system of the redundant group. [Explanation of message variables] *<nif group no.>*: NIF redundant group number [Action] 1. Check the NIF or port log, and take action appropriate for the failure that has occurred. 2. If a command or scheduling was used to change the operating status, no action is required.				
12	E3	NIF	25000700	1240	NIF online dump command executed.
	The memory dump initiated by executing the NIF dump (without NIF restart) command was completed. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
13	E3	NIF	25000701	1240	Can't execute dump command(other dump executing).
	Other dump processing is being performed. [Explanation of message variables] None. [Action] Wait a while and then re-execute the command.				
14	E3	NIF	25000702	1240	NIF dump canceled.
	The NIF dump was canceled. [Explanation of message variables] None. [Action] 1. Use the `show system` command to check the amount of free space in the user area (the recommended amount is 30 MB). If there is not enough free space, delete dump files and then re-execute the command. 2. After other dump processing has been completed, re-execute the command.				
15	E3	NIF	25000800	1240	NIF offline dump command executed.
	The memory dump initiated by executing the NIF dump (with NIF restart) command was completed. [Explanation of message variables] None. [Action] None.				
16	E3	NIF	25000a01	1240	NIF restarted because of its HDC update done.
	The NIF was restarted because the HDC (Hardware Dependent Code) was updated. [Explanation of message variables] None. [Action] None.				
17	E3	NIF	25000a02	1240	HDC on NIF will updated. Do not pull out NIF.
	The HDC (Hardware Dependent Code) will be updated. [Explanation of message variables] None. [Action] Do not remove the NIF until the log message saying `NIF restarted because of its HDC update done.` is displayed.				
18	E3	NIF	25000a03	1240	HDC on NIF update required, but not updated by configuration.
	Although the HDC (Hardware Dependent Code) needs to be updated, it was not updated because `no system nif-hdc restart` was configured by using a configuration command. [Explanation of message variables] None. [Action] Restart the NIF.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
19	E3	NIF	2523000c	1240	The nif does not support the specified shaper mode.
	This NIF does not support the specified shaper mode. [Explanation of message variables] None. [Action] Review the shaper mode specified for the relevant NIF.				
20	E3	NIF	2523000d	1240	The nif does not support hierarchical shaper.
	This NIF does not support the hierarchical shaper functionality. [Explanation of message variables] None. [Action] Delete the hierarchical shaper information from the configuration of the relevant NIF.				
21	E6	NIF	25000200	1240	NIF restarted because its hardware failure detected during the self diagnosis.
	A failure was detected during NIF self-diagnosis. The NIF will be restarted. [Explanation of message variables] None. [Action] After the restart, check the log information to determine if recovery from the failure was successful. If recovery was successful, operations can resume. If recovery failed, replace the NIF.				
22	E6	NIF	25000201	1240	NIF stopped because its hardware failure.
	A hardware failure was detected in a NIF. The NIF will stop. [Explanation of message variables] None. [Action] Replace the NIF.				
23	E6	NIF	25000400	1240	NIF restarted, but not recovered from hardware failure.
	The NIF was restarted although the NIF had not recovered from the hardware failure or a failure detected during self-diagnosis. [Explanation of message variables] None. [Action] Replace the NIF.				
24	E6	NIF	25000500	1240	NIF not initialized because of its unknown NIF.
	The NIF board could not be initialized because it is an unknown NIF board. [Explanation of message variables] None. [Action] 1. The NIF board is not fully inserted. Insert the NIF board properly. 2. The NIF board is not supported by the software version. Check the NIF board type and the software version, and then either replace the NIF board or update the software. 3. The NIF board is not supported by the Switch. Replace the NIF board.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
25	E6	NIF	25000a00	1240	NIF restarted because of its HDC update failure.
	The NIF was restarted because updating of the HDC (Hardware Dependent Code) failed. [Explanation of message variables] None. [Action] Replace the NIF.				
26	R6	NIF	25000002	1240	NIF initialized.
	The NIF has been initialized. [Explanation of message variables] None. [Action] None.				
27	R6	NIF	25000200	1240	NIF recovered from hardware failure detected during the self diagnosis.
	The NIF has recovered from the hardware failure detected during NIF self-diagnosis. [Explanation of message variables] None. [Action] None.				
28	R6	NIF	25000900	1240	NIF event initialized as a result of changing this system from active to standby.
	Past NIF event information was initialized because the Switch was switched from the active system to the standby system. This log data is displayed only for the standby system. [Explanation of message variables] None. [Action] None.				

3.5 Port

3.5.1 Event location = PORT

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

Table 3-14: Switch 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 1353	Port enabled administratively.
	The port was released from the disabled state by configuring `no shutdown` or `no schedule-power-control shutdown` with a configuration command. [Explanation of message variables] None. [Action] None.				
2	E3	PORT	25011006	1350 1353	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 1353	Port disabled administratively.
	The port was disabled by using the `shutdown` or `schedule-power-control shutdown` configuration command. [Explanation of message variables] None. [Action] None.				
4	E3	PORT	25011106	1350 1353	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	25011301	1350	Port does not support 10BASE-T half.
	10BASE-T half-duplex mode is not supported. [Explanation of message variables] None. [Action] Change the duplex mode setting in the port configuration to a value other than `half`. For details, see *10BASE-T, 100BASE-TX, and 1000BASE-T connection specifications* in *15.4.1 Functionality* in the manual *Configuration Guide Vol. 1 For Version 11.7*.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
6	E3	PORT	25011302	1350	Port does not support 100BASE-TX half.
	100BASE-TX half-duplex mode is not supported. [Explanation of message variables] None. [Action] Change the duplex mode setting in the port configuration to a value other than `half`. For details, see *10BASE-T, 100BASE-TX, and 1000BASE-T connection specifications* in *15.4.1 Functionality* in the manual *Configuration Guide Vol. 1 For Version 11.7*.				
7	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] 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 configuring `no traffic-shape rate` with a configuration command.				
8	E3	PORT	25230008	1350	Port does not support traffic-shape rate feature.
	Port bandwidth control is not supported. [Explanation of message variables] None. [Action] Check the operating conditions of port bandwidth control in *Notes* for the `traffic-shape rate` configuration command. After the check, do either of the following: 1. If port bandwidth control is to be used, replace the board with a board that supports port bandwidth control. 2. If port bandwidth control is not to be used, delete port bandwidth control by configuring `no traffic-shape rate` with a configuration command.				
9	E3	PORT	25230009	1350	Port does not support *<scheduling mode>* scheduling mode.
	The scheduling mode *<scheduling mode>* is not supported. [Explanation of message variables] *<scheduling mode>*: Scheduling mode specified in the `qos-queue-group` and `qos-queue-list` configuration commands [Action] Check the operating conditions of the scheduling mode in *Notes* for the `qos-queue-list` command. After the check, do either of the following: 1. If the scheduling mode *<scheduling mode>* indicated in the message is to be used, replace the board with a board that supports that scheduling mode. 2. If the scheduling mode *<scheduling mode>* indicated in the message is not to be used, use the `qos-queue-group` and `qos-queue-list` command to change the mode to the available scheduling mode.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
10	E3	PORT	2523000a	1350	Port does not support *<number of queue>* queue.
	The number of queues *<number of queues>* is not supported. [Explanation of message variables] *<number of queues>*: Number of queues specified in the `qos-queue-group` and `qos-queue-list` configuration commands [Action] Check the operating conditions for the number of queues in *Notes* for the `qos-queue-list` command. After the check, do either of the following: 1. If the number of queues *<number of queues>* indicated in the message is to be used, replace the board with a board that supports that number of queues. 2. If the number of queues *<number of queues>* indicated in the message is not to be used, use the `qos-queue-group` or `qos-queue-list` command to change the value of the `number_of_queue` parameter.				
11	E3	PORT	2523000b	1350	Unable to use traffic-shape rate feature because value exceeding setting range was specified.
	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 specified for the `traffic-shape rate` command to a value within the setting range. For details about the valid setting range, see the explanation of the `rate` parameter of the `traffic-shape rate` configuration command.				
12	E3	PORT	2523000e	1350	Port does not support legacy shaper.
	This NIF does not support the legacy shaper functionality. [Explanation of message variables] None. [Action] Delete the legacy shaper information from the configuration for the relevant NIF.				
13	E3	PORT	2523000f	1350	The specified shaper port-rate exceeded the interface bandwidth.
	Port bandwidth control is not available because a bandwidth exceeding the line speed was set for the port bandwidth control of the hierarchical shaper functionality specified for the port, or for the maximum bandwidth control for user bandwidth control. [Explanation of message variables] None. [Action] Change the port bandwidth control value or the maximum bandwidth control value for user bandwidth control to a value equal to or less than the line bandwidth.				
14	E3	PORT	25230010	1350	The specified sum of shaper min-rate exceeded the interface bandwidth.
	Minimum bandwidth control is not available because the total minimum bandwidth for the hierarchical shaper specified for the port exceeds the line speed. For llrlq1 and llrlq2 users, the maximum bandwidth applies. [Explanation of message variables] None. [Action] Review and change the minimum bandwidth for each user and the maximum bandwidth for llrlq1 and llrlq2 users so that the total of the minimum bandwidth values is equal to or less than the line bandwidth value.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
15	E3	PORT	25230011	1350	Cannot configure all the shaper users, because there is an inconsistency in the number of shaper users or shaper nif parameters.
	Some of the hierarchical shaper users specified for the port could not be configured. The reasons are as follows: • The number of users that can be specified for the specified port has been exceeded. • A parameter required for the specified shaper mode has not been configured. [Explanation of message variables] None. [Action] Perform the following procedure: 1. Check the number of users specified in the shaper information in the configuration to make sure that the number of specified users does not exceed the capacity limit. If the capacity limit has been exceeded, revise the number of users to be within the capacity limit. If the capacity limit has not been exceeded, do the following: 2. Execute the `show shaper` command and check which users have not been configured for the port. Note that the users not displayed by the `show shaper` command are users that have not been configured for the port. 3. See the user-list information for these users and check if all parameters required for configuring these users for the port have been specified for the shaper mode of the specified port. For details about the parameters required for each shaper mode, see *6.4 Description of the hierarchical shaper* in the manual *Configuration Guide Vol. 2 For Version 11.7*.					
16	E3	PORT	25230012	1350	Some of the shaper user parameters reduced to their maximum values, because they exceeded the upper limit.
	The values of some hierarchical shaper user parameters specified for the port were changed to the upper limit values. The reason for the change is that the values exceeded the range of values that can be specified for the applicable port. [Explanation of message variables] None. [Action] Check if the following parameter values specified for the users that are configured for the port exceeded the upper limit for the shaper mode of the specified port. For details about the upper limit values, see the description of the following configuration commands: • `shaper port buffer` command • `shaper user-list` command with the `weight` parameter					
17	E3	PORT	25230013	1350	Some of the shaper parameters reset to the default values, because they are not supported in the shaper mode of the target nif.
	The values of some hierarchical shaper parameters specified for the port were changed to their initial values because the values cannot be specified for the port. [Explanation of message variables] None. [Action] Check if the following parameter values specified for the users configured for the port are values that can be specified for the shaper mode for the specified port. For details about the values that can be specified for each shaper mode, see the description of the scheduling mode for the `shaper user-list` configuration command.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
18	E3	PORT	25230014	1350	Cannot specify the shaper parameters, because they are inconsistent with the shaper mode of the target nif.
	Of the hierarchical shaper parameters set for the port, those that were inconsistent with the configuration conditions were invalidated. [Explanation of message variables] None. [Action] The parameters listed below have configuration conditions for each NIF type and shaper mode set for the specified NIF. For details, see *6.10 Correspondence between NIF models and send control functionality* in the manual *Configuration Guide Vol. 2 For Version 11.7*. • `shaper wgq-group rate-limit` • `shaper user-list peak-rate` • `shaper user-list llpq-peak-rate` • `shaper user-list min-rate` • `shaper user-list weight` • `shaper user`				
19	E3	PORT	25230015	1350	The nif does not support the specified shaper mode.
	This NIF does not support the specified shaper mode. [Explanation of message variables] None. [Action] Review the shaper mode specified for the relevant NIF.				
20	E3	PORT	25230016	1350	The min-rate of all shaper users is not guaranteed because the specified llpq-peak-rate exceeded the min-rate.
	The minimum bandwidth for the hierarchical shaper users set on the port and the default user cannot be guaranteed because the LLPQ bandwidth control value for the user list of the hierarchical shaper set on the port exceeded the minimum bandwidth. [Explanation of message variables] None. [Action] To guarantee the minimum bandwidth for each user, set the LLPQ bandwidth control value to a value equal to or less than the minimum bandwidth value.				
21	E3	PORT	25230017	1350	Unable to use traffic-shape rate feature because its setting unit was an unjust value.
	Port bandwidth control is not available because the units used for the setting are invalid. [Explanation of message variables] None. [Action] Change the units specified for the `traffic-shape rate` command to the setting units that can be specified. For details about specifiable setting units, see the explanation of the `rate` parameter of the `traffic-shape rate` configuration command.				
22	E4	PORT	25011001	1350 1353	Port up.
	The port is up. [Explanation of message variables] None. [Action] None.				

198

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
23	E4	PORT	25011002	1350	Transceiver connected.
	A transceiver insertion was detected. [Explanation of message variables] None. [Action] None.				
24	E4	PORT	25011101	1350 1353	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 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 an optical attenuator is used, 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.				
25	E4	PORT	25011102	1350	Transceiver notconnected.
	A transceiver removal was detected. [Explanation of message variables] None. [Action] Insert the transceiver properly.				
26	E4	PORT	25011103	1350	Auto negotiation failed.
	Auto negotiation has failed. [Explanation of message variables] None. [Action] 1. Check the auto negotiation status. 2. Execute the `test interfaces` command, and make sure that the switch has no problem. 3. If the switches and cables are normal, check the connected devices.				
27	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 noise errors. [Explanation of message variables] None. [Action] 1. Execute the `test interfaces` command, and make sure that the cables have no problem. 2. If the switches and cables are normal, check the connected devices.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
28	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 noise errors. [Explanation of message variables] None. [Action] 1. Execute the `test interfaces` command, and make sure that the switches and cables have no errors. 2. If the switches and cables are normal, check the connected devices.					
29	E4	PORT	25011200	1350	Transceiver stopped because its hardware failure.
	A transceiver failure was detected. The transceiver will stop. [Explanation of message variables] None. [Action] Replace the transceiver.					
30	E4	PORT	25011500	1350	Transceiver not supported.
	An unsupported transceiver was detected. [Explanation of message variables] None. [Action] Insert a supported transceiver. When you are using an SFP transceiver for 10BASE-T, 100BASE-TX, or 1000BASE-T, see *15.4.3 SFP for 10BASE-T/100BASE-TX/1000BASE-T* in the manual *Configuration Guide Vol. 1 For Version 11.7* and confirm that the NIF supports the transceiver.					
31	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] 1. Make sure that the IEEE802.3ah/OAM function is valid at the connection destination. 2. Execute the `test interfaces` command, and make sure that the switches and cables have no errors. 3. If the switches and cables are normal, check the connected devices. After the above, activate the port by using the `activate` command.					
32	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
33	E4	PORT	25100027	1350	NIF *<nif no.>* Port *<port no.>*:inactivated because of storm detection.
	A port was deactivated because a storm was detected. [Explanation of message variables] *<nif no.>*: NIF number *<port no.>*: Port number [Action] After recovery from the storm, use the `activate` command to change the port status to active.					
34	E4	PORT	25100028	1350	NIF *<nif no.>* Port *<port no.>*:storm detected.
	A storm was detected. [Explanation of message variables] *<nif no.>*: NIF number *<port no.>*: Port number [Action] None.					
35	E4	PORT	25100029	1350	NIF *<nif no.>* Port *<port no.>*:storm recovered.
	The system has recovered from a storm. [Explanation of message variables] *<nif no.>*: NIF number *<port no.>*: Port number [Action] None.					

3.6 Optional modules

3.6.1 Event location = FAN

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

Table 3-15: Switch 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	01200174	1800	Failed in accumulated running time access to *<fan unit no.>*.
	Access to the total operating time for the fan unit *<fan unit no.>* failed. [Explanation of message variables] *<fan unit no.>*: Number of the fan unit for which access to the total operating time failed (`FAN1`, `FAN2`, `FAN3`, or `FAN4` is displayed) [Action] There are no effects on communication and normal operation. However, the functionality for managing the total operating time cannot be used. If you want to use this function, replace the fan unit.				
2	E8	FAN	00000001	1800	Error detected on *<fan no.>*, Replace *<fan unit no.>*.
	A failure occurred in the fan *<fan no.>*. [Explanation of message variables] *<fan no.>*: Number of the fan in which the failure occurred (one of `FAN1(1)`, `FAN1(2)`, `FAN1(3)`, `FAN2(4)`, `FAN2(5)`, `FAN2(6)`, `FAN3(7)`, `FAN3(8)`, `FAN3(9)`, `FAN4(10)`, `FAN4(11)`, and `FAN4(12)` is displayed) *<fan unit no.>*: Number of the fan unit in which the failure occurred (`FAN1`, `FAN2`, `FAN3`, or `FAN4` is displayed) A message is displayed for each fan unit as follows. Example 1: When a failure occurs in the fan `FAN1(1)`: Error detected on FAN1(1), Replace FAN1. Example 2: When a failure occurs in the fans `FAN1(1)` and `FAN2(1)`: Error detected on FAN1(1), Replace FAN1. Error detected on FAN2(1), Replace FAN2. For details about the fan locations, see *Table 9-5 Correspondence between fan numbers, operation log data, and chassis* in the manual *Operation Command Reference Vol. 1 For Version 11.7.* [Action] Replace the fan unit *<fan unit no.>*.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
3	E8	FAN	00000002	1800	*<fan no.>* stopped. Replace *<fan unit no.>* immediately.
	The fan *<fan no.>* stopped. [Explanation of message variables] *<fan no>*.: Number of the fan in which the failure occurred (two or more of `FAN1(1)`, `FAN1(2)`, `FAN1(3)`, `FAN2(4)`, `FAN2(5)`, `FAN2(6)`, `FAN3(7)`, `FAN3(8)`, `FAN3(9)`, `FAN4(10)`, `FAN4(11)`, and `FAN4(12)` are displayed) *<fan unit no.>*: Number of the fan unit in which the failure occurred (`FAN1`, `FAN2`, `FAN3`, or `FAN4` is displayed) A message is displayed for each fan unit as follows. Example 1: When a failure occurs in the fans `FAN1(1)` and `FAN2(2)`: FAN1(1), FAN1(2) stopped. Replace FAN1 immediately. Example 2: When a failure occurs in the fans `FAN1(1)`, `FAN2(2)`, `FAN1(3)`, `FAN2(4)`, and `FAN2(5)`: FAN1(1), FAN1(2), FAN1(3) stopped. Replace FAN1 immediately. FAN2(4), FAN2(5) stopped. Replace FAN2 immediately. For details about the fan locations, see *Table 9-5 Correspondence between fan numbers, operation log data, and chassis* in the manual *Operation Command Reference Vol. 1 For Version 11.7*. [Action] Immediately replace the fan unit *<fan unit no.>*.					
4	E8	FAN	00000003	1800	*<fan unit no.>* is notconnect.
	The fan unit *<fan unit no.>* is not installed. [Explanation of message variables] *<fan unit no.>*: Number of the fan unit that is not installed (`FAN1`, `FAN2`, `FAN3`, or `FAN4` is displayed) A message is displayed for each fan unit as follows. Example 1: When the fan unit `FAN1` is not installed: FAN1 is notconnect. Example 2: When the fan units `FAN1` and `FAN2` are not installed: FAN1 is notconnect. FAN2 is notconnect. For details about the fan locations, see *Table 9-5 Correspondence between fan numbers, operation log data, and chassis* in the manual *Operation Command Reference Vol. 1 For Version 11.7*. [Action] 1. If the fan unit is being replaced, continue the replacement process. 2. If no replacement is being made, check the installation status. If the fan unit is not installed, install it. 3. If the fan has been installed, it might not be fully inserted. Remove the fan unit and then install it again. 4. If the problem cannot be corrected by taking the above action, replace the fan unit.					
5	E8	FAN	00000004	1800	Failed in speed change of *<fan unit no.>*.
	An attempt to change the fan rotation speed of *<fan unit no.>* failed. [Explanation of message variables] *<fan unit no.>*: Number of the fan unit for which the attempt to change the speed failed (`FAN1`, `FAN2`, `FAN3`, or `FAN4` is displayed) A message is displayed for each fan unit as follows. Example 1: When an attempt to change the speed of `FAN1` failed: Failed in speed change of FAN1. Example 2: When an attempt to change the speed of `FAN1` and `FAN2` failed: Failed in speed change of FAN1. Failed in speed change of FAN2. For details about the fan locations, see *Table 9-5 Correspondence between fan numbers, operation log data, and chassis* in the manual *Operation Command Reference Vol. 1 For Version 11.7*. [Action] Replace the fan unit *<fan unit no.>*.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
6	E9	FAN	00000022	1800	Fan unit is down.Replace fan and restart the device.
	The fan unit stopped. [Explanation of message variables] None. [Action] Replace the fan unit and restart the switch.				
7	R8	FAN	00000001	1800	*<fan unit no.>* is normal.

	Fan unit *<fan unit no.>* is operating normally.
	[Explanation of message variables]
	<fan unit no.>: Number of the fan unit for which failure recovery was successful (`FAN1`, `FAN2`, `FAN3`, or `FAN4` is displayed)
	A message is displayed for each fan unit as follows.
	Example 1: When the fan unit `FAN1` is operating normally:
	    FAN1 is normal.
	Example 2: When the fan units `FAN1` and `FAN2` are operating normally:
	    FAN1 is normal.
	    FAN2 is normal.
	
	For details about the fan locations, see *Table 9-5 Correspondence between fan numbers, operation log data, and chassis* in the manual *Operation Command Reference Vol. 1 For Version 11.7.*
	[Action]
	None.				

3.6.2 Event location = PS

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

Table 3-16: Switch 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	01200174	2200	Failed in accumulated running time access to *<ps>*.
	Access to the total operating time of the power supply failed. [Explanation of message variables] *<ps>*: Power supply for which access to the total operating time failed (`PS1`, `PS2`, `PS3`, `PS4`, `PS5`, `PS6`, `PS7`, or `PS8` is displayed) [Action] There are no effects on communication and normal operation. However, the functionality for managing the total operating time cannot be used. If you want to use this functionality, replace the power supply.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
2	E8	PS	00000001	2200	*<ps>* is power off. *<ps>* is notconnect.
	The displayed power supply is off. The displayed power supply has not been installed. If there is no power supply whose power is off, *<ps>* `is notconnect.` is displayed. If there is no power supply that has not been installed, *<ps>* `is power off.` is displayed. Only when there are a power supply that has been turned off and a power supply that has not been installed, *<ps>* `is power off.` *<ps>* `is notconnect.` is displayed. [Explanation of message variables] *<ps>*: Power supply that is off or that has not been installed (`PS1`, `PS2`, `PS3`, `PS4`, `PS5`, `PS6`, `PS7`, or `PS8` is displayed) The following shows an example of the log message displayed when an AX6304S (AC model) is used. Example 1: When PS1 is off: PS1 is power off. Example 2: When PS2 is not installed: PS2 is notconnect. Example 3: When PS1 is off and PS3 and PS4 are not installed: PS1 is power off. PS3, PS4 is notconnect. [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 status of the power supply. 4. If the problem cannot be corrected after the above actions, replace the power supply.				
3	E8	PS	00000102	2200	Power unit isn't redundantly mounted.
	The power supply is not in a redundant configuration. [Explanation of message variables] None. [Action] Check the status of the power supply. If the power supply is not in a redundant configuration, configure `no power redundancy-mode` with a configuration command.				
4	E9	PS	00000201	2200	Power supply unit for AC and for DC is consolidated.
	AC and DC power supplies are installed together. [Explanation of message variables] None. [Action] Install only AC power units or DC power supplies.				
5	R8	PS	00000001	2200	*<ps>* is normal.
	The displayed power supply is operating normally. When the power supply is normal, this message is also output during startup of a BCU, CSU, or MSU. [Explanation of message variables] *<ps>*: Power supply in a normal state (`PS1`, `PS2`, `PS3`, `PS4`, `PS5`, `PS6`, `PS7`, or `PS8` is displayed) The following shows an example of the log message displayed when an AX6304S (AC model) is used. Example: When PS1, PS2, PS3, and PS4 are in a normal state: PS1, PS2, PS3, PS4 is normal. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
6	R8	PS	00000102	2200	Power unit is mounted redundantly or mode changed.
	The power supply is operating redundantly. Alternatively, the operation mode has changed. [Explanation of message variables] None. [Action] None.				

3.7 Basic control unit [AX6700S]

3.7.1 Event location = BCU

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

Table 3-17: Switch failure and event information when the event location is BCU

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
1	E3	BCU	00020106	2301	The temperature of BCU reached the warning level (*<temperature>* degree).
	The hardware temperature has reached the temperature specified by the `system temperature-warning-level` configuration command. [Explanation of message variables] *<temperature>*: Temperature of the switch (degrees Celsius) [Action] The hardware temperature has reached the specified temperature. Check the environment around the switch (such as the status of the fan, the ventilation, and the existence of any heat sources).					
2	E3	BCU	00020107	2301	The temperature of BCU came down from the warning level.
	The hardware temperature dropped three degrees or more below the temperature specified by the `system temperature-warning-level` configuration command. [Explanation of message variables] None. [Action] None.					
3	E3	BCU	01200160	2314	Standby system inactivated because of SOP operation.
	The standby system was placed in the inactive state in response to an `inactivate` instruction from the system operation panel. [Explanation of message variables] None. [Action] None.					
4	E3	BCU	01200164	2314	Standby system activated because of SOP operation.
	The standby system was released from the inactive state in response to an `activate` instruction from the system operation panel. [Explanation of message variables] None. [Action] None.					
5	E3	BCU	01200174	2301	Failed in accumulated running time access to *<bcu>*.
	Access to the total operating time for the BCU failed. [Explanation of message variables] *<bcu>*: BCU for which access to the total operating time failed (either BCU1 or BCU2 is displayed) [Action] There are no effects on communication and normal operation. However, the functionality for managing the total operating time cannot be used. If you want to use this functionality, replace the BCU.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
6	E3	BCU	01200180	2301	Fan speed is high because temperature of BCU hardware exceeded tolerance level of high temperature.
	The fan was rotating at high speed because the hardware temperature exceeded the allowable range. [Explanation of message variables] None. [Action] Check and improve the environment such as ventilation and heat sources around the switches.				
7	E3	BCU	01200181	2301	Fan speed is normal because temperature of BCU hardware returned to normal level.
	The fan returned to regular speed because the hardware temperature returned to normal. [Explanation of message variables] None. [Action] None.				
8	E3	BCU	01200182	2301	Recovery due to the failure was restrained.
	The board suppressed recovery because of a failure. [Explanation of message variables] None. [Action] Use the `show logging` or `show logging` command with the `standby` parameter specified to check the log. If a problem is indicated in the log, take appropriate action according to the error message. If recovery of the active system is suppressed, startup (recovery) of the standby system is also suppressed. In this case, there is no need to replace the standby system because a failure has not occurred in the standby system.				
9	E3	BCU	01300408	2314	This system (BCU1) changed from standby to active.BCU2 is standby.
	The BCU1 system was switched from the standby to the active state. BCU2 is the standby system. This message is displayed when system switching occurs due to a fatal error in the former active BSU, or by clicking the Reset button, or by pressing the ACH switch. [Explanation of message variables] None. [Action] 1. There is no problem if the system switching occurred because the Reset button was clicked or the ACH switch was pressed. 2. In all other cases, execute the `show logging` command with the `standby` parameter specified, check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. If the new standby system has not started yet, wait a while before checking for messages.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
10	E3	BCU	01300409	2314	This system (BCU2) changed from standby to active.BCU1 is standby.
	The BCU2 system was switched from the standby to the active state. BCU1 is the standby system. This message is displayed when system switching occurs due to a fatal error in the former active system, by clicking the Reset button, or by pressing the ACH switch. [Explanation of message variables] None. [Action] 1. There is no problem if the system switching occurred because the Reset button was clicked or the ACH switch was pressed. 2. In all other cases, execute the `show logging` command with the `standby` parameter specified, check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. If the new standby system has not started yet, wait a while before checking for messages.				
11	E3	BCU	01300410	2314	This system (BCU1) changed from active to standby.BCU2 is active.
	The BCU1 system was switched from the active to the standby state. BCU2 is the active system. This message is displayed when system switching occurs because of a fatal error in the former active system. [Explanation of message variables] None. [Action] Use the `show logging` command with the `standby` parameter specified to check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. If the new standby system has not started yet, wait a while before checking for messages.				
12	E3	BCU	01300411	2314	This system (BCU2) changed from active to standby.BCU1 is active.
	The BCU2 system was switched from the active to the standby state. BCU1 is the active system. This message is displayed when system switching occurs because of a fatal error in the former active system. [Explanation of message variables] None. [Action] Use the `show logging` command with the `standby` parameter specified to check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. If the new standby system has not started yet, wait a while before checking for messages.				
13	E3	BCU	01300412	2314	System status changed from duplex to simplex.
	The system operating status changed from duplex configuration to single configuration. [Explanation of message variables] None. [Action] None.				
14	E3	BCU	01300413	2314	System status changed from simplex to duplex.
	The system operating status changed from single configuration to duplex configuration. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
15	E3	BCU	01300414	2314	Time is matched at the time of active system.
	The time was matched to the time in the active system. This message is displayed only for the standby system. [Explanation of message variables] None. [Action] None.				
16	E3	BCU	01300417	2314	This system (BCU1) changed from standby to active.BCU2 is standby.
	The BCU1 system was switched from the standby to the active state. BCU2 is the standby system. This message is displayed when system switching occurs because the `reload` command with the `active` parameter specified or the `redundancy force-switchover` command has been executed. [Explanation of message variables] None. [Action] None.				
17	E3	BCU	01300418	2314	This system (BCU2) changed from standby to active.BCU1 is standby.
	The BCU2 system was switched from the standby to the active state. BCU1 is the standby system. This message is displayed when system switching occurs because the `reload` command with the `active` parameter specified or the `redundancy force-switchover` command has been executed. [Explanation of message variables] None. [Action] None.				
18	E3	BCU	01300419	2314	This system (BCU1) changed from active to standby.BCU2 is active.
	The BCU1 system was switched from the active to the standby state. BCU2 is the active system. This message is displayed when system switching occurs because the `reload` command with the `active` parameter specified or the `redundancy force-switchover` command has been executed. [Explanation of message variables] None. [Action] None.				
19	E3	BCU	01300420	2314	This system (BCU2) changed from active to standby.BCU1 is active.
	The BCU2 system was switched from the active to the standby state. BCU1 is the active system. This message is displayed when system switching occurs because the `reload` command with the `active` parameter specified or the `redundancy force-switchover` command has been executed. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
20	E3	BCU	01300421	2314	This system (BCU1) will be changed from active to standby and restarted because of ACH SWITCH pressed.
	The BCU1 system will be switched from the active to the standby state and restarted because the ACH switch was pressed. [Explanation of message variables] None. [Action] None.				
21	E3	BCU	01300422	2314	This system (BCU2) will be changed from active to standby and restarted because of ACH SWITCH pressed.
	The BCU2 system will be switched from the active to the standby state and restarted because the ACH switch was pressed. [Explanation of message variables] None. [Action] None.				
22	E3	BCU	01300442	2314	Partial error detected on other system. Replace unit having error. This system (BCU1) is active.
	A partial failure occurred in the standby BCU. Replace the part in which a failure occurred. The BCU1 system is the active system. [Explanation of message variables] None. [Action] Use the show logging command with the standby parameter specified to check the message regarding the partial failure that occurred in the standby system, and then take action appropriate for the message.				
23	E3	BCU	01300443	2314	Partial error detected on other system. Replace unit.having error. This system (BCU2) is active.
	A partial failure occurred in the standby BCU. Replace the part in which a failure occurred. The BCU2 system is the active system. [Explanation of message variables] None. [Action] Use the show logging command with the standby parameter specified to check the message regarding the partial failure that occurred in the standby system, and then take action appropriate for the message.				
24	E3	BCU	01300457	2314	This system (BCU1) restarted with system changed.
	The BCU1 system will be restarted because system switching occurred. This message is displayed when the configuration was inconsistent, the license key was inconsistent, or a dual configuration had not been set up and system switching occurs due to one of the following causes: A fatal error occurred, the Reset button was clicked, the ACH switch was pressed, the active parameter was specified in the reload command, or the active parameter was specified in the ppupdate command. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
25	E3	BCU	01300458	2314	This system (BCU2) restarted with system changed.
	The BCU2 system will be restarted because system switching occurred. This message is displayed when the configuration was inconsistent, the license key was inconsistent, or a dual configuration had not been set up and system switching occurs due to one of the following causes: A fatal error occurred, the Reset button was clicked, the ACH switch was pressed, the `active` parameter was specified in the `reload` command, or the `active` parameter was specified in the `ppupdate` command. [Explanation of message variables] None. [Action] None.				
26	E3	BCU	01300466	2314	Other system stopped due to temperature trouble. This system (BCU1) is active.
	The standby system stopped because of a temperature error. The BCU1 system is the active system. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
27	E3	BCU	01300467	2314	Other system stopped due to temperature trouble. This system (BCU1) is standby.
	The active system stopped because of a temperature error. The BCU1 system is the standby system. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
28	E3	BCU	01300468	2314	Other system stopped due to temperature trouble. This system (BCU2) is active.
	The standby system stopped because of a temperature error. The BCU2 system is the active system. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
29	E3	BCU	01300469	2314	Other system stopped due to temperature trouble. This system (BCU2) is standby.
	The active system stopped because of a temperature error. The BCU2 system is the standby system. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
30	E3	BCU	01300470	2314	Standby system inactivated because BCU hardware error detected. This system (BCU1) is active.
	The standby system was deactivated because a hardware failure was detected. The BCU1 system is the active system. [Explanation of message variables] None. [Action] Replace the standby BCU.				
31	E3	BCU	01300471	2314	Standby system inactivated because BCU hardware error detected. This system (BCU2) is active.
	The standby system was deactivated because a hardware failure was detected. The BCU2 system is the active system. [Explanation of message variables] None. [Action] Replace the standby BCU.				
32	E3	BCU	01300475	2314	Standby system restarted because BCU hardware error detected. This system (BCU1) is active.
	The standby system was restarted because a hardware failure was detected. The BCU1 system is the active system. [Explanation of message variables] None. [Action] Replace the standby BCU.				
33	E3	BCU	01300476	2314	Standby system restarted because BCU hardware error detected. This system (BCU2) is active.
	The standby system was restarted because a hardware failure was detected. The BCU2 system is the active system. [Explanation of message variables] None. [Action] Replace the standby BCU.				
34	E3	BCU	01300477	2314	Standby system inactivated administratively.
	The standby system was placed in the inactive state by using the `inactivate` command. [Explanation of message variables] None. [Action] None.				
35	E3	BCU	01300478	2314	Standby system activated administratively.
	The standby system was placed in the active state by using the `activate` command. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
36	E3	BCU	01c00200	2301	BCU restarted because of its HDC update done.
	The BCU was restarted because the HDC (Hardware Dependent Code) was updated. [Explanation of message variables] None. [Action] None.				
37	E5	BCU	01300430	2314	System cannot execute BCU force-switchover. This system (BCU1) is active.
	System switching could not be performed. The BCU1 system is the active system. [Explanation of message variables] None. [Action] Replace both the standby and active BCUs.				
38	E5	BCU	01300432	2314	System cannot execute BCU force-switchover. This system (BCU2) is active.
	System switching could not be performed. The BCU2 system is the active system. [Explanation of message variables] None. [Action] Replace both the standby and active BCUs.				
39	E5	BCU	01300434	2314	Health check error detected on other system. This system (BCU1) is active.
	An error occurred during a health check performed for the standby BCU2 from the active BCU1. The BCU1 system is the active system. [Explanation of message variables] None. [Action] 1. Execute the `show logging` command and make sure that the recovery log message `Health check error recovered.` for this log data has been output. If this message has been output, no action is required. 2. If it has not been output, execute the `show logging` command with the `standby` parameter specified, check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. 3. If no failure has occurred in the standby system, the board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 4. If the problem cannot be corrected after the above actions, replace both the active and standby BCUs.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
40	E5	BCU	01300435	2314	Health check error detected on other system. This system (BCU1) is standby.
	An error occurred during a health check performed for the standby BCU1 from the active BCU2. The BCU1 system is the standby system. [Explanation of message variables] None. [Action] 1. Execute the `show logging` command with the `standby` parameter specified and make sure that the recovery log message `Health check error recovered.` for this log data has been output. If this message has been output, no action is required. 2. If it has not been output, execute the `show logging` command, check the message regarding the failure that occurred in the active system, and then take action appropriate for the message. 3. If no failure has occurred in the active system, the board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 4. If the problem cannot be corrected after the above actions, replace both the active and standby BCUs.					
41	E5	BCU	01300436	2314	Health check error detected on other system. This system (BCU2) is active.
	An error occurred during a health check performed for the standby BCU1 from the active BCU2. The BCU2 system is the active system. [Explanation of message variables] None. [Action] 1. Execute the `show logging` command and make sure that the recovery log message `Health check error recovered.` for this log data has been output. If this message has been output, no action is required. 2. If it has not been output, execute the `show logging` command with the `standby` parameter specified, check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. 3. If no failure has occurred in the standby system, the board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 4. If the problem cannot be corrected after the above actions, replace both the active and standby BCUs.					
42	E5	BCU	01300437	2314	Health check error detected on other system. This system (BCU2) is standby.
	An error occurred during a health check performed for the standby BCU2 from the active BCU1. The BCU2 system is the standby system. [Explanation of message variables] None. [Action] 1. Execute the `show logging` command with the `standby` parameter specified and make sure that the recovery log message `Health check error recovered.` for this log data has been output. If this message has been output, no action is required. 2. If it has not been output, execute the `show logging` command, check the message regarding the failure that occurred in the active system, and then take action appropriate for the message. 3. If no failure has occurred in the active system, the board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 4. If the problem cannot be corrected after the above actions, replace both the active and standby BCUs.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
43	E5	BCU	01300438	2314	Fatal error detected on other system. This system (BCU1) is active.
	A fatal error occurred in the standby BCU. The BCU1 system is the active system. [Explanation of message variables] None. [Action] After the standby system has restarted, execute the show logging command with the standby parameter specified, check the failure explanation, and then take action appropriate for the error message.				
44	E5	BCU	01300439	2314	Fatal error detected on other system. This system (BCU1) is standby.
	A fatal error occurred in the active BCU. The BCU1 system is the standby system. [Explanation of message variables] None. [Action] After the active system has restarted, execute the show logging command, check the failure explanation, and then take action appropriate for the error message.				
45	E5	BCU	01300440	2314	Fatal error detected on other system. This system (BCU2) is active.
	A fatal error occurred in the standby BCU. The BCU2 system is the active system. [Explanation of message variables] None. [Action] After the standby system has restarted, execute the show logging command with the standby parameter specified, check the failure explanation, and then take action appropriate for the error message.				
46	E5	BCU	01300441	2314	Fatal error detected on other system. This system (BCU2) is standby.
	A fatal error occurred in the active BCU. The BCU2 system is the standby system. [Explanation of message variables] None. [Action] After the active system has restarted, execute the show logging command, check the failure explanation, and then take action appropriate for the error message.				
47	E5	BCU	25051911	2314	Health check error detected on NIF <nif no.>. This system (BCU1) is active.
	An error occurred during a health check performed for the NIF from the standby BCU2. The BCU1 system is the active system. [Explanation of message variables] <nif no.>: NIF number [Action] After the standby BCU2 has restarted, execute the show logging command with the standby parameter specified, check the failure explanation, and then take action appropriate for the error message.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
48	E5	BCU	25051912	2314	Health check error detected on NIF *<nif no.>*. This system (BCU2) is active.
	An error occurred during a health check performed for the NIF from the standby BCU1. The BCU2 system is the active system. [Explanation of message variables] *<nif no.>*: NIF number [Action] After the standby BCU1 has restarted, execute the `show logging` command with the `standby` parameter specified, check the failure explanation, and then take action appropriate for the error message.					
49	E5	BCU	25051913	2314	Health check error detected on active BSU *<bsu no.>*. This system (BCU1) is active.
	An error occurred during a health check performed for the active BSU from the standby BCU2. The BCU1 system is the active system. [Explanation of message variables] *<bsu no.>*: BSU number [Action] After the standby BCU2 has restarted, execute the `show logging` command with the `standby` parameter specified, check the failure explanation, and then take action appropriate for the error message.					
50	E5	BCU	25051914	2314	Health check error detected on active BSU *<bsu no.>*. This system (BCU2) is active.
	An error occurred during a health check performed for the active BSU from the standby BCU1. The BCU2 system is the active system. [Explanation of message variables] *<bsu no.>*: BSU number [Action] After the standby BCU1 has restarted, execute the `show logging` command with the `standby` parameter specified, check the failure explanation, and then take action appropriate for the error message.					
51	E5	BCU	25051915	2314	Health check error detected on standby BSU *<bsu no.>*. This system (BCU1) is active.
	An error occurred during a health check performed for the standby BSU from the standby BCU2. The BCU1 system is the active system. [Explanation of message variables] *<bsu no.>*: BSU number [Action] After the standby BCU2 has restarted, execute the `show logging` command with the `standby` parameter specified, check the failure explanation, and then take action appropriate for the error message.					
52	E5	BCU	25051916	2314	Health check error detected on standby BSU *<bsu no.>*. This system (BCU2) is active.
	An error occurred during a health check performed for the standby BSU from the standby BCU1. The BCU2 system is the active system. [Explanation of message variables] *<bsu no.>*: BSU number [Action] After the standby BCU1 has restarted, execute the `show logging` command with the `standby` parameter specified, check the failure explanation, and then take action appropriate for the error message.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
53	E7	BCU	00020102	2301	BCU hardware exceeded tolerance level of low temperature(2 degree). Check room temperature.
	The hardware temperature dropped below the allowable temperature range (2 degrees Celsius or lower). [Explanation of message variables] None. [Action] 1. Check and improve the environment such as the room temperature around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
54	E7	BCU	00020103	2301	BCU hardware exceeded tolerance level of high temperature (43 degree). Check that room temperature and the fan is operating normally.
	The hardware temperature rose above the allowable temperature range (43 degrees Celsius or higher). [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
55	E7	BCU	00020104	2301	BCU hardware is becoming high temperature (58 degree). immediately, and check that room temperature and the fan is operating normally.
	The hardware temperature is approaching the high temperature value that affects operation of the switch. [Explanation of message variables] None. [Action] 1. A malfunction might occur in the switch. Immediately check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
56	E8	BCU	01200184	2301	BCU not initialized because it is unknown BCU.
	The BCS board could not be initialized because it was an unknown BCS board. [Explanation of message variables] None. [Action] 1. The BCU board is not fully inserted. Insert the BCU properly. 2. The BCU board is not supported by the software version. Check the BCU board type and the software version, and then either replace the BCU board or update the software. 3. The BCU board is not supported by the Switch. Replace the BCU board.				
57	E9	BCU	00020105	2301	BCU hardware is becoming high temperature which give damage to this system. (65 degree)
	The hardware temperature has reached a temperature (65 degrees Celsius) that is likely to critically damage device operation. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
58	E9	BCU	01200173 01300474 2b061200	2314	System restarted because BCU hardware error detected.
	The system was restarted because a hardware failure was detected. [Explanation of message variables] None. [Action] Replace the BCU.				
59	E9	BCU	01300472	2314	This system (BCU1) inactivated because BCU hardware error detected.
	The BCU1 system was inactivated because a hardware failure was detected. [Explanation of message variables] None. [Action] Replace the standby BCU.				
60	E9	BCU	01300473	2314	This system (BCU2) inactivated because BCU hardware error detected.
	The BCU2 system was inactivated because a hardware failure was detected. [Explanation of message variables] None. [Action] Replace the standby BCU.				
61	E9	BCU	01c00100	2301	BCU restarted because of its HDC update failure.
	The BCU was restarted because updating of the HDC (Hardware Dependent Code) failed. [Explanation of message variables] None. [Action] Replace the BCU.				
62	E9	BCU	25051905	2314	Health check error detected on active BSU *<bsu no.>*. This system (BCU1) is standby.
	An error occurred during a health check performed for the active BSU from the standby BCU1. The BCU1 system is the standby system. [Explanation of message variables] *<bsu no.>*: BSU number [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
63	E9	BCU	25051906	2314	Health check error detected on active BSU *<bsu no.>*. This system (BCU2) is standby.
	An error occurred during a health check performed for the active BSU from the standby BCU2. The BCU2 system is the standby system. [Explanation of message variables] *<bsu no.>*: BSU number [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.				
64	E9	BCU	25051907	2314	Health check error detected on standby BSU *<bsu no.>*. This system (BCU1) is standby.
	An error occurred during a health check performed for the standby BSU from the standby BCU1. The BCU1 system is the standby system. [Explanation of message variables] *<bsu no.>*: BSU number [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.				
65	E9	BCU	25051908	2314	Health check error detected on standby BSU *<bsu no.>*. This system (BCU2) is standby.
	An error occurred during a health check performed for the standby BSU from the standby BCU2. The BCU2 system is the standby system. [Explanation of message variables] *<bsu no.>*: BSU number [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.				
66	E9	BCU	25051909	2314	Health check error detected on NIF *<nif no.>*. This system (BCU1) is standby.
	An error occurred during a health check performed for the NIF from the standby BCU1. The BCU1 system is the standby system. [Explanation of message variables] *<nif no.>*: NIF number [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
67	E9	BCU	25051910	2314	Health check error detected on NIF *<nif no.>*. This system (BCU2) is standby.
	An error occurred during a health check performed for the NIF from the standby BCU2. The BCU2 system is the standby system. [Explanation of message variables] *<nif no.>*: NIF number [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.				
68	R5	BCU	01300430	2314	BCU force-switchover available. This system (BCU1) is active.
	The system switching functionality has recovered. The BCU1 system is the active system. [Explanation of message variables] None. [Action] None.				
69	R5	BCU	01300431	2314	BCU force-switchover available. This system (BCU1) is standby.
	The system switching functionality has recovered. The BCU1 system is the standby system. [Explanation of message variables] None. [Action] None.				
70	R5	BCU	01300432	2314	BCU force-switchover available. This system (BCU2) is active.
	The system switching functionality has recovered. The BCU2 system is the active system. [Explanation of message variables] None. [Action] None.				
71	R5	BCU	01300433	2314	BCU force-switchover available. This system (BCU2) is standby.
	The system switching functionality has recovered. The BCU2 system is the standby system. [Explanation of message variables] None. [Action] None.				
72	R5	BCU	01300434	2314	Health check error recovered. This system (BCU1) is active.
	Recovery from a health check error was successful. The BCU1 system is the active system. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
73	R5	BCU	01300435	2314	Health check error recovered. This system (BCU1) is standby.
	Recovery from a health check error was successful. The BCU1 system is the standby system. [Explanation of message variables] None. [Action] None.				
74	R5	BCU	01300436	2314	Health check error recovered. This system (BCU2) is active.
	Recovery from a health check error was successful. The BCU2 system is the active system. [Explanation of message variables] None. [Action] None.				
75	R5	BCU	01300437	2314	Health check error recovered. This system (BCU2) is standby.
	Recovery from a health check error was successful. The BCU2 system is the standby system. [Explanation of message variables] None. [Action] None.				
76	R5	BCU	01300438	2314	Other system recovered from fatal error. This system (BCU1) is active.
	The standby BCU has recovered from a fatal error. The BCU1 system is the active system. [Explanation of message variables] None. [Action] None.				
77	R5	BCU	01300439	2314	Other system recovered from fatal error. This system (BCU1) is standby.
	The active BCU has recovered from a fatal error. The BCU1 system is the standby system. [Explanation of message variables] None. [Action] None.				
78	R5	BCU	01300440	2314	Other system recovered from fatal error. This system (BCU2) is active.
	The standby BCU has recovered from a fatal error. The BCU2 system is the active system. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
79	R5	BCU	01300441	2314	Other system recovered from fatal error. This system (BCU2) is standby.
	The active BCU has recovered from a fatal error. The BCU2 system is the standby system. [Explanation of message variables] None. [Action] None.				
80	R7	BCU	00020102	2301	The temperature of BCU hardware returned to normal level (5 degree).
	The hardware temperature returned to normal (5 degrees Celsius). The low temperature warning was cleared because the hardware temperature rose to 5 degrees Celsius or higher. [Explanation of message variables] None. [Action] None.				
81	R7	BCU	00020103	2301	The temperature of BCU hardware returned to normal level (40 degree).
	The hardware temperature returned to normal (40 degrees Celsius). [Explanation of message variables] None. [Action] None.				
82	R7	BCU	00020104	2301	BCU hardware recovered to normal from high temperature(55 degree). However, be careful until it is becoming temperature of tolerance level.
	The hardware temperature has been restored from a high temperature value that could affect operation of the switch. However, care must be taken because the temperature is still higher than the allowable range. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
83	R8	BCU	01300461	2314	BCU initialized.
	The BCS has been initialized. [Explanation of message variables] None. [Action] None.				

3.8 Basic switching unit [AX6700S]

3.8.1 Event location = BSU-LA

The following table describes switch failure and event information when the event location is `BSU-LA`.

Table 3-18: Switch failure and event information when the event location is BSU-LA

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
1	E6	BSU-LA	25080200	3280	BSU restarted because of its hardware failure.
	The BSU was restarted because the hardware failed. [Explanation of message variables] None. [Action] After the restart, check the log information to determine if recovery from the failure was successful. If recovery was successful, operations can resume. If recovery failed, replace the BSU.				
2	E6	BSU-LA	25080400	3281	BSU restarted, but not recovered from hardware failure.
	The BSU was restarted although the BUS had not recovered from the hardware failure or a failure detected during self-diagnosis. [Explanation of message variables] None. [Action] Replace the BSU.				
3	R6	BSU-LA	25080200	3280	BSU recovered from hardware failure.
	A BSU has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

3.8.2 Event location = BSU-LB

The following table describes switch failure and event information when the event location is `BSU-LB`.

Table 3-19: Switch failure and event information when the event location is BSU-LB

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
1	E6	BSU-LB	25080200	3380	BSU restarted because of its hardware failure.
	The BSU was restarted because the hardware failed. [Explanation of message variables] None. [Action] After the restart, check the log information to determine if recovery from the failure was successful. If recovery was successful, operations can resume. If recovery failed, replace the BSU.				
2	E6	BSU-LB	25080400	3381	BSU restarted, but not recovered from hardware failure.
	The BSU was restarted although the BUS had not recovered from the hardware failure or a failure detected during self-diagnosis. [Explanation of message variables] None. [Action] Replace the BSU.				
3	R6	BSU-LB	25080200	3380	BSU recovered from hardware failure.
	A BSU has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

3.9 Control and switching unit [AX6600S]

3.9.1 Event location = CSU

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

Table 3-20: Switch failure and event information when the event location is CSU

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
1	E3	CSU	00020106	2301	The temperature of CSU reached the warning level (*<temperature>* degree).
	The hardware temperature has reached the temperature specified by the system temperature-warning-level configuration command. [Explanation of message variables] *<temperature>*: Temperature of the switch (degrees Celsius) [Action] The hardware temperature has reached the specified temperature. Check the environment around the switch (such as the status of the fan, the ventilation, and the existence of any heat sources).					
2	E3	CSU	00020107	2301	The temperature of CSU came down from the warning level.
	The hardware temperature dropped three degrees or more below the the temperature specified by the system temperature-warning-level configuration command. [Explanation of message variables] None. [Action] None.					
3	E3	CSU	01200160	2314	Standby system inactivated because of SOP operation.
	The standby system was placed in the inactive state in response to an inactivate instruction from the system operation panel. [Explanation of message variables] None. [Action] None.					
4	E3	CSU	01200164	2314	Standby system activated because of SOP operation.
	The standby system was released from the inactive state in response to an activate instruction from the system operation panel. [Explanation of message variables] None. [Action] None.					
5	E3	CSU	01200171	2314	This system (CSU1) restarted due to its failure.
	The CSU1 system was restarted because of a failure. [Explanation of message variables] None. [Action] Execute the show logging command with or without the standby parameter specified and check the details of the failure that occurred before this log data was output, and then take action appropriate for the error message.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
6	E3	CSU	01200172	2314	This system (CSU2) restarted due to its failure.
	The CSU2 system was restarted because of a failure. [Explanation of message variables] None. [Action] Execute the `show logging` command with or without the `standby` parameter specified and check the details of the failure that occurred before this log data was output, and then take action appropriate for the error message.					
7	E3	CSU	01200174	2301	Failed in accumulated running time access to *<csu>*.
	Access to the total operating time for the CSU failed. [Explanation of message variables] *<csu>*: CSU for which access to the total operating time failed (either `CSU1` or `CSU2` is displayed) [Action] There are no effects on communication and normal operation. However, the functionality for managing the total operating time cannot be used. If you want to use this functionality, replace the CSU.					
8	E3	CSU	01200180	2301	Fan speed is high because temperature of CSU hardware exceeded tolerance level of high temperature.
	The fan was rotating at high speed because the hardware temperature exceeded the allowable range. [Explanation of message variables] None. [Action] Check and improve the environment such as ventilation and heat sources around the switches.					
9	E3	CSU	01200181	2301	Fan speed is normal because temperature of CSU hardware returned to normal level.
	The fan returned to regular speed because the hardware temperature returned to normal. [Explanation of message variables] None. [Action] None.					
10	E3	CSU	01200182	2301	Recovery due to the failure was restrained.
	The board suppressed recovery because of a failure. [Explanation of message variables] None. [Action] Use the `show logging` or `show logging` command with the `standby` parameter specified to check the log. If a problem is indicated in the log, take appropriate action according to the error message. If recovery of the active system is suppressed, startup (recovery) of the standby system is also suppressed. In this case, there is no need to replace the standby system because a failure has not occurred in the standby system.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
11	E3	CSU	01300408	2314	This system (CSU1) changed from standby to active.CSU2 is standby.
	The CSU1 system was switched from the standby to the active state. CSU2 is the standby system. This message is displayed when system switching occurs due to a fatal error in the former active system, by clicking the Reset button, or by pressing the ACH switch. [Explanation of message variables] None. [Action] 1. There is no problem if the system switching occurred because the Reset button was clicked or the ACH switch was pressed. 2. In all other cases, execute the `show logging` command with the `standby` parameter specified, check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. If the new standby system has not started yet, wait a while before checking for messages.				
12	E3	CSU	01300409	2314	This system (CSU2) changed from standby to active.CSU1 is standby.
	The CSU2 system was switched from the standby to the active state. CSU1 is the standby system. This message is displayed when system switching occurs due to a fatal error in the former active system, by clicking the Reset button, or by pressing the ACH switch. [Explanation of message variables] None. [Action] 1. There is no problem if the system switching occurred because the Reset button was clicked or the ACH switch was pressed. 2. In all other cases, execute the `show logging` command with the `standby` parameter specified, check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. If the new standby system has not started yet, wait a while before checking for messages.				
13	E3	CSU	01300410	2314	This system (CSU1) changed from active to standby.CSU2 is active.
	The CSU1 system was switched from the active to the standby state. CSU2 is the active system. This message is displayed when system switching occurs because of a fatal error in the former active system. [Explanation of message variables] None. [Action] Use the `show logging` command with the `standby` parameter specified to check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. If the new standby system has not started yet, wait a while before checking for messages.				
14	E3	CSU	01300411	2314	This system (CSU2) changed from active to standby.CSU1 is active.
	The CSU2 system was switched from the active to the standby state. CSU1 is the active system. This message is displayed when system switching occurs because of a fatal error in the former active system. [Explanation of message variables] None. [Action] Use the `show logging` command with the `standby` parameter specified to check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. If the new standby system has not started yet, wait a while before checking for messages.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
15	E3	CSU	01300412	2314	System status changed from duplex to simplex.
	The system operating status changed from duplex configuration to single configuration. [Explanation of message variables] None. [Action] None.				
16	E3	CSU	01300413	2314	System status changed from simplex to duplex.
	The system operating status changed from single configuration to duplex configuration. [Explanation of message variables] None. [Action] None.				
17	E3	CSU	01300414	2314	Time is matched at the time of active system.
	The time was matched to the time in the active system. This message is displayed only for the standby system. [Explanation of message variables] None. [Action] None.				
18	E3	CSU	01300417	2314	This system (CSU1) changed from standby to active.CSU2 is standby.
	The CSU1 system was switched from the standby to the active state. CSU2 is the standby system. This message is displayed when system switching occurs because the `reload` command with the `active` parameter specified or the `redundancy force-switchover` command has been executed. [Explanation of message variables] None. [Action] None.				
19	E3	CSU	01300418	2314	This system (CSU2) changed from standby to active.CSU1 is standby.
	The CSU2 system was switched from the standby to the active state. CSU1 is the standby system. This message is displayed when system switching occurs because the `reload` command with the `active` parameter specified or the `redundancy force-switchover` command has been executed. [Explanation of message variables] None. [Action] None.				
20	E3	CSU	01300419	2314	This system (CSU1) changed from active to standby.CSU2 is active.
	The CSU1 system was switched from the active to the standby state. CSU2 is the active system. This message is displayed when system switching occurs because the `reload` command with the `active` parameter specified or the `redundancy force-switchover` command has been executed. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
21	E3	CSU	01300420	2314	This system (CSU2) changed from active to standby.CSU1 is active.
	The CSU2 system was switched from the active to the standby state. CSU1 is the active system. This message is displayed when system switching occurs because the `reload` command with the `active` parameter specified or the `redundancy force-switchover` command has been executed. [Explanation of message variables] None. [Action] None.				
22	E3	CSU	01300421	2314	This system (CSU1) will be changed from active to standby and restarted because of ACH SWITCH pressed.
	The CSU1 system will be switched from the active to the standby state and restarted because the ACH switch was pressed. [Explanation of message variables] None. [Action] None.				
23	E3	CSU	01300422	2314	This system (CSU2) will be changed from active to standby and restarted because of ACH SWITCH pressed.
	The CSU2 system will be switched from the active to the standby state and restarted because the ACH switch was pressed. [Explanation of message variables] None. [Action] None.				
24	E3	CSU	01300442	2314	Partial error detected on other system. Replace unit having error. This system (CSU1) is active.
	A partial failure occurred in the standby CSU. Replace the part in which a failure occurred. The CSU1 system is the active system. [Explanation of message variables] None. [Action] Use the `show logging` command with the `standby` parameter specified to check the message regarding the partial failure that occurred in the standby system, and then take action appropriate for the message.				
25	E3	CSU	01300443	2314	Partial error detected on other system. Replace unit.having error. This system (CSU2) is active.
	A partial failure occurred in the standby CSU. Replace the part in which a failure occurred. The CSU2 system is the active system. [Explanation of message variables] None. [Action] Use the `show logging` command with the `standby` parameter specified to check the message regarding the partial failure that occurred in the standby system, and then take action appropriate for the message.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
26	E3	CSU	01300457	2314	This system (CSU1) restarted with system changed.
	The CSU1 system will be restarted because system switching occurred. This message is displayed when the configuration was inconsistent, the license key was inconsistent, or a dual configuration had not been set up and system switching occurs due to one of the following causes: A fatal error occurred, the Reset button was clicked, the ACH switch was pressed, the `active` parameter was specified in the `reload` command, or the `active` parameter was specified in the `ppupdate` command. [Explanation of message variables] None. [Action] None.				
27	E3	CSU	01300458	2314	This system (CSU2) restarted with system changed.
	The CSU2 system will be restarted because system switching occurred. This message is displayed when the configuration was inconsistent, the license key was inconsistent, or a dual configuration had not been set up and system switching occurs due to one of the following causes: A fatal error occurred, the Reset button was clicked, the ACH switch was pressed, the `active` parameter was specified in the `reload` command, or the `active` parameter was specified in the `ppupdate` command. [Explanation of message variables] None. [Action] None.				
28	E3	CSU	01300466	2314	Other system stopped due to temperature trouble. This system (CSU1) is active.
	The standby system stopped because of a temperature error. The CSU1 system is the active system. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
29	E3	CSU	01300467	2314	Other system stopped due to temperature trouble. This system (CSU1) is standby.
	The active system stopped because of a temperature error. The CSU1 system is the standby system. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
30	E3	CSU	01300468	2314	Other system stopped due to temperature trouble. This system (CSU2) is active.
	The standby system stopped because of a temperature error. The CSU2 system is the active system. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
31	E3	CSU	01300469	2314	Other system stopped due to temperature trouble. This system (CSU2) is standby.
	The active system stopped because of a temperature error. The CSU2 system is the standby system. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.					
32	E3	CSU	01300470	2314	Standby system inactivated because CSU hardware error detected. This system (CSU1) is active.
	The standby system was deactivated because a hardware failure was detected. The CSU1 system is the active system. [Explanation of message variables] None. [Action] Replace the standby CSU.					
33	E3	CSU	01300471	2314	Standby system inactivated because CSU hardware error detected. This system (CSU2) is active.
	The standby system was deactivated because a hardware failure was detected. The CSU2 system is the active system. [Explanation of message variables] None. [Action] Replace the standby CSU.					
34	E3	CSU	01300475	2314	Standby system restarted because CSU hardware error detected. This system (CSU1) is active.
	The standby system was restarted because a hardware failure was detected. The CSU1 system is the active system. [Explanation of message variables] None. [Action] Replace the standby CSU.					
35	E3	CSU	01300476	2314	Standby system restarted because CSU hardware error detected. This system (CSU2) is active.
	The standby system was restarted because a hardware failure was detected. The CSU2 system is the active system. [Explanation of message variables] None. [Action] Replace the standby CSU.					
36	E3	CSU	01300477	2314	Standby system inactivated administratively.
	The standby system was placed in the inactive state by using the `inactivate` command. [Explanation of message variables] None. [Action] None.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
37	E3	CSU	01300478	2314	Standby system activated administratively.
	The standby system was placed in the active state by using the `activate` command. [Explanation of message variables] None. [Action] None.				
38	E3	CSU	01c00200	2301	CSU restarted because of its HDC update done.
	The CSU was restarted because the HDC (Hardware Dependent Code) was updated. [Explanation of message variables] None. [Action] None.				
39	E3	CSU	25070700	2301	PSP online dump command executed.
	The memory dump initiated by executing the PSP dump (without switch restart) command was completed. [Explanation of message variables] None. [Action] None.				
40	E3	CSU	25070701	2301	Can't execute dump command(other dump executing).
	Other dump processing is being performed. [Explanation of message variables] None. [Action] Wait a while and then re-execute the command.				
41	E3	CSU	25070702	2301	PSP dump canceled.
	The PSP dump was canceled. [Explanation of message variables] None. [Action] 1. Use the `show system` command to check the amount of free space in the user area (the recommended amount is 30 MB). If there is not enough free space, delete dump files and then re-execute the command. 2. After other dump processing has been completed, re-execute the command.				
42	E3	CSU	25070800	2301	PSP offline dump command executed.
	The memory dump initiated by executing the PSP dump (with switch restart) command was completed. [Explanation of message variables] None. [Action] None.				
43	E3	CSU	25070911	2301	PSP on this system (CSU1) changed to active.
	The PSP of the CSU1 system was switched to the active state. [Explanation of message variables] None. [Action] Check the CSU log, and take action appropriate for the failure that has occurred. If a command was used to switch the PSP, no action is required.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
44	E3	CSU	25070912	2301	PSP on this system (CSU1) changed from active.
	The PSP of the CSU1 system was switched out of the active state. [Explanation of message variables] None. [Action] Check the CSU log, and take action appropriate for the failure that has occurred. If a command was used to switch the PSP, no action is required.				
45	E3	CSU	25070913	2301	PSP on this system (CSU2) changed to active.
	The PSP of the CSU2 system was switched to the active state. [Explanation of message variables] None. [Action] Check the CSU log, and take action appropriate for the failure that has occurred. If a command was used to switch the PSP, no action is required.				
46	E3	CSU	25070914	2301	PSP on this system (CSU2) changed from active.
	The PSP of the CSU2 system was switched out of the active state. [Explanation of message variables] None. [Action] Check the CSU log, and take action appropriate for the failure that has occurred. If a command was used to switch the PSP, no action is required.				
47	E3	CSU	25070915	2301	PSP on other system (CSU1) changed to active.
	The PSP of the standby system (CSU1) was switched to the active state. [Explanation of message variables] None. [Action] Check the CSU log, and take action appropriate for the failure that has occurred. If a command was used to switch the PSP, no action is required.				
48	E3	CSU	25070916	2301	PSP on other system (CSU1) changed from active.
	The PSP of the standby system (CSU1) was switched out of the active state. [Explanation of message variables] None. [Action] Check the CSU log, and take action appropriate for the failure that has occurred. If a command was used to switch the PSP, no action is required.				
49	E3	CSU	25070917	2301	PSP on other system (CSU2) changed to active.
	The PSP of the standby system (CSU2) was switched to the active state. [Explanation of message variables] None. [Action] Check the CSU log, and take action appropriate for the failure that has occurred. If a command was used to switch the PSP, no action is required.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
50	E3	CSU	25070918	2301	PSP on other system (CSU2) changed from active.
	The PSP of the standby system (CSU2) was switched out of the active state. [Explanation of message variables] None. [Action] Check the CSU log, and take action appropriate for the failure that has occurred. If a command was used to switch the PSP, no action is required.				
51	E5	CSU	01200183	2301	Standby CSU is mismatch.
	The board type of the standby CSU is different. [Explanation of message variables] None. [Action] Make sure that the board types of the active and standby CSUs are the same.				
52	E5	CSU	01200185	2301	Standby CSU is unknown CSU.
	The standby CSU board is unknown. [Explanation of message variables] None. [Action] The CSU board is not supported by the Switch. Replace the standby CSU board.				
53	E5	CSU	01300430	2314	System cannot execute CSU force-switchover. This system (CSU1) is active.
	System switching could not be performed. The CSU1 system is the active system. [Explanation of message variables] None. [Action] Replace both the standby and active CSUs.				
54	E5	CSU	01300432	2314	System cannot execute CSU force-switchover. This system (CSU2) is active.
	System switching could not be performed. The CSU2 system is the active system. [Explanation of message variables] None. [Action] Replace both the standby and active CSUs.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
55	E5	CSU	01300434	2314	Health check error detected on other system. This system (CSU1) is active.
	An error occurred during a health check performed for the standby CSU2 from the active CSU1. The CSU1 system is the active system. [Explanation of message variables] None. [Action] 1. Execute the `show logging` command and make sure that the recovery log message `Health check error recovered.` for this log data has been output. If this message has been output, no action is required. 2. If it has not been output, execute the `show logging` command with the `standby` parameter specified, check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. 3. If no failure has occurred in the standby system, the board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 4. If the problem cannot be corrected after the above actions, replace both the active and standby CSUs.				
56	E5	CSU	01300435	2314	Health check error detected on other system. This system (CSU1) is standby.
	An error occurred during a health check performed for the standby CSU1 from the active CSU2. The CSU1 system is the standby system. [Explanation of message variables] None. [Action] 1. Execute the `show logging` command with the `standby` parameter specified and make sure that the recovery log message `Health check error recovered.` for this log data has been output. If this message has been output, no action is required. 2. If it has not been output, execute the `show logging` command, check the message regarding the failure that occurred in the active system, and then take action appropriate for the message. 3. If no failure has occurred in the active system, the board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 4. If the problem cannot be corrected after the above actions, replace both the active and standby CSUs.				
57	E5	CSU	01300436	2314	Health check error detected on other system. This system (CSU2) is active.
	An error occurred during a health check performed for the standby CSU1 from the active CSU2. The CSU2 system is the active system. [Explanation of message variables] None. [Action] 1. Execute the `show logging` command and make sure that the recovery log message `Health check error recovered.` for this log data has been output. If this message has been output, no action is required. 2. If it has not been output, execute the `show logging` command with the `standby` parameter specified, check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. 3. If no failure has occurred in the standby system, the board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 4. If the problem cannot be corrected after the above actions, replace both the active and standby CSUs.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
58	E5	CSU	01300437	2314	Health check error detected on other system. This system (CSU2) is standby.
	An error occurred during a health check performed for the standby CSU2 from the active CSU1. The CSU2 system is the standby system. [Explanation of message variables] None. [Action] 1. Execute the `show logging` command with the `standby` parameter specified and make sure that the recovery log message `Health check error recovered.` for this log data has been output. If this message has been output, no action is required. 2. If it has not been output, execute the `show logging` command, check the message regarding the failure that occurred in the active system, and then take action appropriate for the message. 3. If no failure has occurred in the active system, the board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 4. If the problem cannot be corrected after the above actions, replace both the active and standby CSUs.				
59	E5	CSU	01300438	2314	Fatal error detected on other system. This system (CSU1) is active.
	A fatal error occurred in the standby CSU. The CSU1 system is the active system. [Explanation of message variables] None. [Action] After the standby system has restarted, execute the `show logging` command with the `standby` parameter specified, check the failure explanation, and then take action appropriate for the error message.				
60	E5	CSU	01300439	2314	Fatal error detected on other system. This system (CSU1) is standby.
	A fatal error occurred in the active CSU. The CSU1 system is the standby system. [Explanation of message variables] None. [Action] After the active system has restarted, execute the `show logging` command, check the failure explanation, and then take action appropriate for the error message.				
61	E5	CSU	01300440	2314	Fatal error detected on other system. This system (CSU2) is active.
	A fatal error occurred in the standby CSU. The CSU2 system is the active system. [Explanation of message variables] None. [Action] After the standby system has restarted, execute the `show logging` command with the `standby` parameter specified, check the failure explanation, and then take action appropriate for the error message.				
62	E5	CSU	01300441	2314	Fatal error detected on other system. This system (CSU2) is standby.
	A fatal error occurred in the active CSU. The CSU2 system is the standby system. [Explanation of message variables] None. [Action] After the active system has restarted, execute the `show logging` command, check the failure explanation, and then take action appropriate for the error message.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
63	E5	CSU	25070913	2301	Health check error detected on active PSP. This system (CSU1) is active.
	An error occurred during a health check performed for the active PSP from the standby CSU2. The CSU1 system is the active system. [Explanation of message variables] None. [Action] After the standby CSU2 has restarted, execute the `show logging` command with the `standby` parameter specified, check the failure explanation, and then take action appropriate for the error message.				
64	E5	CSU	25070914	2301	Health check error detected on active PSP. This system (CSU2) is active.
	An error occurred during a health check performed for the active PSP from the standby CSU1. The CSU2 system is the active system. [Explanation of message variables] None. [Action] After the standby CSU1 has restarted, execute the `show logging` command with the `standby` parameter specified, check the failure explanation, and then take action appropriate for the error message.				
65	E5	CSU	25070919	2301	Health check error detected on NIF *<nif no.>*. This system (CSU1) is active.
	An error occurred during a health check performed for the NIF from the standby CSU2. The CSU1 system is the active system. [Explanation of message variables] *<nif no.>*: NIF number [Action] After the standby CSU2 has restarted, execute the `show logging` command with the `standby` parameter specified, check the failure explanation, and then take action appropriate for the error message.				
66	E5	CSU	25070920	2301	Health check error detected on NIF *<nif no.>*. This system (CSU2) is active.
	An error occurred during a health check performed for the NIF from the standby CSU1. The CSU2 system is the active system. [Explanation of message variables] *<nif no.>*: NIF number [Action] After the standby CSU1 has restarted, execute the `show logging` command with the `standby` parameter specified, check the failure explanation, and then take action appropriate for the error message.				
67	E7	CSU	00020102	2301	CSU hardware exceeded tolerance level of low temperature(2 degree). Check room temperature.
	The hardware temperature dropped below the allowable temperature range (2 degrees Celsius or lower). [Explanation of message variables] None. [Action] 1. Check and improve the environment such as the room temperature around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
68	E7	CSU	00020103	2301	CSU hardware exceeded tolerance level of high temperature (43 degree). Check that room temperature and the fan is operating normally.
	The hardware temperature rose above the allowable temperature range (43 degrees Celsius or higher). [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
69	E7	CSU	00020104	2301	CSU hardware is becoming high temperature (58 degree). immediately, and check that room temperature and the fan is operating normally.
	The hardware temperature is approaching the high temperature value that affects operation of the switch. [Explanation of message variables] None. [Action] 1. A malfunction might occur in the switch. Immediately check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
70	E8	CSU	01200178	2301	PSP not initialized because it is unknown CSU.
	The PSP could not be initialized because the CSU board was unknown. [Explanation of message variables] None. [Action] 1. The CSU board is not fully inserted. Insert the CSU properly. 2. The CSU board is not supported by the software version. Check the CSU board type and the software version, and then either replace the CSU board or update the software. 3. The CSU board is not supported by the Switch. Replace the CSU board.				
71	E8	CSU	01200179	2301	PSP not initialized because it is mismatch between active and standby CSU.
	The PSP could not be initialized because the board types of the active CSU and the standby CSU were different. [Explanation of message variables] None. [Action] Make sure that the board types of the active and standby CSUs are the same.				
72	E8	CSU	25070200	2301	CSU restarted because PSP hardware failure detected during the self diagnosis.
	A failure was detected during PSP self-diagnosis. The CSU will be restarted. [Explanation of message variables] None. [Action] If the log message `PSP initialized.` appears after the restart, operations can resume.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
73	E8	CSU	25070202	2301	CSU restarted because of PSP hardware failure.
	The CSU was restarted because a hardware failure occurred in the PSP. [Explanation of message variables] None. [Action] If the log message `PSP initialized.` appears after the restart, operations can resume.					
74	E8	CSU	25070500	2301	PSP not initialized because it is unavailable configuration.
	Initialization failed because the configuration was unusable. [Explanation of message variables] None. [Action] Change the configuration of the following so that they are correct: • Flow distribution pattern for filtering and the QoS functionality • Distribution pattern for the maximum number of entries per switch					
75	E8	CSU	25070903	2301	Health check error detected on standby PSP. This system (CSU1) is standby.
	An error occurred during a health check performed for the standby PSP from the active CSU2. The CSU1 system is the standby system. [Explanation of message variables] None. [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.					
76	E8	CSU	25070904	2301	Health check error detected on standby PSP. This system (CSU2) is standby.
	An error occurred during a health check performed for the standby PSP from the active CSU1. The CSU2 system is the standby system. [Explanation of message variables] None. [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.					
77	E8	CSU	25070908	2301	System cannot execute PSP swap. All PSP restarted.
	System switching for the PSP could not be performed. All PSPs will be restarted. [Explanation of message variables] None. [Action] None.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
78	E9	CSU	00020105	2301	CSU hardware is becoming high temperature which give damage to this system. (65 degree)
	The hardware temperature has reached a temperature (65 degrees Celsius) that is likely to critically damage device operation. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
79	E9	CSU	01200173 01300474 2b061200	2314	System restarted because CSU hardware error detected.
	The system was restarted because a hardware failure was detected. [Explanation of message variables] None. [Action] Replace the CSU.				
80	E9	CSU	01200186	2301	CSU restarted because it is unknown CSU.
	The CSU will be restarted because the CSU board is unknown. This message is displayed when the active CSU board is unknown and the standby CSU board is normal. [Explanation of message variables] None. [Action] The CSU board is not supported by the Switch. Replace the CSU board.				
81	E9	CSU	01300472	2314	This system (CSU1) inactivated because CSU hardware error detected.
	The CSU1 system was inactivated because a hardware failure was detected. [Explanation of message variables] None. [Action] Replace the standby CSU.				
82	E9	CSU	01300473	2314	This system (CSU2) inactivated because CSU hardware error detected.
	The CSU2 system was inactivated because a hardware failure was detected. [Explanation of message variables] None. [Action] Replace the standby CSU.				
83	E9	CSU	01c00100	2301	CSU restarted because of its HDC update failure.
	The CSU was restarted because updating of the HDC (Hardware Dependent Code) failed. [Explanation of message variables] None. [Action] Replace the CSU.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
84	E9	CSU	25070905	2301	Health check error detected on active PSP. This system (CSU1) is standby.
	An error occurred during a health check performed for the active PSP from the standby CSU1. The CSU1 system is the standby system. [Explanation of message variables] None. [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.				
85	E9	CSU	25070906	2301	Health check error detected on active PSP. This system (CSU2) is standby.
	An error occurred during a health check performed for the active PSP from the standby CSU2. The CSU2 system is the standby system. [Explanation of message variables] None. [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.				
86	E9	CSU	25070909	2301	Health check error detected on NIF *<nif no.>*. This system (CSU1) is standby.
	An error occurred during a health check performed for the NIF from the standby CSU1. The CSU1 system is the standby system. [Explanation of message variables] *<nif no.>*: NIF number [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.				
87	E9	CSU	25070910	2301	Health check error detected on NIF *<nif no.>*. This system (CSU2) is standby.
	An error occurred during a health check performed for the NIF from the standby CSU2. The CSU2 system is the standby system. [Explanation of message variables] *<nif no.>*: NIF number [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
88	R5	CSU	01200185	2301	Standby unknown CSU is notconnect.
	The unknown standby CSU board was removed. This message is displayed when the standby CSU was uninstalled after the log message `Standby CSU is unknown CSU.` was displayed. [Explanation of message variables] None. [Action] None.				
89	R5	CSU	01300430	2314	CSU force-switchover available. This system (CSU1) is active.
	The system switching functionality has recovered. The CSU1 system is the active system. [Explanation of message variables] None. [Action] None.				
90	R5	CSU	01300431	2314	CSU force-switchover available. This system (CSU1) is standby.
	The system switching functionality has recovered. The CSU1 system is the standby system. [Explanation of message variables] None. [Action] None.				
91	R5	CSU	01300432	2314	CSU force-switchover available. This system (CSU2) is active.
	The system switching functionality has recovered. The CSU2 system is the active system. [Explanation of message variables] None. [Action] None.				
92	R5	CSU	01300433	2314	CSU force-switchover available. This system (CSU2) is standby.
	The system switching functionality has recovered. The CSU2 system is the standby system. [Explanation of message variables] None. [Action] None.				
93	R5	CSU	01300434	2314	Health check error recovered. This system (CSU1) is active.
	Recovery from a health check error was successful. The CSU1 system is the active system. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
94	R5	CSU	01300435	2314	Health check error recovered. This system (CSU1) is standby.
	Recovery from a health check error was successful. The CSU1 system is the standby system. [Explanation of message variables] None. [Action] None.				
95	R5	CSU	01300436	2314	Health check error recovered. This system (CSU2) is active.
	Recovery from a health check error was successful. The CSU2 system is the active system. [Explanation of message variables] None. [Action] None.				
96	R5	CSU	01300437	2314	Health check error recovered. This system (CSU2) is standby.
	Recovery from a health check error was successful. The CSU2 system is the standby system. [Explanation of message variables] None. [Action] None.				
97	R5	CSU	01300438	2314	Other system recovered from fatal error. This system (CSU1) is active.
	The standby CSU has recovered from a fatal error. The CSU1 system is the active system. [Explanation of message variables] None. [Action] None.				
98	R5	CSU	01300439	2314	Other system recovered from fatal error. This system (CSU1) is standby.
	The active CSU has recovered from a fatal error. The CSU1 system is the standby system. [Explanation of message variables] None. [Action] None.				
99	R5	CSU	01300440	2314	Other system recovered from fatal error. This system (CSU2) is active.
	The standby CSU has recovered from a fatal error. The CSU2 system is the active system. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
100	R5	CSU	01300441	2314	Other system recovered from fatal error. This system (CSU2) is standby.
	The active CSU has recovered from a fatal error. The CSU2 system is the standby system. [Explanation of message variables] None. [Action] None.				
101	R7	CSU	00020102	2301	The temperature of CSU hardware returned to normal level (5 degree).
	The hardware temperature returned to normal (5 degrees Celsius). [Explanation of message variables] None. [Action] None.				
102	R7	CSU	00020103	2301	The temperature of CSU hardware returned to normal level (40 degree).
	The hardware temperature returned to normal (40 degrees Celsius). [Explanation of message variables] None. [Action] None.				
103	R7	CSU	00020104	2301	CSU hardware recovered to normal from high temperature(55 degree). However, be careful until it is becoming temperature of tolerance level.
	The hardware temperature has been restored from a high temperature value that could affect operation of the switch. However, care must be taken because the temperature is still higher than the allowable range. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
104	R8	CSU	01200179	2301	Standby CSU is notconnect.
	The standby CSU is not installed. This message is displayed when the standby CSU was uninstalled after either of the following log messages was displayed: • PSP not initialized because it is mismatch between active and standby CSU. • Standby CSU is mismatch. [Explanation of message variables] None. [Action] None.				
105	R8	CSU	01300461	2314	CSU initialized.
	The CSU has been initialized. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
106	R8	CSU	25070002	2301	PSP initialized.
	The PSP has been initialized. [Explanation of message variables] None. [Action] None.				

3.10 Management switching unit [AX6300S]

3.10.1 Event location = MSU

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

Table 3-21: Switch failure and event information when the event location is MSU

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
1	E3	MSU	00020106	2301	The temperature of MSU reached the warning level (*<temperature>* degree).
	The hardware temperature has reached the temperature specified by the `system temperature-warning-level` configuration command. [Explanation of message variables] *<temperature>*: Temperature of the switch (degrees Celsius) [Action] The hardware temperature has reached the specified temperature. Check the environment around the switch (such as the status of the fan, the ventilation, and the existence of any heat sources).				
2	E3	MSU	00020107	2301	The temperature of MSU came down from the warning level.
	The hardware temperature dropped three degrees or more below the the temperature specified by the `system temperature-warning-level` configuration command. [Explanation of message variables] None. [Action] None.				
3	E3	MSU	01200160	2314	Standby system inactivated because of SOP operation.
	The standby system was placed in the inactive state in response to an `inactivate` instruction from the system operation panel. [Explanation of message variables] None. [Action] None.				
4	E3	MSU	01200164	2314	Standby system activated because of SOP operation.
	The standby system was released from the inactive state in response to an `activate` instruction from the system operation panel. [Explanation of message variables] None. [Action] None.				
5	E3	MSU	01200171	2314	This system (MSU1) restarted due to its failure.
	The MSU1 system was restarted because of a failure. [Explanation of message variables] None. [Action] Execute the `show logging` command with or without the `standby` parameter specified and check the details of the failure that occurred before this log data was output, and then take action appropriate for the error message.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
6	E3	MSU	01200172	2314	This system (MSU2) restarted due to its failure.
	The MSU2 system was restarted because of a failure. [Explanation of message variables] None. [Action] Execute the `show logging` command with or without the `standby` parameter specified and check the details of the failure that occurred before this log data was output, and then take action appropriate for the error message.					
7	E3	MSU	01200174	2301	Failed in accumulated running time access to <*msu*>.
	Access to the total operating time for the MSU failed. [Explanation of message variables] <*msu*>: MSU for which access to the total operating time failed (either `MSU1` or `MSU2` is displayed) [Action] There are no effects on communication and normal operation. However, the functionality for managing the total operating time cannot be used. If you want to use this functionality, replace the MSU.					
8	E3	MSU	01200180	2301	Fan speed is high because temperature of MSU hardware exceeded tolerance level of high temperature.
	The fan was rotating at high speed because the hardware temperature exceeded the allowable range. [Explanation of message variables] None. [Action] Check and improve the environment such as ventilation and heat sources around the switches.					
9	E3	MSU	01200181	2301	Fan speed is normal because temperature of MSU hardware returned to normal level.
	The fan returned to regular speed because the hardware temperature returned to normal. [Explanation of message variables] None. [Action] None.					
10	E3	MSU	01200182	2301	Recovery due to the failure was restrained.
	The board suppressed recovery because of a failure. [Explanation of message variables] None. [Action] Use the `show logging` or `show logging` command with the `standby` parameter specified to check the log. If a problem is indicated in the log, take appropriate action according to the error message. If recovery of the active system is suppressed, startup (recovery) of the standby system is also suppressed. In this case, there is no need to replace the standby system because a failure has not occurred in the standby system.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
11	E3	MSU	01300408	2314	This system (MSU1) changed from standby to active.MSU2 is standby.
	The MSU1 system was switched from the standby to the active state. MSU2 is the standby system. This message is displayed when system switching occurs due to a fatal error in the former active system, by clicking the Reset button, or by pressing the ACH switch. [Explanation of message variables] None. [Action] 1. There is no problem if the system switching occurred because the Reset button was clicked or the ACH switch was pressed. 2. In all other cases, execute the `show logging` command with the `standby` parameter specified, check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. If the new standby system has not started yet, wait a while before checking for messages.					
12	E3	MSU	01300409	2314	This system (MSU2) changed from standby to active.MSU1 is standby.
	The MSU2 system was switched from the standby to the active state. MSU1 is the standby system. This message is displayed when system switching occurs due to a fatal error in the former active system, by clicking the Reset button, or by pressing the ACH switch. [Explanation of message variables] None. [Action] 1. There is no problem if the system switching occurred because the Reset button was clicked or the ACH switch was pressed. 2. In all other cases, execute the `show logging` command with the `standby` parameter specified, check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. If the new standby system has not started yet, wait a while before checking for messages.					
13	E3	MSU	01300410	2314	This system (MSU1) changed from active to standby.MSU2 is active.
	The MSU1 system was switched from the active to the standby state. MSU2 is the active system. This message is displayed when system switching occurs because of a fatal error in the former active system. [Explanation of message variables] None. [Action] Use the `show logging` command with the `standby` parameter specified to check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. If the new standby system has not started yet, wait a while before checking for messages.					
14	E3	MSU	01300411	2314	This system (MSU2) changed from active to standby.MSU1 is active.
	The MSU2 system was switched from the active to the standby state. MSU1 is the active system. This message is displayed when system switching occurs because of a fatal error in the former active system. [Explanation of message variables] None. [Action] Use the `show logging` command with the `standby` parameter specified to check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. If the new standby system has not started yet, wait a while before checking for messages.					

249

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
15	E3	MSU	01300412	2314	System status changed from duplex to simplex.
	The system operating status changed from duplex configuration to single configuration. [Explanation of message variables] None. [Action] None.				
16	E3	MSU	01300413	2314	System status changed from simplex to duplex.
	The system operating status changed from single configuration to duplex configuration. [Explanation of message variables] None. [Action] None.				
17	E3	MSU	01300414	2314	Time is matched at the time of active system.
	The time was matched to the time in the active system. This message is displayed only for the standby system. [Explanation of message variables] None. [Action] None.				
18	E3	MSU	01300417	2314	This system (MSU1) changed from standby to active.MSU2 is standby.
	The MSU1 system was switched from the standby to the active state. MSU2 is the standby system. This message is displayed when system switching occurs because the `reload` command with the `active` parameter specified or the `redundancy force-switchover` command has been executed. [Explanation of message variables] None. [Action] None.				
19	E3	MSU	01300418	2314	This system (MSU2) changed from standby to active.MSU1 is standby.
	The MSU2 system was switched from the standby to the active state. MSU1 is the standby system. This message is displayed when system switching occurs because the `reload` command with the `active` parameter specified or the `redundancy force-switchover` command has been executed. [Explanation of message variables] None. [Action] None.				
20	E3	MSU	01300419	2314	This system (MSU1) changed from active to standby.MSU2 is active.
	The MSU1 system was switched from the active to the standby state. MSU2 is the active system. This message is displayed when system switching occurs because the `reload` command with the `active` parameter specified or the `redundancy force-switchover` command has been executed. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
21	E3	MSU	01300420	2314	This system (MSU2) changed from active to standby.MSU1 is active.
	The MSU2 system was switched from the active to the standby state. MSU1 is the active system. This message is displayed when system switching occurs because the `reload` command with the `active` parameter specified or the `redundancy force-switchover` command has been executed. [Explanation of message variables] None. [Action] None.				
22	E3	MSU	01300421	2314	This system (MSU1) will be changed from active to standby and restarted because of ACH SWITCH pressed.
	The MSU1 system will be switched from the active to the standby state and restarted because the ACH switch was pressed. [Explanation of message variables] None. [Action] None.				
23	E3	MSU	01300422	2314	This system (MSU2) will be changed from active to standby and restarted because of ACH SWITCH pressed.
	The MSU2 system will be switched from the active to the standby state and restarted because the ACH switch was pressed. [Explanation of message variables] None. [Action] None.				
24	E3	MSU	01300442	2314	Partial error detected on other system. Replace unit having error. This system (MSU1) is active.
	A partial failure occurred in the standby MSU. Replace the part in which a failure occurred. The MSU1 system is the active system. [Explanation of message variables] None. [Action] Use the `show logging` command with the `standby` parameter specified to check the message regarding the partial failure that occurred in the standby system, and then take action appropriate for the message.				
25	E3	MSU	01300443	2314	Partial error detected on other system. Replace unit.having error. This system (MSU2) is active.
	A partial failure occurred in the standby MSU. Replace the part in which a failure occurred. The MSU2 system is the active system. [Explanation of message variables] None. [Action] Use the `show logging` command with the `standby` parameter specified to check the message regarding the partial failure that occurred in the standby system, and then take action appropriate for the message.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
26	E3	MSU	01300457	2314	This system (MSU1) restarted with system changed.
	The MSU1 system will be restarted because system switching occurred. This message is displayed when the configuration was inconsistent, the license key was inconsistent, or a dual configuration had not been set up and system switching occurs due to one of the following causes: A fatal error occurred, the Reset button was clicked, the ACH switch was pressed, the `active` parameter was specified in the `reload` command, or the `active` parameter was specified in the `ppupdate` command. [Explanation of message variables] None. [Action] None.				
27	E3	MSU	01300458	2314	This system (MSU2) restarted with system changed.
	The MSU2 system will be restarted because system switching occurred. This message is displayed when the configuration was inconsistent, the license key was inconsistent, or a dual configuration had not been set up and system switching occurs due to one of the following causes: A fatal error occurred, the Reset button was clicked, the ACH switch was pressed, the `active` parameter was specified in the `reload` command, or the `active` parameter was specified in the `ppupdate` command. [Explanation of message variables] None. [Action] None.				
28	E3	MSU	01300466	2314	Other system stopped due to temperature trouble. This system (MSU1) is active.
	The standby system stopped because of a temperature error. The MSU1 system is the active system. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
29	E3	MSU	01300467	2314	Other system stopped due to temperature trouble. This system (MSU1) is standby.
	The active system stopped because of a temperature error. The MSU1 system is the standby system. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
30	E3	MSU	01300468	2314	Other system stopped due to temperature trouble. This system (MSU2) is active.
	The standby system stopped because of a temperature error. The MSU2 system is the active system. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
31	E3	MSU	01300469	2314	Other system stopped due to temperature trouble. This system (MSU2) is standby.
	The active system stopped because of a temperature error. The MSU2 system is the standby system. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
32	E3	MSU	01300470	2314	Standby system inactivated because MSU hardware error detected. This system (MSU1) is active.
	The standby system was deactivated because a hardware failure was detected. The MSU1 system is the active system. [Explanation of message variables] None. [Action] Replace the standby MSU.				
33	E3	MSU	01300471	2314	Standby system inactivated because MSU hardware error detected. This system (MSU2) is active.
	The standby system was deactivated because a hardware failure was detected. The MSU2 system is the active system. [Explanation of message variables] None. [Action] Replace the standby MSU.				
34	E3	MSU	01300475	2314	Standby system restarted because MSU hardware error detected. This system (MSU1) is active.
	The standby system was restarted because a hardware failure was detected. The MSU1 system is the active system. [Explanation of message variables] None. [Action] Replace the standby MSU.				
35	E3	MSU	01300476	2314	Standby system restarted because MSU hardware error detected. This system (MSU2) is active.
	The standby system was restarted because a hardware failure was detected. The MSU2 system is the active system. [Explanation of message variables] None. [Action] Replace the standby MSU.				
36	E3	MSU	01300477	2314	Standby system inactivated administratively.
	The standby system was placed in the inactive state by using the `inactivate` command. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
37	E3	MSU	01300478	2314	Standby system activated administratively.
	The standby system was placed in the active state by using the `activate` command. [Explanation of message variables] None. [Action] None.				
38	E3	MSU	01c00200	2301	MSU restarted because of its HDC update done.
	The MSU was restarted because the HDC (Hardware Dependent Code) was updated. [Explanation of message variables] None. [Action] None.				
39	E3	MSU	25070700	2301	PSP online dump command executed.
	The memory dump initiated by executing the PSP dump (without switch restart) command was completed. [Explanation of message variables] None. [Action] None.				
40	E3	MSU	25070701	2301	Can't execute dump command(other dump executing).
	Other dump processing is being performed. [Explanation of message variables] None. [Action] Wait a while and then re-execute the command.				
41	E3	MSU	25070702	2301	PSP dump canceled.
	The PSP dump was canceled. [Explanation of message variables] None. [Action] 1. Use the `show system` command to check the amount of free space in the user area (the recommended amount is 30 MB). If there is not enough free space, delete dump files and then re-execute the command. 2. After other dump processing has been completed, re-execute the command.				
42	E3	MSU	25070800	2301	PSP offline dump command executed.
	The memory dump initiated by executing the PSP dump (with switch restart) command was completed. [Explanation of message variables] None. [Action] None.				
43	E5	MSU	01200183	2301	Standby MSU is mismatch.
	The board type of the standby MSU is different. [Explanation of message variables] None. [Action] Make sure that the board types of the active and standby MSUs are the same.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
44	E5	MSU	01200185	2301	Standby MSU is unknown MSU.
	The standby MSU board is unknown. [Explanation of message variables] None. [Action] The MSU board is not supported by the Switch. Replace the standby MSU board.				
45	E5	MSU	01300430	2314	System cannot execute MSU force-switchover. This system (MSU1) is active.
	System switching could not be performed. The MSU1 system is the active system. [Explanation of message variables] None. [Action] Replace both the standby and active MSUs.				
46	E5	MSU	01300432	2314	System cannot execute MSU force-switchover. This system (MSU2) is active.
	System switching could not be performed. The MSU2 system is the active system. [Explanation of message variables] None. [Action] Replace both the standby and active MSUs.				
47	E5	MSU	01300434	2314	Health check error detected on other system. This system (MSU1) is active.
	An error occurred during a health check performed for the standby MSU2 from the active MSU1. The MSU1 system is the active system. [Explanation of message variables] None. [Action] 1. Execute the `show logging` command and make sure that the recovery log message `Health check error recovered.` for this log data has been output. If this message has been output, no action is required. 2. If it has not been output, execute the `show logging` command with the `standby` parameter specified, check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. 3. If no failure has occurred in the standby system, the board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 4. If the problem cannot be corrected after the above actions, replace both the active and standby MSUs.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
48	E5	MSU	01300435	2314	Health check error detected on other system. This system (MSU1) is standby.
	An error occurred during a health check performed for the standby MSU1 from the active MSU2. The MSU1 system is the standby system. [Explanation of message variables] None. [Action] 1. Execute the `show logging` command with the `standby` parameter specified and make sure that the recovery log message `Health check error recovered.` for this log data has been output. If this message has been output, no action is required. 2. If it has not been output, execute the `show logging` command, check the message regarding the failure that occurred in the active system, and then take action appropriate for the message. 3. If no failure has occurred in the active system, the board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 4. If the problem cannot be corrected after the above actions, replace both the active and standby MSUs.					
49	E5	MSU	01300436	2314	Health check error detected on other system. This system (MSU2) is active.
	An error occurred during a health check performed for the standby MSU1 from the active MSU2. The MSU2 system is the active system. [Explanation of message variables] None. [Action] 1. Execute the `show logging` command and make sure that the recovery log message `Health check error recovered.` for this log data has been output. If this message has been output, no action is required. 2. If it has not been output, execute the `show logging` command with the `standby` parameter specified, check the message regarding the failure that occurred in the standby system, and then take action appropriate for the message. 3. If no failure has occurred in the standby system, the board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 4. If the problem cannot be corrected after the above actions, replace both the active and standby MSUs.					
50	E5	MSU	01300437	2314	Health check error detected on other system. This system (MSU2) is standby.
	An error occurred during a health check performed for the standby MSU2 from the active MSU1. The MSU2 system is the standby system. [Explanation of message variables] None. [Action] 1. Execute the `show logging` command with the `standby` parameter specified and make sure that the recovery log message `Health check error recovered.` for this log data has been output. If this message has been output, no action is required. 2. If it has not been output, execute the `show logging` command, check the message regarding the failure that occurred in the active system, and then take action appropriate for the message. 3. If no failure has occurred in the active system, the board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 4. If the problem cannot be corrected after the above actions, replace both the active and standby MSUs.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
51	E5	MSU	01300438	2314	Fatal error detected on other system. This system (MSU1) is active.
	A fatal error occurred in the standby MSU. The MSU1 system is the active system. [Explanation of message variables] None. [Action] After the standby system has restarted, execute the show logging command with the standby parameter specified, check the failure explanation, and then take action appropriate for the error message.				
52	E5	MSU	01300439	2314	Fatal error detected on other system. This system (MSU1) is standby.
	A fatal error occurred in the active MSU. The MSU1 system is the standby system. [Explanation of message variables] None. [Action] After the active system has restarted, execute the show logging command, check the failure explanation, and then take action appropriate for the error message.				
53	E5	MSU	01300440	2314	Fatal error detected on other system. This system (MSU2) is active.
	A fatal error occurred in the standby MSU. The MSU2 system is the active system. [Explanation of message variables] None. [Action] After the standby system has restarted, execute the show logging command with the standby parameter specified, check the failure explanation, and then take action appropriate for the error message.				
54	E5	MSU	01300441	2314	Fatal error detected on other system. This system (MSU2) is standby.
	A fatal error occurred in the active MSU. The MSU2 system is the standby system. [Explanation of message variables] None. [Action] After the active system has restarted, execute the show logging command, check the failure explanation, and then take action appropriate for the error message.				
55	E5	MSU	25070913	2301	Health check error detected on active PSP. This system (MSU1) is active.
	An error occurred during a health check performed for the active PSP from the standby MSU2. The MSU1 system is the active system. [Explanation of message variables] None. [Action] After the standby MSU2 has restarted, execute the show logging command with the standby parameter specified, check the failure explanation, and then take action appropriate for the error message.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
56	E5	MSU	25070914	2301	Health check error detected on active PSP. This system (MSU2) is active.
	An error occurred during a health check performed for the active PSP from the standby MSU1. The MSU2 system is the active system. [Explanation of message variables] None. [Action] After the standby MSU1 has restarted, execute the `show logging` command with the `standby` parameter specified, check the failure explanation, and then take action appropriate for the error message.				
57	E5	MSU	25070919	2301	Health check error detected on NIF *<nif no.>*. This system (MSU1) is active.
	An error occurred during a health check performed for the NIF from the standby MSU2. The MSU1 system is the active system. [Explanation of message variables] *<nif no.>*: NIF number [Action] After the standby MSU2 has restarted, execute the `show logging` command with the `standby` parameter specified, check the failure explanation, and then take action appropriate for the error message.				
58	E5	MSU	25070920	2301	Health check error detected on NIF *<nif no.>*. This system (MSU2) is active.
	An error occurred during a health check performed for the NIF from the standby MSU1. The MSU2 system is the active system. [Explanation of message variables] *<nif no.>*: NIF number [Action] After the standby MSU1 has restarted, execute the `show logging` command with the `standby` parameter specified, check the failure explanation, and then take action appropriate for the error message.				
59	E7	MSU	00020102	2301	MSU hardware exceeded tolerance level of low temperature(2 degree). Check room temperature.
	The hardware temperature dropped below the allowable temperature range (2 degrees Celsius or lower). [Explanation of message variables] None. [Action] 1. Check and improve the environment such as the room temperature around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
60	E7	MSU	00020103	2301	MSU hardware exceeded tolerance level of high temperature (43 degree). Check that room temperature and the fan is operating normally.
	The hardware temperature rose above the allowable temperature range (43 degrees Celsius or higher). [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
61	E7	MSU	00020104	2301	MSU hardware is becoming high temperature (58 degree). immediately, and check that room temperature and the fan is operating normally.
	The hardware temperature is approaching the high temperature value that affects operation of the switch. [Explanation of message variables] None. [Action] 1. A malfunction might occur in the switch. Immediately check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.					
62	E8	MSU	01200178	2301	PSP not initialized because it is unknown MSU.
	The PSP could not be initialized because the MSU board was unknown. [Explanation of message variables] None. [Action] 1. The MSU board is not fully inserted. Insert the MSU properly. 2. The MSU board is not supported by the software version. Check the MSU board type and the software version, and then either replace the MSU board or update the software. 3. The MSU board is not supported by the Switch. Replace the MSU board.					
63	E8	MSU	01200179	2301	PSP not initialized because it is mismatch between active and standby MSU.
	The PSP could not be initialized because the board types of the active MSU and the standby MSU were different. [Explanation of message variables] None. [Action] Make sure that the board types of the active and standby MSUs are the same.					
64	E8	MSU	25070200	2301	MSU restarted because PSP hardware failure detected during the self diagnosis.
	A failure was detected during PSP self-diagnosis. The MSU will be restarted. [Explanation of message variables] None. [Action] If the log message `PSP initialized.` appears after the restart, operations can resume.					
65	E8	MSU	25070202	2301	MSU restarted because of PSP hardware failure.
	The MSU was restarted because a hardware failure occurred in the PSP. [Explanation of message variables] None. [Action] If the log message `PSP initialized.` appears after the restart, operations can resume.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
66	E8	MSU	25070500	2301	PSP not initialized because it is unavailable configuration.
	Initialization failed because the configuration was unusable. [Explanation of message variables] None. [Action] Change the configuration of the following so that they are correct: • Flow distribution pattern for filtering and the QoS functionality • Distribution pattern for the maximum number of entries per switch					
67	E8	MSU	25070903	2301	Health check error detected on standby PSP. This system (MSU1) is standby.
	An error occurred during a health check performed for the standby PSP from the active MSU2. The MSU1 system is the standby system. [Explanation of message variables] None. [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.					
68	E8	MSU	25070904	2301	Health check error detected on standby PSP. This system (MSU2) is standby.
	An error occurred during a health check performed for the standby PSP from the active MSU1. The MSU2 system is the standby system. [Explanation of message variables] None. [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.					
69	E9	MSU	00020105	2301	MSU hardware is becoming high temperature which give damage to this system. (65 degree)
	The hardware temperature has reached a temperature (65 degrees Celsius) that is likely to critically damage device operation. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.					
70	E9	MSU	01200173 01300474 2b061200	2314	System restarted because MSU hardware error detected.
	The system was restarted because a hardware failure was detected. [Explanation of message variables] None. [Action] Replace the MSU.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
71	E9	MSU	01200186	2301	MSU restarted because it is unknown MSU.
	The MSU will be restarted because the MSU board is unknown. This message is displayed when the active MSU board is unknown and the standby MSU board is normal. [Explanation of message variables] None. [Action] The MSU board is not supported by the Switch. Replace the MSU board.				
72	E9	MSU	01300472	2314	This system (MSU1) inactivated because MSU hardware error detected.
	The MSU1 system was inactivated because a hardware failure was detected. [Explanation of message variables] None. [Action] Replace the standby MSU.				
73	E9	MSU	01300473	2314	This system (MSU2) inactivated because MSU hardware error detected.
	The MSU2 system was inactivated because a hardware failure was detected. [Explanation of message variables] None. [Action] Replace the standby MSU.				
74	E9	MSU	01c00100	2301	MSU restarted because of its HDC update failure.
	The MSU was restarted because updating of the HDC (Hardware Dependent Code) failed. [Explanation of message variables] None. [Action] Replace the MSU.				
75	E9	MSU	25070905	2301	Health check error detected on active PSP. This system (MSU1) is standby.
	An error occurred during a health check performed for the active PSP from the standby MSU1. The MSU1 system is the standby system. [Explanation of message variables] None. [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
76	E9	MSU	25070906	2301	Health check error detected on active PSP. This system (MSU2) is standby.
	An error occurred during a health check performed for the active PSP from the standby MSU2. The MSU2 system is the standby system. [Explanation of message variables] None. [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.				
77	E9	MSU	25070909	2301	Health check error detected on NIF *<nif no.>*. This system (MSU1) is standby.
	An error occurred during a health check performed for the NIF from the standby MSU1. The MSU1 system is the standby system. [Explanation of message variables] *<nif no.>*: NIF number [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.				
78	E9	MSU	25070910	2301	Health check error detected on NIF *<nif no.>*. This system (MSU2) is standby.
	An error occurred during a health check performed for the NIF from the standby MSU2. The MSU2 system is the standby system. [Explanation of message variables] *<nif no.>*: NIF number [Action] 1. The board might not be fully inserted. If this message is displayed immediately after the board is replaced, check that it is properly inserted. 2. If the problem cannot be corrected after the above action, see the *Troubleshooting Guide* and take appropriate action.				
79	R5	MSU	01200185	2301	Standby unknown MSU is notconnect.
	The unknown standby MSU board was removed. This message is displayed when the standby MSU was uninstalled after the log message `Standby MSU is unknown MSU.` was displayed. [Explanation of message variables] None. [Action] None.				
80	R5	MSU	01300430	2314	MSU force-switchover available. This system (MSU1) is active.
	The system switching functionality has recovered. The MSU1 system is the active system. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
81	R5	MSU	01300431	2314	MSU force-switchover available. This system (MSU1) is standby.
	The system switching functionality has recovered. The MSU1 system is the standby system. [Explanation of message variables] None. [Action] None.				
82	R5	MSU	01300432	2314	MSU force-switchover available. This system (MSU2) is active.
	The system switching functionality has recovered. The MSU2 system is the active system. [Explanation of message variables] None. [Action] None.				
83	R5	MSU	01300433	2314	MSU force-switchover available. This system (MSU2) is standby.
	The system switching functionality has recovered. The MSU2 system is the standby system. [Explanation of message variables] None. [Action] None.				
84	R5	MSU	01300434	2314	Health check error recovered. This system (MSU1) is active.
	Recovery from a health check error was successful. The MSU1 system is the active system. [Explanation of message variables] None. [Action] None.				
85	R5	MSU	01300435	2314	Health check error recovered. This system (MSU1) is standby.
	Recovery from a health check error was successful. The MSU1 system is the standby system. [Explanation of message variables] None. [Action] None.				
86	R5	MSU	01300436	2314	Health check error recovered. This system (MSU2) is active.
	Recovery from a health check error was successful. The MSU2 system is the active system. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
Description					
87	R5	MSU	01300437	2314	Health check error recovered. This system (MSU2) is standby.
Recovery from a health check error was successful. The MSU2 system is the standby system. [Explanation of message variables] None. [Action] None.					
88	R5	MSU	01300438	2314	Other system recovered from fatal error. This system (MSU1) is active.
The standby MSU has recovered from a fatal error. The MSU1 system is the active system. [Explanation of message variables] None. [Action] None.					
89	R5	MSU	01300439	2314	Other system recovered from fatal error. This system (MSU1) is standby.
The active MSU has recovered from a fatal error. The MSU1 system is the standby system. [Explanation of message variables] None. [Action] None.					
90	R5	MSU	01300440	2314	Other system recovered from fatal error. This system (MSU2) is active.
The standby MSU has recovered from a fatal error. The MSU2 system is the active system. [Explanation of message variables] None. [Action] None.					
91	R5	MSU	01300441	2314	Other system recovered from fatal error. This system (MSU2) is standby.
The active MSU has recovered from a fatal error. The MSU2 system is the standby system. [Explanation of message variables] None. [Action] None.					
92	R7	MSU	00020102	2301	The temperature of MSU hardware returned to normal level (5 degree).
The hardware temperature returned to normal (5 degrees Celsius). [Explanation of message variables] None. [Action] None.					

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
93	R7	MSU	00020103	2301	The temperature of MSU hardware returned to normal level (40 degree).
	The hardware temperature returned to normal (40 degrees Celsius). [Explanation of message variables] None. [Action] None.				
94	R7	MSU	00020104	2301	MSU hardware recovered to normal from high temperature(55 degree). However, be careful until it is becoming temperature of tolerance level.
	The hardware temperature has been restored from a high temperature value that could affect operation of the switch. However, care must be taken because the temperature is still higher than the allowable range. [Explanation of message variables] None. [Action] 1. Check and improve the environment such as ventilation and heat sources around the switches. 2. Check the fans. If a failure has occurred, replace the fan unit containing the faulty fan.				
95	R8	MSU	01200179	2301	Standby MSU is notconnect.
	The standby MSU is not installed. This message is displayed when the standby MSU was uninstalled after either of the following log messages was displayed: • PSP not initialized because it is mismatch between active and standby MSU. • Standby MSU is mismatch. [Explanation of message variables] None. [Action] None.				
96	R8	MSU	01300461	2314	MSU initialized.
	The MSU has been initialized. [Explanation of message variables] None. [Action] None.				
97	R8	MSU	25070002	2301	PSP initialized.
	The PSP has been initialized. [Explanation of message variables] None. [Action] None.				

3.11 AX6700S and AX6600S series network interface unit [AX6700S] [AX6600S]

3.11.1 Event location = NK1G-24T

The following table describes switch failure and event information when the event location is NK1G-24T.

Table 3-22: Switch failure and event information when the event location is NK1G-24T

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
1	E6	NK1G-24T	25020200	5540	NIF restarted because of its hardware failure.
	The NIF was restarted because the NIF hardware failed. [Explanation of message variables] None. [Action] Check for subsequent fault recoveries or fault recovery failure log entries. If recovery was successful, operations can resume. If recovery failed, replace the NIF.				
2	E6	NK1G-24T	25020201	5550	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 recovery failed, replace the NIF.				
3	E6	NK1G-24T	25020400	5540	NIF restarted, but not recovered from hardware failure.
	The NIF was restarted although the NIF had not recovered from the hardware failure or a failure detected during self-diagnosis. [Explanation of message variables] None. [Action] Replace the NIF.				
4	E6	NK1G-24T	25020401	5550	Port restarted, but not recovered from hardware failure.
	A port was restarted, but it has not recovered from a hardware failure. [Explanation of message variables] None. [Action] Replace the NIF.				
5	R6	NK1G-24T	25020200	5540	NIF recovered from hardware failure.
	A NIF has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
			Description		
6	R6	NK1G-24T	25020201	5550	Port recovered from hardware failure.
	A port has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

3.11.2 Event location = NK1G-24S

The following table describes switch failure and event information when the event location is NK1G-24S.

Table 3-23: Switch failure and event information when the event location is NK1G-24S

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
			Description		
1	E6	NK1G-24S	25020200	5640	NIF restarted because of its hardware failure.
	The NIF was restarted because the NIF hardware failed. [Explanation of message variables] None. [Action] Check for subsequent fault recoveries or fault recovery failure log entries. If recovery was successful, operations can resume. If recovery failed, replace the NIF.				
2	E6	NK1G-24S	25020201	5650	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 recovery failed, replace the NIF.				
3	E6	NK1G-24S	25020400	5640	NIF restarted, but not recovered from hardware failure.
	The NIF was restarted although the NIF had not recovered from the hardware failure or a failure detected during self-diagnosis. [Explanation of message variables] None. [Action] Replace the NIF.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
4	E6	NK1G-24S	25020401	5650	Port restarted, but not recovered from hardware failure.
	A port was restarted, but it has not recovered from a hardware failure. [Explanation of message variables] None. [Action] Replace the NIF.				
5	R6	NK1G-24S	25020200	5640	NIF recovered from hardware failure.
	A NIF has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				
6	R6	NK1G-24S	25020201	5650	Port recovered from hardware failure.
	A port has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

3.11.3 Event location = NK1GS-8M

The following table describes switch failure and event information when the event location is NK1GS-8M.

Table 3-24: Switch failure and event information when the event location is NK1GS-8M

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
1	E6	NK1GS-8M	25020200	5940	NIF restarted because of its hardware failure.
	The NIF was restarted because the NIF hardware failed. [Explanation of message variables] None. [Action] Check for subsequent fault recoveries or fault recovery failure log entries. If recovery was successful, operations can resume. If recovery failed, replace the NIF.				
2	E6	NK1GS-8M	25020400	5940	NIF restarted, but not recovered from hardware failure.
	The NIF was restarted although the NIF had not recovered from the hardware failure or a failure detected during self-diagnosis. [Explanation of message variables] None. [Action] Replace the NIF.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
3	R6	NK1GS-8M	25020200	5940	NIF recovered from hardware failure.
	A NIF has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

3.11.4 Event location = NK10G-4RX

The following table describes switch failure and event information when the event location is `NK10G-4RX`.

Table 3-25: Switch failure and event information when the event location is NK10G-4RX

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
1	E6	NK10G-4RX	25020200	5340	NIF restarted because of its hardware failure.
	The NIF was restarted because the NIF hardware failed. [Explanation of message variables] None. [Action] Check for subsequent fault recoveries or fault recovery failure log entries. If recovery was successful, operations can resume. If recovery failed, replace the NIF.				
2	E6	NK10G-4RX	25020201	5350	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 recovery failed, replace the NIF.				
3	E6	NK10G-4RX	25020400	5340	NIF restarted, but not recovered from hardware failure.
	The NIF was restarted although the NIF had not recovered from the hardware failure or a failure detected during self-diagnosis. [Explanation of message variables] None. [Action] Replace the NIF.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
4	E6	NK10G-4RX	25020401	5350	Port restarted, but not recovered from hardware failure.
	A port was restarted, but it has not recovered from a hardware failure. [Explanation of message variables] None. [Action] Replace the NIF.				
5	R6	NK10G-4RX	25020200	5340	NIF recovered from hardware failure.
	A NIF has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				
6	R6	NK10G-4RX	25020201	5350	Port recovered from hardware failure.
	A port has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

3.11.5 Event location = NK10G-8RX

The following table describes switch failure and event information when the event location is `NK10G-8RX`.

Table 3-26: Switch failure and event information when the event location is NK10G-8RX

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
1	E6	NK10G-8RX	25020200	5440	NIF restarted because of its hardware failure.
	The NIF was restarted because the NIF hardware failed. [Explanation of message variables] None. [Action] Check for subsequent fault recoveries or fault recovery failure log entries. If recovery was successful, operations can resume. If recovery failed, replace the NIF.				
2	E6	NK10G-8RX	25020201	5450	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 recovery failed, replace the NIF.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
3	E6	NK10G-8RX	25020400	5440	NIF restarted, but not recovered from hardware failure.
	The NIF was restarted although the NIF had not recovered from the hardware failure or a failure detected during self-diagnosis. [Explanation of message variables] None. [Action] Replace the NIF.				
4	E6	NK10G-8RX	25020401	5450	Port restarted, but not recovered from hardware failure.
	A port was restarted, but it has not recovered from a hardware failure. [Explanation of message variables] None. [Action] Replace the NIF.				
5	R6	NK10G-8RX	25020200	5440	NIF recovered from hardware failure.
	A NIF has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				
6	R6	NK10G-8RX	25020201	5450	Port recovered from hardware failure.
	A port has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

3.12 AX6300S series network interface unit [AX6300S]

3.12.1 Event location = NH1G-16S

The following table describes switch failure and event information when the event location is
`NH1G-16S`.

Table 3-27: Switch failure and event information when the event location is NH1G-16S

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
1	E6	NH1G-16S	25020200	5140	NIF restarted because of its hardware failure.
	The NIF was restarted because the NIF hardware failed. [Explanation of message variables] None. [Action] Check for subsequent fault recoveries or fault recovery failure log entries. If recovery was successful, operations can resume. If recovery failed, replace the NIF.				
2	E6	NH1G-16S	25020201	5150	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 recovery failed, replace the NIF.				
3	E6	NH1G-16S	25020400	5140	NIF restarted, but not recovered from hardware failure.
	The NIF was restarted although the NIF had not recovered from the hardware failure or a failure detected during self-diagnosis. [Explanation of message variables] None. [Action] Replace the NIF.				
4	E6	NH1G-16S	25020401	5150	Port restarted, but not recovered from hardware failure.
	A port was restarted, but it has not recovered from a hardware failure. [Explanation of message variables] None. [Action] Replace the NIF.				
5	R6	NH1G-16S	25020200	5140	NIF recovered from hardware failure.
	A NIF has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
			Description		
6	R6	NH1G-16S	25020201	5150	Port recovered from hardware failure.
	A port has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

3.12.2 Event location = NH1G-24T

The following table describes switch failure and event information when the event location is `NH1G-24T`.

Table 3-28: Switch failure and event information when the event location is NH1G-24T

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
			Description		
1	E6	NH1G-24T	25020200	5540	NIF restarted because of its hardware failure.
	The NIF was restarted because the NIF hardware failed. [Explanation of message variables] None. [Action] Check for subsequent fault recoveries or fault recovery failure log entries. If recovery was successful, operations can resume. If recovery failed, replace the NIF.				
2	E6	NH1G-24T	25020201	5550	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 recovery failed, replace the NIF.				
3	E6	NH1G-24T	25020400	5540	NIF restarted, but not recovered from hardware failure.
	The NIF was restarted although the NIF had not recovered from the hardware failure or a failure detected during self-diagnosis. [Explanation of message variables] None. [Action] Replace the NIF.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
4	E6	NH1G-24T	25020401	5550	Port restarted, but not recovered from hardware failure.
	A port was restarted, but it has not recovered from a hardware failure. [Explanation of message variables] None. [Action] Replace the NIF.				
5	R6	NH1G-24T	25020200	5540	NIF recovered from hardware failure.
	A NIF has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				
6	R6	NH1G-24T	25020201	5550	Port recovered from hardware failure.
	A port has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

3.12.3 Event location = NH1G-24S

The following table describes switch failure and event information when the event location is NH1G-24S.

Table 3-29: Switch failure and event information when the event location is NH1G-24S

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
1	E6	NH1G-24S	25020200	5640	NIF restarted because of its hardware failure.
	The NIF was restarted because the NIF hardware failed. [Explanation of message variables] None. [Action] Check for subsequent fault recoveries or fault recovery failure log entries. If recovery was successful, operations can resume. If recovery failed, replace the NIF.				
2	E6	NH1G-24S	25020201	5650	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 recovery failed, replace the NIF.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
3	E6	NH1G-24S	25020400	5640	NIF restarted, but not recovered from hardware failure.
	The NIF was restarted although the NIF had not recovered from the hardware failure or a failure detected during self-diagnosis. [Explanation of message variables] None. [Action] Replace the NIF.				
4	E6	NH1G-24S	25020401	5650	Port restarted, but not recovered from hardware failure.
	A port was restarted, but it has not recovered from a hardware failure. [Explanation of message variables] None. [Action] Replace the NIF.				
5	R6	NH1G-24S	25020200	5640	NIF recovered from hardware failure.
	A NIF has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				
6	R6	NH1G-24S	25020201	5650	Port recovered from hardware failure.
	A port has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

3.12.4 Event location = NH1G-48T

The following table describes switch failure and event information when the event location is NH1G-48T.

Table 3-30: Switch failure and event information when the event location is NH1G-48T

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
1	E6	NH1G-48T	25020200	5040	NIF restarted because of its hardware failure.
	The NIF was restarted because the NIF hardware failed. [Explanation of message variables] None. [Action] Check for subsequent fault recoveries or fault recovery failure log entries. If recovery was successful, operations can resume. If recovery failed, replace the NIF.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
2	E6	NH1G-48T	25020201	5050	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 recovery failed, replace the NIF.					
3	E6	NH1G-48T	25020400	5040	NIF restarted, but not recovered from hardware failure.
	The NIF was restarted although the NIF had not recovered from the hardware failure or a failure detected during self-diagnosis. [Explanation of message variables] None. [Action] Replace the NIF.					
4	E6	NH1G-48T	25020401	5050	Port restarted, but not recovered from hardware failure.
	A port was restarted, but it has not recovered from a hardware failure. [Explanation of message variables] None. [Action] Replace the NIF.					
5	R6	NH1G-48T	25020200	5040	NIF recovered from hardware failure.
	A NIF has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.					
6	R6	NH1G-48T	25020201	5050	Port recovered from hardware failure.
	A port has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.					

3.12.5 Event location = NH1GS-6M

The following table describes switch failure and event information when the event location is NH1GS-6M.

Table 3-31: Switch failure and event information when the event location is NH1GS-6M

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
1	E6	NH1GS-6M	25020200	5840	NIF restarted because of its hardware failure.
	The NIF was restarted because the NIF hardware failed. [Explanation of message variables] None. [Action] Check for subsequent fault recoveries or fault recovery failure log entries. If recovery was successful, operations can resume. If recovery failed, replace the NIF.				
2	E6	NH1GS-6M	25020400	5840	NIF restarted, but not recovered from hardware failure.
	The NIF was restarted although the NIF had not recovered from the hardware failure or a failure detected during self-diagnosis. [Explanation of message variables] None. [Action] Replace the NIF.				
3	R6	NH1GS-6M	25020200	5840	NIF recovered from hardware failure.
	A NIF has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

3.12.6 Event location = NH10G-1RX

The following tables describe switch failure and event information when the event location is NH10G-1RX.

Table 3-32: Switch failure and event information when the event location is NH10G-1RX

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
1	E6	NH10G-1RX	25020200	5240	NIF restarted because of its hardware failure.
	The NIF was restarted because the NIF hardware failed. [Explanation of message variables] None. [Action] Check for subsequent fault recoveries or fault recovery failure log entries. If recovery was successful, operations can resume. If recovery failed, replace the NIF.				

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
2	E6	NH10G-1RX	25020201	5250	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 recovery failed, replace the NIF.				
3	E6	NH10G-1RX	25020400	5240	NIF restarted, but not recovered from hardware failure.
	The NIF was restarted although the NIF had not recovered from the hardware failure or a failure detected during self-diagnosis. [Explanation of message variables] None. [Action] Replace the NIF.				
4	E6	NH10G-1RX	25020401	5250	Port restarted, but not recovered from hardware failure.
	A port was restarted, but it has not recovered from a hardware failure. [Explanation of message variables] None. [Action] Replace the NIF.				
5	R6	NH10G-1RX	25020200	5240	NIF recovered from hardware failure.
	A NIF has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				
6	R6	NH10G-1RX	25020201	5250	Port recovered from hardware failure.
	A port has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

3.12.7 Event location = NH10G-4RX

The following table describes switch failure and event information when the event location is NH10G-4RX.

Table 3-33: Switch failure and event information when the event location is NH10G-4RX

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
					Description
1	E6	NH10G-4RX	25020200	5340	NIF restarted because of its hardware failure.
	The NIF was restarted because the NIF hardware failed. [Explanation of message variables] None. [Action] Check for subsequent fault recoveries or fault recovery failure log entries. If recovery was successful, operations can resume. If recovery failed, replace the NIF.				
2	E6	NH10G-4RX	25020201	5350	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 recovery failed, replace the NIF.				
3	E6	NH10G-4RX	25020400	5340	NIF restarted, but not recovered from hardware failure.
	The NIF was restarted although the NIF had not recovered from the hardware failure or a failure detected during self-diagnosis. [Explanation of message variables] None. [Action] Replace the NIF.				
4	E6	NH10G-4RX	25020401	5350	Port restarted, but not recovered from hardware failure.
	A port was restarted, but it has not recovered from a hardware failure. [Explanation of message variables] None. [Action] Replace the NIF.				
5	R6	NH10G-4RX	25020200	5340	NIF recovered from hardware failure.
	A NIF has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				
6	R6	NH10G-4RX	25020201	5350	Port recovered from hardware failure.
	A port has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

3.12.8 Event location = NH10G-8RX

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

NH10G-8RX.

Table 3-34: Switch failure and event information when the event location is NH10G-8RX

#	Event level	Event location	Message ID	Added info. Highest 4 digits	Message text
				Description	
1	E6	NH10G-8RX	25020200	5440	NIF restarted because of its hardware failure.
	The NIF was restarted because the NIF hardware failed. [Explanation of message variables] None. [Action] Check for subsequent fault recoveries or fault recovery failure log entries. If recovery was successful, operations can resume. If recovery failed, replace the NIF.				
2	E6	NH10G-8RX	25020201	5450	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 recovery failed, replace the NIF.				
3	E6	NH10G-8RX	25020400	5440	NIF restarted, but not recovered from hardware failure.
	The NIF was restarted although the NIF had not recovered from the hardware failure or a failure detected during self-diagnosis. [Explanation of message variables] None. [Action] Replace the NIF.				
4	E6	NH10G-8RX	25020401	5450	Port restarted, but not recovered from hardware failure.
	A port was restarted, but it has not recovered from a hardware failure. [Explanation of message variables] None. [Action] Replace the NIF.				
5	R6	NH10G-8RX	25020200	5440	NIF recovered from hardware failure.
	A NIF has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				
6	R6	NH10G-8RX	25020201	5450	Port recovered from hardware failure.
	A port has recovered from a hardware failure. [Explanation of message variables] None. [Action] None.				

Chapter

4. Access List Logs

This chapter describes the log data output by access list logging. When access list logging is in operation, information regarding packets discarded by the filter is output.

4.1 Access list log

4.1 Access list log

The following table describes the access list log.

Table 4-1: Access list log

#	Message text	Description
1	ACL:denied:*<denied filter point>*:*<protocol no.>* *<source ip address>*(*<source port>*, *<received interface>*) -> *<destination ip address>*(*<destination port>*, *<send interface>*), *<packets>*	A flow discarded by the filter was detected by access list logging. [Explanation of message variables] *<denied filter point>*: Point where the flow was discarded by the filter (receiving side or sending side) • IN: Discarded by the receiving-side filter • OUT: Discarded by the sending-side filter *<protocol no.>*: Upper-layer protocol number *<source ip address>*: Source IPv4 address *<source port>*: Source port number *<received interface>*: Receiving interface • VLAN *<vlan id>*: VLAN ID • Ethernet *<nif no.>*/*<port no.>*: Ethernet interface *<destination ip address>*: Destination IPv4 address *<destination port>*: Destination port number *<send interface>*: Sending interface • VLAN *<vlan id>*: VLAN ID • Ethernet *<nif no.>*/*<port no.>*: Ethernet interface *<packets>*: Number of relevant packets • *<packet>* packet: The number of displayed packets is 1 or less. • *<packets>* packets: The number of displayed packets is 2 or more. [Action] None.
2	ACL:denied:*<denied filter point>*:*<next header>* *<source ip address>*(*<source port>*, *<received interface>*) -> *<destination ip address>*(*<destination port>*, *<send interface>*), *<packets>*	A flow discarded by the filter was detected by access list logging. [Explanation of message variables] *<denied filter point>*: Point where the flow was discarded by the filter (receiving side or sending side) • IN: Discarded by the receiving-side filter • OUT: Discarded by the sending-side filter *<next header>*: Next header number *<source ip address>*: Source IPv6 address *<source port>*: Source port number *<received interface>*: Receiving interface • VLAN *<vlan id>*: VLAN ID • Ethernet *<nif no.>*/*<port no.>*: Ethernet interface *<destination ip address>*: Destination IPv6 address *<destination port>*: Destination port number *<send interface>*: Sending interface • VLAN *<vlan id>*: VLAN ID • Ethernet *<nif no.>*/*<port no.>*: Ethernet interface *<packets>*: Number of relevant packets • *<packet>* packet: The number of displayed packets is 1 or less. • *<packets>* packets: The number of displayed packets is 2 or more. [Action] None.

#	Message text	Description
3	ACL:denied:*<denied filter point>*:*<source mac>*(*<received interface>*) -> *<destination mac>*(*<ethernet type>* *<send interface>*), *<packets>*	A flow discarded by the filter was detected by access list logging. [Explanation of message variables] *<denied filter point>*: Point where the flow was discarded by the filter (receiving side or sending side) • IN: Discarded by the receiving-side filter • OUT: Discarded by the sending-side filter *<source mac>*: Source MAC address *<received interface>*: Receiving interface • VLAN *<vlan id>*: VLAN ID • Ethernet *<nif no.>*/*<port no.>*: Ethernet interface *<destination mac>*: Destination MAC address *<ethernet type>*: Ethernet type *<send interface>*: Sending interface • VLAN *<vlan id>*: VLAN ID • Ethernet *<nif no.>*/*<port no.>*: Ethernet interface *<packets>*: Number of relevant packets • *<packet>* packet: The number of displayed packets is 1 or less. • *<packets>* packets: The number of displayed packets is 2 or more. [Action] None.

Chapter

5. Tracking Object Log

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

5.1 Tracking object log

5.1 Tracking object log

The following table describes the tracking object log.

Table 5-1: Tracking object log

#	Message text	Description
1	Track object *<track object id>* is up. (type ICMP, address *<destination address>* [VRF *<vrf id>*])	Event (local device)
		The tracking status of the policy-based routing has transitioned from Down to Up. [Explanation of message variables] *<track object id>*: Tracking ID of the policy-based routing *<destination address>*: Polling destination address *<vrf id>*: VRF ID [Action] None.
2	Track object *<track object id>* is down. (type ICMP, address *<destination address>* [VRF *<vrf id>*])	Event (local device)
		The tracking status of the policy-based routing has transitioned from Up to Down. [Explanation of message variables] *<track object id>*: Tracking ID of the policy-based routing *<destination address>*: Polling destination address *<vrf id>*: VRF ID [Action] None.

Chapter

6. System Operation Panel Operation Log Information

This chapter describes the operation log information for the system log panel. Information about the operation instructions issued from the operation panel and the operation results are saved as operation log information for the system operation panel.

6.1 Operation log information for the system operation panel (KEY) [AX6700S]

This section describes the operation log information for the system operation panel when the log type is KEY.

The following table describes the operation log messages for the system operation panel.

Table 6-1: Operation log messages for the system operation panel (log type: KEY) [AX6700S]

#	Message text	Description
1	SOP:Inactivate operation canceled.	Information (local device)
		NO is selected for the inactivate instruction (this message is displayed only for the active system). [Explanation of message variables] None. [Action] None.
2	SOP:Inactivate operation confirmed.	Information (local device)
		YES is selected for the inactivate instruction (this message is displayed only for the active system). [Explanation of message variables] None. [Action] None.
3	SOP:Inactivate operation of *<board>* selected.	Information (local device)
		The inactivate instruction for *<board>* is selected (this message is displayed only for the active system). [Explanation of message variables] *<board>*: Board type • Standby system: Standby system • BSU *<bsu no.>*: BSU number • NIF *<nif no.>*: NIF number [Action] None.
4	SOP:Activate operation canceled.	Information (local device)
		NO is selected for the activate instruction (this message is displayed only for the active system). [Explanation of message variables] None. [Action] None.
5	SOP:Activate operation confirmed.	Information (local device)
		YES is selected for the activate instruction (this message is displayed only for the active system). [Explanation of message variables] None. [Action] None.
6	SOP:Activate operation of *<board>* selected.	Information (local device)

#	Message text	Description
		The `activate` instruction for *\<board\>* is selected (this message is displayed only for the active system). [Explanation of message variables] *\<board\>*: Board type • `Standby system`: Standby system • `BSU` *\<bsu no.\>*: BSU number • `NIF` *\<nif no.\>*: NIF number [Action] None.
7	SOP:Shutdown operation canceled.	Information (local device)
		`NO` is selected for the `shutdown` instruction. [Explanation of message variables] None. [Action] None.
8	SOP:Shutdown operation confirmed.	Information (local device)
		`Yes` is selected for the `shutdown` instruction. [Explanation of message variables] None. [Action] None.

6.2 Operation log information for the system operation panel (KEY) [AX6600S] [AX6300S]

This section describes the operation log information for the system operation panel when the log type is KEY.

The following table describes the operation log messages for the system operation panel.

Table 6-2: Operation log messages for the system operation panel (log type: KEY) [AX6600S] [AS6300S]

#	Message text	Description
1	SOP:Inactivate operation canceled.	Information (local device)
		NO is selected for the inactivate instruction (this message is displayed only for the active system). [Explanation of message variables] None. [Action] None.
2	SOP:Inactivate operation confirmed.	Information (local device)
		YES is selected for the inactivate instruction (this message is displayed only for the active system). [Explanation of message variables] None. [Action] None.
3	SOP:Inactivate operation of *<board>* selected.	Information (local device)
		The inactivate instruction for *<board>* is selected (this message is displayed only for the active system). [Explanation of message variables] *<board>*: Board type • Standby system: Standby system • NIF *<nif no.>*: NIF number [Action] None.
4	SOP:Activate operation canceled.	Information (local device)
		NO is selected for the activate instruction (this message is displayed only for the active system). [Explanation of message variables] None. [Action] None.
5	SOP:Activate operation confirmed.	Information (local device)
		YES is selected for the activate instruction (this message is displayed only for the active system). [Explanation of message variables] None. [Action] None.
6	SOP:Activate operation of *<board>* selected.	Information (local device)

#	Message text	Description
		The `activate` instruction for *<board>* is selected (this message is displayed only for the active system). [Explanation of message variables] *<board>*: Board type • `Standby system`: Standby system • `NIF` *<nif no.>*: NIF number [Action] None.
7	SOP:Shutdown operation canceled.	Information (local device)
		`NO` is selected for the `shutdown` instruction. [Explanation of message variables] None. [Action] None.
8	SOP:Shutdown operation confirmed.	Information (local device)
		`Yes` is selected for the `shutdown` instruction. [Explanation of message variables] None. [Action] None.

6.3 Operation log information for the system operation panel (RSP) [AX6700S]

This section describes the operation log information for the system operation panel when the log type is `RSP`.

The following table describes the operation log messages for the system operation panel.

Table 6-3: Operation log messages for the system operation panel (log type: RSP) [AX6700S]

#	Message text	Description
1	SOP:*<board>* will be stopped because of shutdown operation.	Information (local device)
		The *<board>* will be stopped because of the `shutdown` instruction. [Explanation of message variables] *<board>*: Board type • `Active system`: Active system • `Standby system`: Standby system • `All system`: Active and standby systems [Action] None.
2	SOP:Canceled inactivate operation because activated board not found.	Information (local device)
		The `inactivate` operation was not performed because the activated board was not found (this message is displayed only for the active system). [Explanation of message variables] None. [Action] None.
3	SOP:Canceled activate operation because inactivated board not found.	Information (local device)
		The `activate` operation was not performed because the inactivated board was not found (this message is displayed only for the active system). [Explanation of message variables] None. [Action] None.
4	SOP:Can't accept command (system is busy).	Error response for the `inactivate` or `activate` command for the board.
		The `inactivate` or `activate` operation cannot be accepted because the system is busy. [Explanation of message variables] None. [Action] None.
5	SOP:Can't display Line status because all NIF Not Active.	Information (local device)

#	Message text	Description
		The line status was not displayed because all NIFs were not active (this message is displayed only for the active system). [Explanation of message variables] None. [Action] None.
6	SOP:Can't execute.	Error response for the `inactivate` or `activate` command for the board.
		The `inactivate` or `activate` command for the board cannot be executed. [Explanation of message variables] None. [Action] None.
7	SOP:Can't execute this command in standby system.	Error response for the `inactivate` or `activate` command for the board.
		The `inactivate` or `activate` command for the board cannot be executed in the standby system. [Explanation of message variables] None. [Action] None.
8	SOP:Illegal NIF -- *<nif no.>*.	Error response for the `inactivate` or `activate` command for the NIF.
		The NIF number is outside the valid range. [Explanation of message variables] *<nif no.>*: NIF number [Action] None.
9	SOP:Illegal BSU -- *<bsu no.>*.	Error response for the `inactivate` or `activate` command for the BSU.
		The BSU number is outside the valid range. [Explanation of message variables] *<bsu no.>*: BSU number [Action] None.
10	SOP:NIF *<nif no.>* is already active.	Error response for the `activate` command for the NIF.
		The specified NIF is in the active state. [Explanation of message variables] *<nif no.>*: NIF number [Action] None.
11	SOP:NIF *<nif no.>* is already inactivated.	Error response for the `inactivate` command for the NIF.
		The specified NIF is in the inactive state. [Explanation of message variables] *<nif no.>*: NIF number [Action] None.
12	SOP:NIF *<nif no.>* is already initializing.	Error response for the `activate` command for the NIF.

#	Message text	Description
		The specified NIF is being initialized. [Explanation of message variables] *<nif no.>*: NIF number [Action] None.
13	SOP:NIF *<nif no.>* is not connected.	Error response for the `inactivate` or `activate` command for the NIF.
		The specified NIF is not installed. [Explanation of message variables] *<nif no.>*: NIF number [Action] None.
14	SOP:NIF *<nif no.>* is during the inactivate process.	Error response for the `activate` command for the NIF.
		The specified NIF is being inactivated. [Explanation of message variables] *<nif no.>*: NIF number [Action] None.
15	SOP:NIF *<nif no.>* is failed.	Error response for the `inactivate` or `activate` command for the NIF.
		The specified NIF is not in the active state. [Explanation of message variables] *<nif no.>*: NIF number [Action] None.
16	SOP:NIF *<nif no.>* is disabled.	Error response for the `inactivate` or `activate` command for the NIF.
		The specified NIF is disabled by the `shutdown` configuration command. [Explanation of message variables] *<nif no.>*: NIF number [Action] None.
17	SOP:BSU *<bsu no.>* is already active.	Error response for the `activate` command for the BSU.
		The specified BSU is in the active state. [Explanation of message variables] *<bsu no.>*: BSU number [Action] None.
18	SOP:BSU *<bsu no.>* is already inactivated.	Error response for the `inactivate` command for the BSU.
		The specified BSU is in the inactive state. [Explanation of message variables] *<bsu no.>*: BSU number [Action] None.
19	SOP:BSU *<bsu no.>* is already initializing.	Error response for the `activate` command for the BSU.

#	Message text	Description
		The specified BSU is already being initialized. [Explanation of message variables] *<bsu no.>*: BSU number [Action] None.
20	SOP:BSU *<bsu no.>* is not connected.	Error response for the `inactivate` or `activate` command for the BSU.
		The specified BSU is not installed. [Explanation of message variables] *<bsu no.>*: BSU number [Action] None.
21	SOP:BSU *<bsu no.>* is failed.	Error response for the `activate` command for the BSU.
		The specified BSU is not in the active state. [Explanation of message variables] *<bsu no.>*: BSU number [Action] None.
22	SOP:BSU *<bsu no.>* is disabled.	Error response for the `inactivate` or `activate` command for the BSU.
		The specified BSU is disabled by the `shutdown` configuration command. [Explanation of message variables] *<bsu no.>*: BSU number [Action] None.
23	SOP:BSU *<bsu no.>* that controls NIF *<nif no.>* is inactivated.	Error response for the `inactivate` or `activate` command for the NIF.
		The BSU that controls the specified NIF is in the inactive state. [Explanation of message variables] *<bsu no.>*: BSU number *<nif no.>*: NIF number [Action] None.
24	SOP:BSU *<bsu no.>* that controls NIF *<nif no.>* is not connected.	Error response for the `inactivate` or `activate` command for the NIF.
		The BSU that controls the specified NIF is not installed. [Explanation of message variables] *<bsu no.>*: BSU number *<nif no.>*: NIF number [Action] None.
25	SOP:BSU *<bsu no.>* that controls NIF *<nif no.>* is failed.	Error response for the `inactivate` or `activate` command for the NIF.
		The BSU that controls the specified NIF is not in the active state. [Explanation of message variables] *<bsu no.>*: BSU number *<nif no.>*: NIF number [Action] None.

#	Message text	Description
26	SOP:BSU *<bsu no.>* that controls NIF *<nif no.>* is initializing.	Error response for the `inactivate` or `activate` command for the NIF.
		The BSU that controls the specified NIF is being initialized. [Explanation of message variables] *<bsu no.>*: BSU number *<nif no.>*: NIF number [Action] None.
27	SOP:BSU *<bsu no.>* that controls NIF *<nif no.>* is disabled.	Error response for the `inactivate` or `activate` command for the NIF.
		The BSU that controls the specified NIF is disabled by the `shutdown` configuration command. [Explanation of message variables] *<bsu no.>*: BSU number *<nif no.>*: NIF number [Action] None.
28	SOP:Rejected operation because of Standby.	Information (local device)
		The operation was not performed because the system was the standby system (this message is displayed only for the standby system). [Explanation of message variables] None. [Action] None.
29	SOP:Return to Main Menu because can't get the information.	Warning (local device)
		The display returns to the Main Menu because no information can be obtained. [Explanation of message variables] None. [Action] None.
30	SOP:Shutdown operation failed.	Warning (local device)
		The `shutdown` instruction has failed. [Explanation of message variables] None. [Action] None.
31	SOP:Standby system is already inactivated.	Error response for the `inactivate` command for the standby system.
		The standby system has already been inactivated. [Explanation of message variables] None. [Action] None.
32	SOP:Standby system is not connected.	Error response for the `inactivate` or `activate` command for the standby system.

#	Message text	Description
		The standby system is not installed. [Explanation of message variables] None. [Action] None.
33	SOP:Standby system is not inactivated.	Error response for the `activate` command for the standby system.
		The standby system is not inactivated. [Explanation of message variables] None. [Action] None.

6.4 Operation log information for the system operation panel (RSP) [AX6600S] [AX6300S]

This section describes the operation log information for the system operation panel when the log type is RSP.

The following table describes the operation log messages for the system operation panel.

Table 6-4: Operation log messages for the system operation panel (log type: RSP) [AX6600S] [AS6300S]

#	Message text	Description
1	SOP:*<board>* will be stopped because of shutdown operation.	Information (local device)
		The *<board>* will be stopped because of the shutdown instruction. [Explanation of message variables] *<board>*: Board type • Active system: Active system • Standby system: Standby system • All system: Active and standby systems [Action] None.
2	SOP:Canceled inactivate operation because activated board not found.	Information (local device)
		The inactivate operation was not performed because the activated board was not found (this message is displayed only for the active system). [Explanation of message variables] None. [Action] None.
3	SOP:Canceled activate operation because inactivated board not found.	Information (local device)
		The activate operation was not performed because the inactivated board was not found (this message is displayed only for the active system). [Explanation of message variables] None. [Action] None.
4	SOP:Can't accept command (system is busy).	Error response for the inactivate or activate command for the board.
		The inactivate or activate operation cannot be accepted because the system is busy. [Explanation of message variables] None. [Action] None.
5	SOP:Can't display Line status because all NIF Not Active.	Information (local device)

#	Message text	Description
		The line status was not displayed because all NIFs were not active (this message is displayed only for the active system). [Explanation of message variables] None. [Action] None.
6	SOP:Can't execute.	Error response for the `inactivate` or `activate` command for the board.
		The `inactivate` or `activate` command for the board cannot be executed. [Explanation of message variables] None. [Action] None.
7	SOP:Can't execute this command in standby system.	Error response for the `inactivate` or `activate` command for the board.
		The `inactivate` or `activate` command for the board cannot be executed in the standby system. [Explanation of message variables] None. [Action] None.
8	SOP:Illegal NIF -- *\<nif no.\>*.	Error response for the `inactivate` or `activate` command for the NIF.
		The NIF number is outside the valid range. [Explanation of message variables] *\<nif no.\>*: NIF number [Action] None.
9	SOP:NIF *\<nif no.\>* is already active.	Error response for the `activate` command for the NIF.
		The specified NIF is in the active state. [Explanation of message variables] *\<nif no.\>*: NIF number [Action] None.
10	SOP:NIF *\<nif no.\>* is already inactivated.	Error response for the `inactivate` command for the NIF.
		The specified NIF is in the inactive state. [Explanation of message variables] *\<nif no.\>*: NIF number [Action] None.
11	SOP:NIF *\<nif no.\>* is already initializing.	Error response for the `activate` command for the NIF.
		The specified NIF is being initialized. [Explanation of message variables] *\<nif no.\>*: NIF number [Action] None.
12	SOP:NIF *\<nif no.\>* is not connected.	Error response for the `inactivate` or `activate` command for the NIF.

#	Message text	Description
		The specified NIF is not installed. [Explanation of message variables] *<nif no.>*: NIF number [Action] None.
13	SOP:NIF *<nif no.>* is during the inactivate process.	Error response for the `activate` command for the NIF.
		The specified NIF is being inactivated. [Explanation of message variables] *<nif no.>*: NIF number [Action] None.
14	SOP:NIF *<nif no.>* is failed.	Error response for the `inactivate` or `activate` command for the NIF.
		The specified NIF is not in the active state. [Explanation of message variables] *<nif no.>*: NIF number [Action] None.
15	SOP:NIF *<nif no.>* is disabled.	Error response for the `inactivate` or `activate` command for the NIF.
		The specified NIF is disabled by the `shutdown` configuration command. [Explanation of message variables] *<nif no.>*: NIF number [Action] None.
16	SOP:Rejected operation because of Standby.	Information (local device)
		The operation was not performed because the system was the standby system (this message is displayed only for the standby system). [Explanation of message variables] None. [Action] None.
17	SOP:Return to Main Menu because can't get the information.	Warning (local device)
		The display returns to the Main Menu because no information can be obtained. [Explanation of message variables] None. [Action] None.
18	SOP:Shutdown operation failed.	Warning (local device)
		The `shutdown` instruction has failed. [Explanation of message variables] None. [Action] None.

#	Message text	Description
19	SOP:Standby system is already inactivated.	Error response for the `inactivate` command for the standby system.
		The standby system has already been inactivated. [Explanation of message variables] None. [Action] None.
20	SOP:Standby system is not connected.	Error response for the `inactivate` or `activate` command for the standby system.
		The standby system is not installed. [Explanation of message variables] None. [Action] None.
21	SOP:Standby system is not inactivated.	Error response for the `activate` command for the standby system.
		The standby system is not inactivated. [Explanation of message variables] None. [Action] None.

Index